

Employing a Secure Cipher Does not Guarantee the Security of RFID Protocols

Masoumeh Safkhani, Nasour Bagheri, Pedro Peris-Lopez, Juan M. E. Tapiador

Abstract—It is a common practice to employ encryption functions to provide security for an application. On the other hand, it is well known that a bad usage of even a very strong cryptographic primitive can destroy the security of an application/scheme. Several RFID protocols have recently been proposed whose security reside on encryption primitives. Among these works we pay attention on the following ones: 1) Khan and Moessner proposed a new RFID authentication protocol [5]; 2) Kapoor and Piramuthu presented a single-tag and single-owner ownership transfer protocol [3]; 3) Kapoor et al. proposed a multi-tag and multi-owner ownership transfer scheme in supply chains [4]; and 4) Zhou et al. presented multi-level RFID tag ownership and transfer in health-care environments [8]. In these four proposals the authors state that their schemes are secure against de-synchronization attacks. Nevertheless, in this article we present efficient de-synchronization attacks against the above mentioned protocols. Our attacks are based on the inappropriate use of the encryption function. The success probability of all the proposed attacks is almost one while the complexity is just one execution of the protocol.

Index Terms—IEEEtran, journal, L^AT_EX, paper, template. RFID, Cryptanalysis, Authentication, Protocol, De-synchronization Attacks, Man-In-The-Middle.

I. INTRODUCTION

A common RFID system includes three parties: tags, readers and a back-end database. The tag, which can be accessed by authorized readers, is attached to an item (i.e., person, animal, or object) and includes some information linked to the tag holder. The back-end database may be used to provide some extra storage or computational capabilities to the reader and also keeps a high level information related to the tag holder.

In an RFID system authentication protocols are used by readers and tags in order to authenticate each other. It commonly is a game-playing argument between both entities. In such game, one of the principals in the protocol sends a(some) challenge(s) to the other principal and then it verifies the response(s) received. The majority of RFID authentication protocols require the authentication process on both sides. This sort of protocols are named as mutual authentication protocols. However, in certain applications only one party is authenticated [5].

On the other hand, nowadays, RFID tags are increasingly being used to identify, track and sense ambient conditions

of tagged items [3]. Most of these applications impose that at various moments during the tag life, the owner of a tag can change. Therefore we need a mechanism to transfer the ownership of tagged objects from the current owner to a new owner. This kind of mechanisms are known as ownership transfer schemes. Attempting to provide the required security in a RFID system, strong (or regrettably weak) mutual authentication and ownership transfer protocols, which rely on encryption or cryptographic hash functions, have appeared in the literature. In this research direction, Khan and Moessner [5] recently proposed a lightweight mutual authentication protocol, Kapoor and Piramuthu [3] presented a single-tag and single-owner ownership transfer scheme, Kapoor *et al.* [4] generalized the above proposal for multi-tag and multi-owner ownership transfer scheme and Zhou *et al.* [8] proposed a multi-level RFID tag ownership and transfer in health-care environments. The just mentioned schemes use encryption functions to offer an appropriate security level. Furthermore the protocol designers claim optimal security for their proposed protocols –including protection against de-synchronization states. Nevertheless, in this paper we present efficient de-synchronization attacks against these four protocols. The success probability of the proposed attacks is almost one and only requires one execution of the protocol.

The proposed attacks mainly exploit that an encrypted message is accepted by an entity without any validation of its origin and/or without any checking of its integrity. Hence, in a man-in-the-middle attack whether the adversary changes either the key K used in the encryption function or the cipher-text C (in the RFID context this second strategy is the simplest one since messages passed through the insecure radio channel), then the receiver will decrypt that altered message and thus the extracted plain-text P' would be incorrect. It must be noted that any change on K or C will not affect the proper working of the decryption function, but the output P' value would be a random value (in comparison to the correct P). In Table I we provide some encryption examples of same/related P s with same/related K s for the AES block cipher. As shown, any modification on any of the inputs (K or P) makes the output (C) –and consequently the decrypted plain-text (P')– random and unpredictable.

Paper Organization: We introduce Khan and Moessner protocol in Section II, explain its security analysis concerning the mutual authentication protocol, and finally show a de-synchronization attack. In Section III we present our security analysis of Kapoor and Piramuthu ownership transfer protocol and then the security of the enhancement scheme proposed by

Masoumeh Safkhani is with the Department of Electrical Engineering, Iran University of Science and Technology (IUST), Tehran, Iran.

Nasour Bagheri is with the Department of Electrical Engineering, Shahid Rajaei Teachers Training University, Tehran, Iran.

Pedro Peris-Lopez and Juan M. E. Tapiador are with the Computer Security Lab (COSEC), Carlos III University of Madrid, Leganes, Madrid.



TABLE I
SAMPLE ENCRYPTIONS WITH AES [1].

Plain text (in hex)	Key (in hex)	Cipher text (in hex)
00000000000000000000000000000000	00000000000000000000000000000000	66e94bd4ef8a2c3b884cfa59ca342b2e
00000000000000000000000000000001	00000000000000000000000000000000	58e2fcccfa7e3061367f1d57a4e7455a
00000000000000000000000000000000	00000000000000000000000000000001	0545aad56da2a97c3663d1432a3d1c84
140f0f1011b5223d79587717fd9ec3a	00000000000000000000000000000000	00000000000000000000000000000000
6c5a75d8a41802ad5a35818dd5abfdcc	00000000000000000000000000000000	00000000000000000000000000000001
140f0f1011b5223d79587717fd9ec3a	00000000000000000000000000000001	9e909d68c4c95f750feaf3f47934a69a

Kapoor et al. is also scrutinized in Section IV. In Section V we present the security analysis of Zhou *et al.* ownership transfer protocol. After this, in Section VI we present a discussion about the principles for designing secure cryptographic protocols and its non-conformity in the four protocols examined through this paper. Finally, Section VII concludes the paper.

II. DESYNCHRONIZATION ATTACK AGAINST KHAN AND MOESSNER'S AUTHENTICATION PROTOCOL

Recently Khan and Moessner [5] have proposed a mutual authentication protocol for RFID systems, hence forth denoted by *KM*-protocol. A description of *KM*-protocol is depicted in Fig. 1. In this protocol (Key_{c1}, Key_{c2}) is a pair of keys for tags belonging to the same class and K_c represents the class key. $ID = ID_l || ID_h$ is the unique identifier of a tag (lower and higher half respectively) and $||$ denotes concatenation. T_c symbolizes the authentication counter in the tag side and $T_{c_{stored}}$ denotes its corresponding record in the server. The authors state that $h(a, b)$ is a cipher or alternatively a hash function [5, Sec. III]. In the protocol calculation, they use $h^{-1}(a, b)$ but it is not possible to compute the inverse of a hash function and thus $h(a, b)$ must be an encryption function.

We present a roughly description of the protocol but details can be checked in the original paper. In *KM*-protocol, the tag is authenticated by the following exchanged of messages. First, the reader generates a random number R_r and sends $m_1 = R_r$ to the tag. Upon receiving m_1 , the tag generates a random number R_t , increments T_c , computes $h_1 = h((R_r || R_t) \oplus ID, Key_{c1})$ and $h_2 = h((R_r || 0) \oplus (R_t || R_t) \oplus ID \oplus T_c, Key_{c2})$, and finally sends $m_2 = k_c || h_1 || h_2$ to the reader. Then, the reader forwards $R_r || m_2$ to the server. The server follows the following procedure: 1) it fetches the key pair that belongs to k_c ; 2) it decrypts h_1 and h_2 with keys Key_{c1} and Key_{c2} respectively; 3) it reveals the upper part of ID as $ID_h = h^{-1}(h_1, Key_{c1}) \oplus (R_r || 0)$; 4) it looks up ID_l and $T_{c_{stored}}$ from its database and reveals R_t as $R_t = h^{-1}(h_1, Key_{c1}) \oplus (R_r || 0) \oplus (ID_h || ID_l)$; 5) it reveals the tag counter as $T_c = h^{-1}(h_2, Key_{c2}) \oplus (R_t || R_t) \oplus (R_r || 0) \oplus (ID_h || ID_l)$; 6) If $(T_c > T_{c_{stored}})$, it sets $m_3 = \text{Authentic}$. Otherwise $m_3 = \text{Not Authentic}$. Finally, the server sends m_3 to the reader.

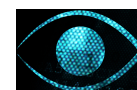
A. De-synchronization Attack

Generally, in a de-synchronization attack the adversary forces the tag and the reader to update their shared values such that both entities will not be able to authenticate each other hence forth.

In *KM*-protocol each query sent to a target tag, either by a legitimate reader or an adversary, increments its counter T_c . Khan and Moessner [5] state that it would be possible to de-synchronize the tag and the reader if the adversary swamps the tag with many queries until its counter starts from zero again. To overcome this drawback, the authors assume that the authentication counter has a length l greater or equal to 32 bits (i.e., $|T_c| > 32$). Nevertheless, in this section, we present a different de-synchronization attack, which does not need to restart the counter to a zero value but forces the reader to set its counter to a value far ahead from the counter value in the tag side. The main observation is that the server only verifies the correctness of h_1 and does not verify the correctness of the received h_2 . Hence the adversary could replace h_2 by any arbitrary value and it would be accepted by the server.

Our adversary, $\mathcal{A}$, is a man in the middle adversary which stays in the public radio channel between the tag and the reader and has the ability to eavesdrop, block or modify the messages exchanged between the reader and the tag, and vice versa. In this attack, when the tag sends $m_2 = k_c || h_1 || h_2$ to the reader, $\mathcal{A}$ intercepts m_2 , generates a random number and assigns it to h_2 , denoted by h'_2 . Then $\mathcal{A}$ sends $m'_2 = k_c || h_1 || h'_2$ to the reader, and finally the reader forwards $R_r || m'_2$ to the server. Upon the reception of that message, the server: 1) fetches the key pair that belongs to k_c ; 2) decrypts h_1 and h'_2 with Key_{c1} and Key_{c2} respectively; 3) discloses the upper part of ID as $ID_h = h^{-1}(h_1, Key_{c1}) \oplus (R_r || 0)$; 4) looks up ID_l and $T_{c_{stored}}$ from its database and reveals R_t as $R_t = h^{-1}(h_1, Key_{c1}) \oplus (R_r || 0) \oplus (ID_h || ID_l)$; 5) it discloses the tag counter as $T'_c = h^{-1}(h'_2, Key_{c2}) \oplus (R_t || R_t) \oplus (R_r || 0) \oplus (ID_h || ID_l)$; 6) If $(T'_c > T_{c_{stored}})$ the server sets $m_3 = \text{Authentic}$ and $T_{c_{stored}} = T'_c$. Finally the server sends m_3 to the reader.

After conducting the above described attack, the tag can not be authenticated by the reader in future sessions as explained below. Assuming that the tag has not been employed for a long time, T_c would be a small value (i.e., $T_c \ll 2^{l-1}$ where l is the bit length of T_c). As consequence of sending a random h'_2 , the expected value for the revealed value of T'_c (step 5 in the previous paragraph) is 2^{l-1} , where $|T'_c| = l$. Hence, the server authenticates the tag (i.e., $T'_c > T_{c_{stored}}$) and updates $T_{c_{stored}} = T'_c \approx 2^{l-1}$ while the T_c in the tag side is not so bigger value – if the adversary is not so lucky and $T'_c < T_{c_{stored}}$, she simply has to repeat the attack and try with another h'_2 random value. Therefore, the adversary could force the server to set its $T_{c_{stored}}$ to a value far advance from the value of T_c in the tag side. Hence forth, the server would not authenticate the tag since $(T'_c < T_{c_{stored}})$. For instance, assuming $l = 64$, which satisfies the designer criteria regarding



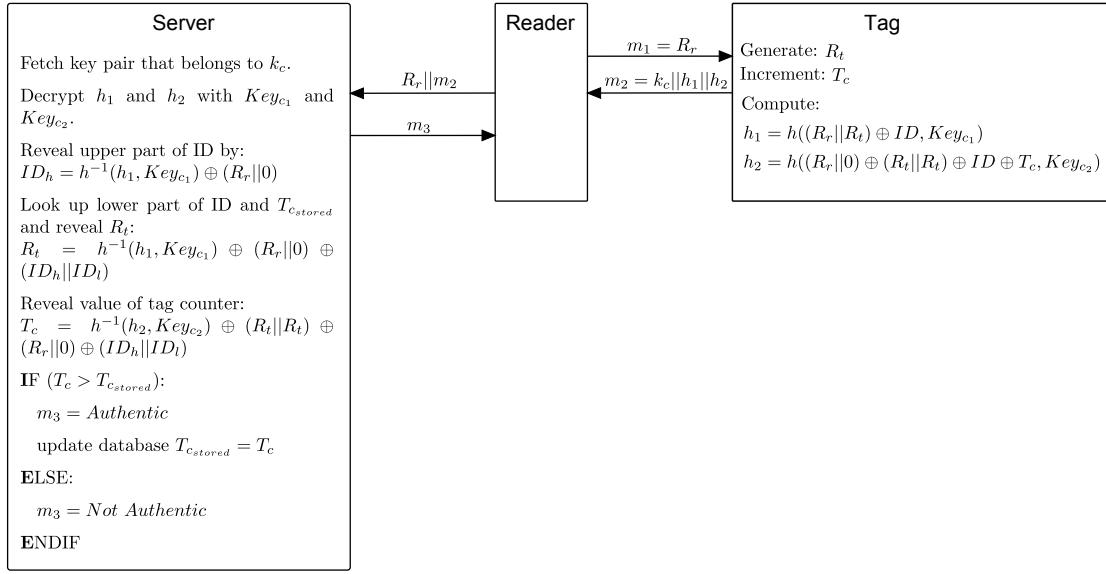


Fig. 1. The KM-protocol description [5].

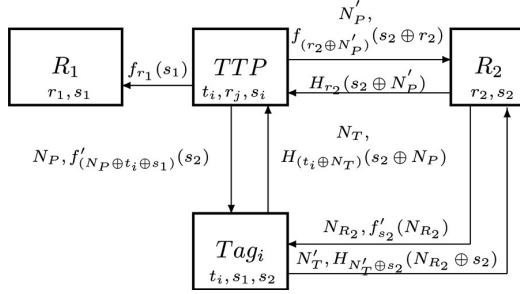


Fig. 2. The KP-protocol description [5].

shared between the tag and the current owner (R_1) and t_i is the secret shared between the tag and TTP. Upon receiving that message, the tag extracts s_2 from the encrypted message and replaces the current secret key s_1 by the new key s_2 . In addition, the tag acknowledges by generating a random nonce N_T and sending the pair $(N_T, H_{(t_i \oplus N_T)}(s_2 \oplus N_P))$. Then, TTP informs R_1 that his privileges on this tag are being revoked. It simply sends a revoke message and a keyed encryption token $f_{r_1}(s_1)$. Next, TTP grants new owners (R_2) full permissions along with the privileges for the tag. The rest of the protocol can be followed from Fig. 2 but it is not relevant for our attack.

the length of the counter ($l > 32$), we expect that after executing the proposed attack, T_{c_stored} is updated to a value around 2^{63} . For this, we can fairly state that the tag would not be authenticated by the reader in the next-legitimate sessions as result of the unsynchronized counters (i.e., $T_{c_stored} \gg T'_c$).

III. DE-SYNCHRONIZATION ATTACK AGAINST KAPOOR AND PIRAMUTHU'S OWNERSHIP TRANSFER PROTOCOL

Ownership transfer protocols are designed with the purpose of transferring ownership of an item that is RFID labelled. Kapoor and PIRAMUTHU [3] have recently proposed an Ownership Transfer Protocol (OTP) with Trusted Third Party (TTP), hence forth denoted by KP-protocol. The protocol is depicted in Fig. 2, but for more details we urge the reader to consult the original paper [3, Sec. III]. Note that $f_k(\cdot)$ and $f'_k(\cdot)$ denote keyed (with key k) encryption functions.

In this protocol, upon receiving an ownership transfer (OT) request, the TTP generates a random nonce N_P and a secret key s_2 which will be shared between the tag and the new owner (R_2). It then computes $f'_{(N_P \oplus t_i \oplus s_1)}(s_2)$ and sends the tuple $(N_P, f'_{(N_P \oplus t_i \oplus s_1)}(s_2))$ to the tag, where s_1 is the secret

A. De-synchronization Attack

As described previously, once the tag updates its secret key from s_1 (old owner R_1) to s_2 (new owner R_2), it will not be accessible by R_1 any more, otherwise it would be vulnerable to a window attack in which for a fraction time both current and new owners could access to the tag [9]. On the other hand, the new secret s_2 is derived from the message $X = f'_{(N_P \oplus t_i \oplus s_1)}(s_2)$ sent by TTP (i.e., $s_2 = f'^{-1}_{(N_P \oplus t_i \oplus s_1)}(X)$). Nevertheless, the protocol does not include any checking mechanism to verify the origin (source) and correctness of the extracted s_2 value. That is, any value obtained from the tag calculations –decryption of X – is accepted without further checking and it is used as the new secret shared with the new owner. An adversary can exploit this fault to render a tag in a de-synchronized state and consequently the OT system. The procedure of the proposed attack is described below.

An adversary intercepts the pair $(N_P, f'_{(N_P \oplus t_i \oplus s_1)}(s_2))$ sent from TTP to the tag and replaces it by any desired pair (x, y) such that $(x, y) \neq (N_P, f'_{(N_P \oplus t_i \oplus s_1)}(s_2))$. The tag is thus cheated to update its current secret to $s'_2 = f'^{-1}_{(x \oplus t_i \oplus s_1)}(y)$. This new key s'_2 does not match any of the TTP records (new s_2 and old s_1). The probability of success in the proposed

attack is $1 - 2^{-n+2}$, where n is the bit length of s_1 . Hence, following this attack, the tag updates its secret key to a value that neither new owners nor TTP has knowledge of it and prevents its access in future-legitimate communications –that is, the tag is render inaccessible. The success probability of the given attack is almost one and the complexity is negligible.

In the above attack, one may argue that the message sent from the tag to TTP ($((N_T, H_{(N_T \oplus t_i)}(s'_2 \oplus N_P))))$) would not be accepted by TTP because the adversary previously altered the tuple sent from TTP to the tag – in consequence it provoked an incorrect key derived by the tag – and the acknowledge tuple generated by the tag would not be valid with high probability. Although it gives the TTP the ability to discover potential attacks, however, it cannot react. In fact, to contact with the tag, TTP needs the tag's secret, which was just updated to s'_2 due to the attack, and it does not know it. Hence, the tag is de-synchronized forever and neither TTP nor the owners can access it any more.

IV. DESYNCHRONIZATION ATTACK AGAINSTS KAPOOR *et al.*'S OWNERSHIP TRANSFER PROTOCOL

While in the previous Section we have analysed the security of a protocol which transfers the ownership of a single tag to a new owner reader, it is not uncommon scenarios in which the tag ownership is shared among multiple owners, and its dual, the case of an object labelled with multiple tags. Motivated by this kind of scenarios, Kapoor *et al.* [4] proposed a shared ownership transfer protocol (multiple-owners) and a protocol for inclusion and exclusion of tags in a multiple-tagged object. The scheme, called *KZP*-protocol in short, is the object of our security analysis. We sketch the protocol in Fig. 3 and interested readers can consult the original paper for details [4, Sec. 3.1].

Similarly to the KP -protocol, in this protocol upon receiving an ownership transfer (OT) request, the TTP generates a random nonce N_P and a new key s_2 . This new secret key will be shared between the tag and the new owner R_2 (or a group of owners $R_{21}, R_{22}, \dots, R_{2M}$). Finally, TTP computes $f'_{(N_P \oplus t_i \oplus s_1)}(s_2)$ and sends the pair $(N_P, f'_{(N_P \oplus t_i \oplus s_1)}(s_2))$ to the tag, where s_1 is the secret shared between the tag and the current owner R_1 (or the group $R_{11}, R_{12}, \dots, R_{1M}$) and t_i is the secret shared between the tag and the TTP. Once that message is received, the tag extracts s_2 from the encrypted message and updates its secret key by replacing the current key s_1 by the new secret key s_2 . The tag then acknowledges the server by generating a random nonce N_T and sending the token $(N_T, H_{(N_T \oplus t_i)}(s_2 \oplus N_P))$. After that, TTP informs the current owners $R_{11}, R_{12}, \dots, R_{1M}$ that their privileges on this tag were revoked. It sends both a revoke message and a cryptographic token $f_{r_{1i}}(s_1)$ to each of the owners in the group, where r_{1i} is a secret shared between R_{1i} and TTP. Next, TTP grants the new owners $(R_{21}, R_{22}, \dots, R_{2M})$ full permissions along with any privileges for the tag. The rest of the protocol can be followed from Fig. 3, but this part has not influence on our attack.

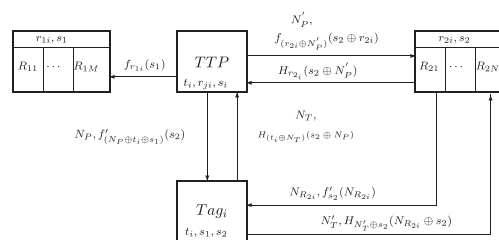


Fig. 3. The *KZP*-protocol description [4].

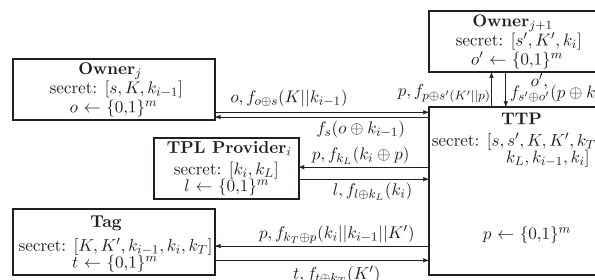


Fig. 4. The *ZYP*-protocol description [8].

A. De-synchronization Attack

In *KZP*-protocol, as occurred in *KP*-protocol, once the tag executes the updating of its secret key from s_1 to s_2 , R_1 cannot gain access to the tag any more, otherwise it will be vulnerable to window attack [9]. As an important drawback in the design of the protocol, the new key s_2 is exclusively derived from the messages that was supposedly sent by the OTP. Let assume that OTP sends $X = f'_{(N_P \oplus t_i \oplus s_1)}(s_2)$, then the key would be obtained by decrypting the received message $s_2 = f'^{-1}_{(N_P \oplus t_i \oplus s_1)}(X)$. Nevertheless, the receiver (tag) can not check neither the correctness of the new key nor the source of this message – it incorrectly assumes that all messages come from a honest OTP. These bad properties can be exploited by an attacker against the protocol as explained below.

Simply, and due to the resemblance with the *KP*-protocol, the adversary could follow the same strategy. She intercepts the tuple $(N_P, f'_{(N_P \oplus t_i \oplus s_1)(s_2)})$ sent by a honest TTP and changes this by a random pair x, y completely different to the values intercepted (i.e., $(x, y) \neq (N_P, f'_{(N_P \oplus t_i \oplus s_1)(s_2)})$). As consequence of this, the tag would update its secret key ($s'_2 = f'^{-1}_{(x \oplus t_i \oplus s_1)(y)}$) with the key sent by the supplanted TTP – the attacker. So, there would not be a match between s'_2 and the records (s_2, s_1) kept by the TTP. The probability of success in this attack is almost one ($1 - 2^{-n+2}$), being n the bit length of s_i , and it renders the tag inaccessible to the honest TTP in future communications.

V. DE-SYNCHRONIZATION ATTACK AGAINST ZHOU *et al.*'S OWNERSHIP TRANSFER PROTOCOL

Zhou, Yoon and Piramuthu [8] have considered a case that includes third party logistics providers and their role in temporary ownership transfer of items in a distributed health-care supply chain environment. Hence forth this protocol is

denoted by ZYP-protocol. In this protocol, the authors consider the simultaneous RF access of an RFID-tagged object by the object's owner and a temporary owner which could be the Third Party Logistics (TPL) provider. The protocol counts with two keys to access the tag, a main key (K) for the owner and a sub-key (k_i) for the TPL provider. The protocol is depicted in Fig. 4, but for more details we urge the reader to consult the original paper [8, Sec. 2.4]. Note that $f_k(\cdot)$ denotes keyed (with key k) encryption functions and TPL provider is assumed to be the one who transport the item between the two owners.

This protocol, includes four loops. The first loop occurs between the current owner and the TTP. This is used by the current owner to inform the TTP of the status change in the RFID-tagged object with the main key K and the sub-key k_{i-1} (i.e., this tagged object either changes ownership or goes through a provider or both). The second loop includes the TTP and the next owner, where the TTP generates a new main key (K') and informs the latter of that new key. In response, the new owner generates a new sub-key k_i and sends it to TTP in an encrypted token (i.e., $f_{s \oplus o}(p \oplus k_i)$ where p is a random number generated by TTP, o is a random number generated by the new owner and s denotes the shared key between the TTP and the new owner). The third and fourth loops are used by the TTP to inform the TPL provider and tag respectively of the new key(s) for the tag. It must be noted, that the first loop closed at the end of protocol.

To access the tag in the above mentioned protocol, the i^{th} owner is enforced to have knowledge of both main-key and sub-key for communicating with the tag, which can be replaced by the composite key, which might be obtained by computing the bitwise XOR of both values: $K \oplus k_i$ [8, Lats Para. Sec. 2.4].

A. De-synchronization Attack

As described previously, once the tag updates its secret key from k_{i-1} (old owner R_{i-1}) to k_i (new owner R_i), it will not be accessible by R_i any more, otherwise it would be vulnerable to a window attack in which for a fraction time both current and new owners could access to the tag [9]. On the other hand, the new secret k_i is derived from the message $X = f_{s \oplus o}(p \oplus k_i)$ sent by R_i (i.e., $k_i = f_{s \oplus o}^{-1}(X)$). Nevertheless, the protocol does not include any checking mechanism to verify the origin and correctness of the extracted k_i value. That is, any value obtained from the TTP calculations—decryption of X —is accepted without further checking and used as the new secret, which is expected to have been shared with R_i . An adversary could exploit this fault to render a tag in a de-synchronized state and consequently the OT system. The procedure is described below.

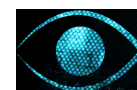
An adversary intercepts the pair $(o, f_{s \oplus o}(p \oplus k_i))$ sent from the i^{th} owner to the TTP and replaces it by any chosen pair (x, y) such that $(x, y) \neq (o, f_{s \oplus o}(p \oplus k_i))$. For this, the TTP is deceived to force the tag to update its current sub-key into $k'_i = f_{s \oplus x}^{-1}(y)$. This new key k'_i does not match any of the owners' sub-keys related to this tag (new k_i and old k_{i-1}). The probability of success in this proposed attack is $1 - 2^{-n+2}$, where n represents the bit length of k . Therefore, following

this attack, the tag would update its secret key to a value that neither new owners nor old owner would have knowledge of it and would render it inoperative for future-legitimate communications. The success probability of the given attack is almost one and the attack only requires the intervention in one protocol execution. We emphasize here that TTP has the knowledge of the new sub-key $k'_i = f_{s \oplus x}^{-1}(y)$ and it could update the tag sub-key. Nevertheless, it is not clear whether it is viable for some of the owners to convince the TTP to change the tag sub-key while she can not prove her privilege over the tag – the supposed owner does not have knowledge of the mentioned sub-key. Note that the main-key and the sub-key are mandatory for communicating with the tag. Even in the case that the TTP accepts to restart the whole protocol under the above assumption, it would be a serious pitfall for the protocol due to the lack of knowledge about one of the keys is disregarded, which contradicts the initial assumptions of the protocol and its claimed security properties.

VI. DISCUSSION

RFID protocols are prone to security pitfalls of every kind. Among theses, de-synchronization attacks are the most extended and commonly the first reported against new proposals. Nevertheless, the attacks presented in this article could have been prevented whether well-known principals and guidelines for the design of cryptographic protocols would have been followed. For instance, in 1996 Abadi and Needham already introduced principles and guidelines for designing secure cryptographic protocols [2]. More precisely, they state eleven principles that we summarize below:

- **Principle 1:** Every message should say what it means.
- **Principle 2:** The conditions applicable to a message have to be clearly set out in order its acceptability or not can be evaluated by an external reviewer.
- **Principle 3:** If the identity of a principal is essential to the meaning of a message, it should be included in the message.
- **Principle 4:** Be clear about why encryption is being done. Encryption is not cheap and is not synonymous with security.
- **Principle 5:** When a principal signs a token that has already been encrypted, it should not be inferred that the principal knows the content of the message. Contrary to this, we can infer that the principal knows the content of the message when a principal signs a message and then encrypts it.
- **Principle 6:** Be clear about what properties you are assuming about nonces.
- **Principle 7:** If a predictable quantity (e.g., counter) is used, it should be protect to avoid attacks such as replay attacks.
- **Principle 8:** If timestamps are used, the differences between clocks at various entities must be much less than the allowable age of a message deemed to be valid.
- **Principle 9:** Recent use of a key does not guarantee to be enough fresh neither its security.



- **Principle 10:** The encoding mechanism has to be public and well-known.
- **Principle 11:** The protocol designer should know which trust relations her protocols depends on, and why the dependence is necessary.

Among them, appropriate consideration of Principle 3 can help to guarantee the integrity of the received message. On the other hand, it is well known that encryption by itself does not guarantee the integrity of the received message [7]. A good example of that could be One-Time-Pad (OTP), an encryption system with perfect security. In OTP if you change any bit of the output, a bit of the retrieved plain text will change, and the recipient has no way to detect this. As shown in previous sections, the four analyzed protocols miss the above mention considerations being susceptible to desynchronization attacks. Taking into consideration Principle 3, suggested by Abadi and Needham, could have avoided the problem. More precisely, describing the original protocols in general terms and assuming that two entities (A and B) share two keys (K_1 and K_{new}) the following message would be exchanged for the ownership transfer:

$$\begin{aligned} A &\rightarrow B : X = f_{K_1}(K_{new}) \\ B &: K_1 = K_{new} \end{aligned}$$

where f symbolizes an encryption function.

Nevertheless, the sending of X message neither guarantees its origin nor its integrity. Essentially, under this design assumption, the receiver would be forced to accept as valid all the messages received. This fault has been exploited in the proposed attacks.

Taking into account the considerations of Principle 3, the attacks could have been prevented by adding the sender signature at the end of the message in order to guarantee the source of the message and also provide the message integrity checking:

$$\begin{aligned} A &\rightarrow B : X = f_{K_1}(K_{new}) || Y = HMAC(K_1, K_{new}) \\ B &: K_1 = K_{new} \end{aligned}$$

where $HMAC$ symbolizes a Hash-based Message Authentication Code and $||$ represents the concatenation operation. When A sends this message, B can discover K_{new} , know that A signed the message and check the integrity of K_{new} . Assuming $HMAC$ complies with the RFC 2104 (i.e. $HMAC(K, text) = H(K \oplus opad, H(K \oplus ipad, text))$, where H and K denote a cryptographic hash function and a secret key respectively (please review [6] for more details), it means that B is certain that A knows K_{new} .

Summarizing, the attacks presented in this article can be prevented with minor changes in the initial designs. The design of a new cryptographic protocol is quite challenging and the designers should check its conformance with well-known principles of design – formal methods are also useful tools. These principles are neither necessary nor sufficient but are very helpful to prevent straightforward errors.

Remark 1: It must be noted that just using the message signature to fix the vulnerability of the analysed protocols

would not be enough. For instance, with only including signature of the message in the revised protocol, it would be possible to mount a desynchronization attack as described below:

- 1) When A sends to B message $X = f_{K_1}(K_{new}) || HMAC(K_1, K_{new})$, the adversary logs the message and blocks it.
- 2) Since the ownership transfer has not been finished successfully, A sends to B a new message $X' = f_{K_1}(K'_{new}) || HMAC(K_1, K'_{new})$.
- 3) Adversary intercepts the new message X' and replaces it by the logged message $X = f_{K_1}(K_{new}) || HMAC(K_1, K_{new})$.
- 4) B receives X and updates K_1 to K_{new} while A expects K'_{new} .

The same attack is applicable to the original version of KP, KZP and ZYP protocols. The complexity of this attack over these schemes is two protocol executions and the success probability is also almost 1. A solution could be keeping the new key fixed but randomizing sessions by nonces contributed by both protocol parties.

VII. CONCLUSION

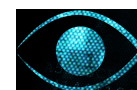
In this article we analyze the security of four protocols that have been recently proposed for RFID systems and whose authors claim to be secure against common RFID attacks – including expressly desynchronization attacks. Nevertheless, we show efficient desynchronization attacks against this range of schemes, having high success probability (~ 1) and negligible complexity (one protocol execution). As shown in Section VI, the authors missed well-know principles for designing cryptographic protocols. Therefore, new security protocols should be checked from an informal (using well-established principles and guidelines) and a formal perspective (e.g., BAN logic).

ACKNOWLEDGEMENTS

This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You).

REFERENCES

- [1] AES Calculator. <http://testprotect.com/appendix/AEScalc>.
- [2] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Trans. Softw. Eng.*, 22(1):6–15, Jan. 1996.
- [3] G. Kapoor and S. Piramuthu. Single RFID Tag Ownership Transfer Protocols. *IEEE Trans. on Sys., Man, and Cyber. PART C: Applications and Reviews*, 42(2):164–173, 2012.
- [4] G. Kapoor, W. Zhou, and S. Piramuthu. Multi-tag and multi-owner RFID ownership transfer in supply chains. *Decision Support Systems*, 52(2):258–270, 2011.
- [5] G. Khan and M. Moessner. Secure authentication protocol for rfid systems. In *20th International Conference on Computer Communications and Networks (ICCCN) 2011*, pages 1–7, 2011.
- [6] H. Krawczyk, M. Bellare, and R. Canetti. Network working group: RFC 2104. pages 1–12, 1997.
- [7] H. Shacham, D. Boneh, and E. Rescorla. Client-side caching for TLS. *ACM Trans. Inf. Syst. Secur.*, 7(4):553–575, 2004.
- [8] W. Zhou, E. J. Yoon, and S. Piramuthu. Simultaneous multi-level RFID tag ownership & transfer in health care environments. *Decision Support Systems*, doi:10.1016/j.dss.2012.04.006, 2012.
- [9] Y. Zuo. Changing hands together: a secure group ownership transfer protocol for RFID tags. pages 1–10, 2010.



EMPLOYING A SECURE CIPHER DOES NOT GUARANTEE THE SECURITY OF RFID PROTOCOLS

Masoumeh Saffkhani is Assistant Professor at Electrical Engineering Department, Shahid Rajaei Teacher Training University, Tehran, Iran. She is the author of 10 articles in cryptology. Her current research interests include RFID security.

Nasour Bagheri is Assistant Professor at Electrical Engineering Department, Shahid Rajaei Teacher Training University, Tehran, Iran. He is the author of over 50 articles in information security and cryptology.

Pedro Peris-Lopez is Visiting Lecturer in the Computer Security (COSEC) Lab at Universidad Carlos III de Madrid, Spain. He holds a M.Sc. in Telecommunications Engineering and a Ph.D. in Computer Science from Universidad Carlos III de Madrid. His research interests are in the design and analysis of cryptographic protocols and primitives and in lightweight cryptography. His current research is focused on Radio Frequency Identification Systems (RFID) and Implantable Medical Devices (IMD). In these fields he has published many papers over the last years in specialized journals and conference proceedings.

Juan E. Tapiador is Associate Professor of Computer Science in the Computer Security (COSEC) Lab at Universidad Carlos III de Madrid, Spain. Prior to joining UC3M, he was Research Associate at the University of York, UK. His work back there was funded by the ITA project (www.usukita.org), a joint effort between the UK Ministry of Defence and the US Army Research Lab led by IBM. His main research interests are in computer/network security and applied cryptography. He holds a M.Sc. (2000) and a Ph.D. (2004) in Computer Science from the University of Granada.



Cats and Dogs An Integrity for Voting Systems Based on Paper Ballots

İhsan H. Akin

Abstract—Voting systems based on paper ballots has a long history with various problems. Vote-selling and correct outcome are two major problems among many. In this work, we propose a new solution to these problems by using UltraViolet (UV) fiber paper Physical Unclonable Function (PUF). When applied this solution not only prevents vote-selling but also ensures the correctness of the outcome. With these two problems eliminated, the voting systems based on paper ballots will have complete integrity.

Index Terms—Paper ballot, Voting Integrity, Vote-selling, Paper PUF

mds
July 28, 2014

I. INTRODUCTION

VOTING plays a crucial role in the democracy, and it is a necessary part of it. Though there are various needs for voting, representative, presidential, and mayor elections are main voting reasons. They have a big impact on the future of a country. In the digitized age, although many e-voting systems are proposed, implemented, produced, and used [1]–[4], the tides are strongly back to voting system using the paper ballots [5], [6].

In this work, our attention is on the voting systems using paper ballots. The verifiability and correct outcome of the voting process are the two main requirements. In elections with little voters, these two requirements are easy to achieve. The voters can wait to the end of voting process and join/observe the counting process from the opening of the ballot box. When the number of voters are overwhelming, the election system may become quite complex, and may differ according to the country or the region. There are various groups involved in the voting process. When considering the integrity of the voting process, many groups such as; the officers, the tally, the parties (or the candidates), the Voting Management Center (VMC), and even the voters can be malicious.

Considering these malicious parties in the voting process, the integrity of the voting is a crucial problem. The ballot box rooms may be filled with malicious people to change the results. The votes can be easily changed during the counting process. In the case that the VMC collects all of the ballots after the local counting process, the undecided ballots are subject to modification. Another interesting case is the vote-selling, in which a voter agrees with a party to cast his ballot

as they required in exchange for money. This action, of course, requires a validation for the vote buying party of the casted vote.

In this work, we concentrate on these two problems, **vote-stealing (integrity)** and **vote-selling** of the voting system based on paper ballots. Our solution is based on the works of Bulens, Standaerty, and Quisquater [7]. They proposed to pour ultra-violet fibers into the paper mixture to create identities for papers. In our solution, we propose a highly controlled ballot distribution, where each party; the VMC, the political parties, and judges, calculates the identity of each ballot and agrees on the identities. Once the agreement is done for the required amount of ballots, the ballots with these identities are assigned and distributed among each ballot box, and these information is made publicly available on the cloud. Under these assumptions, the proposed solution prevents vote-stealing and provides the integrity, with high probability. The cost of successful malicious actions are extremely increased.

This paper consist of 6 sections. In Section II, we talk about the previous works on voting systems based on paper ballots. In Section III, we model a base voting system and discuss the integrity and vote-stealing problems over the model. In Section IV, the model is extended with the UV paper PUF, and honest judges. In Section V, the analysis of the proposed solution is performed. We conclude this work in the Section VI.

II. PREVIOUS WORKS

The problems with the US presidential elections in 2000 increased the awareness towards the problems of the current US voting system. The California Institute of Technology and the Massachusetts Institute of Technology set up a collaborative project to assess the magnitude of the problems of the voting processes, their main causes, and see how technology can scale them down [8]. As of today, 125 works has been listed on their site on various aspect of the voting systems. Jardí-Cedó et al. studied poll-site voting systems under a proposed framework [9]. Among the proposed solutions in the literature 4 of them are notable for us.

- 1) **Prêt à Voter** : is an end-to-end (e2e) verifiable Vote Verification System (VVS), introduced by Chaum et al. [10], Ryan et al. [11], and Ryan [12]. It uses a detachable ballot. The left side contains randomized list of candidates and the right side contains the selection and the encrypted information for the randomized list

İ. H. Akin is with Department of Computer Engineering, Fatih University, Istanbul, Turkey, e-mail: ihakin@fatih.edu.tr. This work is granted by TUBITAK-2219



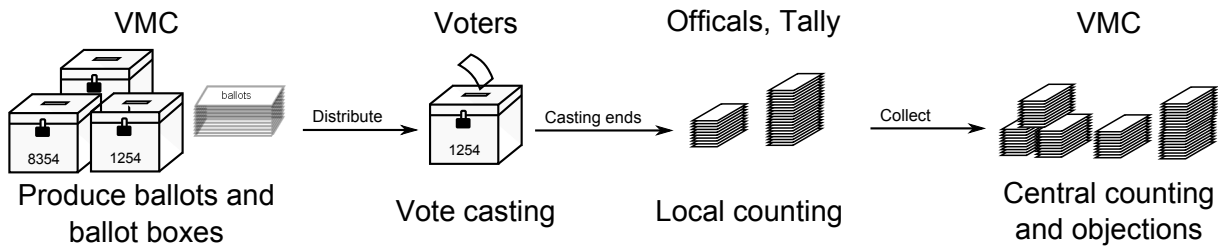


Fig. 1. The Base model for paper based voting process

of the candidates. The encryption is performed with with shared secret key. The voter marks his selection, detaches the left side, and takes a copy of the right side as a receipt before casting. This receipt may be stamped by the officials to become a proof. The voter can check his receipt at the public bulletin boards. Ryan extended this idea with Paillier encryption [13].

- 2) **Punchscan** : is also an e2e voting system, introduced by Fisher et al. [14]. Punchscan is designed to offer integrity, privacy, and transparency. Punch Scan's ballots has two pages to form two layers. In the ballots, the orders of the candidates are pseudo-randomly generated. The vote is marked by an ink dauber larger than the holes. The pages, when viewed alone, gives no information. One layer is destroyed and other layer is scanned and kept as receipt, and can be used to check at the public bulletin boards.
- 3) **Scantegrity-II** : is evolved from Scantegrity by Chaum et al. [15], [16]. It has permuted ballots not to have a connection between the ballot and the receipt. The ballots have unique identification. The verification based on special ink that reveals the verification code. The code, after some minutes, disappears. The ballot id and verification code can be used as an e2e verification.
- 4) **Scratch and Vote** : is developed by Adiada and Rivest [17]. In Scratch and Vote, an encrypted 2D-barcode stores the orders of the candidates. There is also a scratch surface that can be used to verify the orders of the candidates or that can be left it intact to cast as a vote. The left side of the vote must be destroyed as in Prêt à Voter and Punchscan.

All of the briefly described solutions above are e2e verifiable VVSs. Our proposed solution is not e2e verifiable, the voters cannot verify the ballots easily. The verification of the ballots is performed by the parties.

III. THE MODEL AND THE PROBLEMS

In this section, we model an election system based on paper ballots. In our model, local counting is valid and official; however the model is a centralized model and is very different form the other models.

A. The Base Model

In this work, the punching and stamping types are in consideration. In the punching type ballots are punched via

a machine, whereas in the stamping, ballots are stamped with an officially designed stamp. In our model, 6 different main groups, see Figure 1, are participating in the voting system;

- **Voting Management Center (VMC)**: The voting process and organization, the printing, the distribution of the ballots, and ballot boxes are managed by the VMC. For each ballot box, the voters are assigned so that each voter can only cast one vote in a pre-determined ballot box. The votes are counted locally at the end of the voting process in the ballot boxes' room where the ballot boxes reside. During the counting, observing is encouraged for the voters. After the counting, the ballot and the local results are collected by the VMC. In this system, the VMC is assumed **malicious**.
- **Political Parties (PP)**: PP's (or political individuals) are entering the election to acquire political power. The PP's are also assumed to be **malicious**. PP and their members, by any means possible, try to have advantage over the other PP's. They are allowed to observe any stage of the voting process.
- **Voters** : Voters are casting their vote in favor of the PP they supported. They are also considered as **malicious**. They can try to steal votes or purchase other voters' votes to favor the PP they are supported.
- **Officers** : The officers are assigned to the ballot boxes' rooms by the VMC to organize the casting and the counting stages of the voting process. They are also assumed to be **malicious**.
- **Tally** : Tallies are unofficial private observers of the counting process. They are also assumed to be **malicious**.
- **Judges**: Judges are **honest** party in the voting process. They have the final judgment in any conflict between parties.

B. The Two Problems

Integrity (Cats): In the base model, each party can act maliciously to gain advantage. Besides, a malicious PP, can **purchase** the officials, tally, voters, or the VMC. As a result, the PP can modify the results during the counting, collecting and post-election audit in favor of itself. A good example of such an action can be performed during an bogus electricity shortage [18], [19]

Vote-Selling (Dogs): A malicious party can print ballots and pre-stamp (or pre-punch) them for vote purchasing purposes.



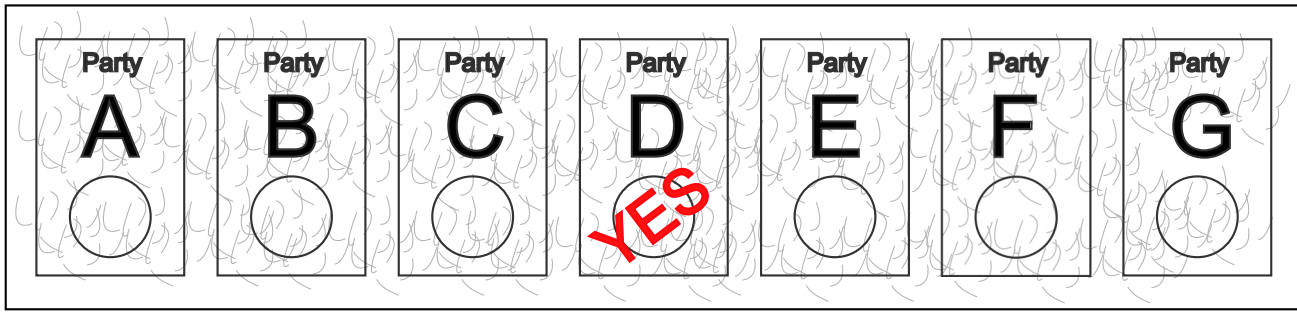


Fig. 2. An imprinted ballot with UV fiber paper PUF. The fibers are made visible for this figure.

The malicious party can purchase a vote from a voter simply by asking the voter to cast the pre-stamped ballot and bring an original ballot back to them.¹

In next section, we will talk about paper ballots which are designed by the UV fiber paper PUF. We will also talk about the new process. In the section following next section we look at provided integrity for the proposed voting system.

IV. INTEGRATED MODEL

In this section, we describe the suggested ballot and the voting process based on the UV fiber paper PUF ballot. The integrity of our voting system is based on the UV fiber paper PUF, which is suggested and analyzed by Bulens, Standaert, and Quisquater [7].

RowID	BallotID	BoxID	iSign
721	0x55E30731A7D	7361	0xB78431A
722	0xF57823D0845	9811	0x7561AA1
723	0xAD693CE13D3	2139	0x6DB821E

TABLE I: A ballot identification table

A. The Paper PUF Ballot

In their work, Bulens et al. used fuzzy extractors to build the identifiers of the UV fiber PUF papers. They have extracted 128-bit strings from the UV fiber PUF with a 96-bit entropy that provides 72-bit identifiers with applied ECC. Finding a collusion will require much effort for malicious actions. We will discuss this in our analysis. They also noted that more

¹A very similar scenario can be applied to receipt based digital ballots.

randomness, robustness, and unclonability can be achieved with the same technology with an additional cost.

In our integrated model, the ballot is formed with the UV fiber PUF technique. We do not consider putting a signature into the ballots like Bulens et al. proposed. See the next section for the details.

B. The Voting Process

Our voting system consists of 7 main steps: the ballot formation; the identification of the ballots by the PPs, VMC, and the judges where they must reach a consensus; the distribution of the ballots; the casting of the ballots by the voters; the local counting in the ballot box rooms; the collection of the results and the ballots by the VMC; and the investigation if necessary.

- **The Ballot Formation :** The ballot papers are mixed with the UV fiber during the paper preparation process, see Figure 3. The papers are printed and cut to form the ballots. The order of the candidate PPs in the ballots are randomly arranged.
- **The Ballot Identification and the Consensus:** In the identification step, the VMC, the PPs, and the judges (in short we call all of them as identifiers) have different but open source and public system to identify the ballots. They extract the features, identify the ballots and have a consensus on each paper ballot. Once the identifiers have a consensus on a ballot, it is assigned to a ballot box by the VMC. With this assignment, the identifiers insert the ballot's information into a cloud database. Each of the identifiers has a unique table, and public and private keys. They sign their tables

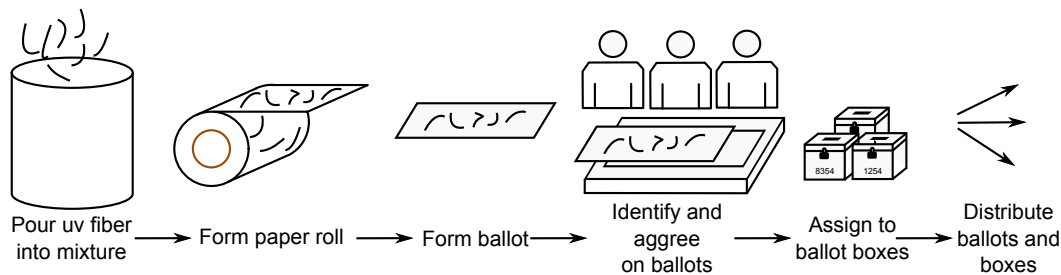


Fig. 3. Ballot preparation and distribution process

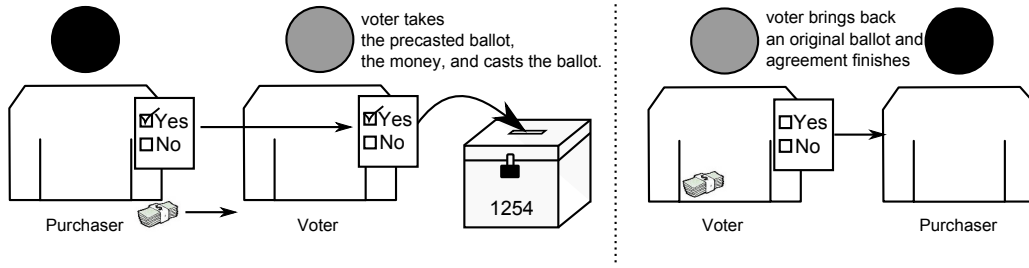


Fig. 4. An example of Dogs action. Left side is before casting and the right side after the vote casted

by their private keys, and integrate the tables, see Table I.

In Table I, the iSign column that stores the incremental signature is a simplified approach of Narasimha et al. [20]. The signature can be calculated as

$$iSign_{row_i} = Sign_{SK}(RowID \parallel BallotID \parallel BoxID \parallel iSign_{i-1}),$$

where $i = 2, \dots, n$, $iSign_0 = 0$, and SK is the secret key of the identifiers. The last iSigns are published at the web site with the public keys. The judges keep a copy of the last signatures of each table. The database administrator on the cloud can be malicious, and his malicious actions can be easily detected by the provided signatures.

- **The Ballot distribution :** The distribution of the ballots can be performed by the traditional ways. The only concern is that the ballots must be secured against tampering so that the voting takes place as planned.
- **The Vote casting :** In the casting stage, the voters cast their votes by stamping or punching. In the punching case, the punching area must be outside of the identification region of the ballots. In our system, the voters don't have an e2e verification for their votes; however, they can join the local counting process as observers. At the end of the vote casting, the unused ballots must be stamped with a "not casted" stamp in the presence of the observers.
- **The Local counting :** In the local counting stage, the ballot boxes' seals are opened, and the officers and the tallies count the casted votes in the presence of the observers.
- **The Collection of the Results:** In this stage, the counted results are sent back to the VMC with the ballots. The result of each ballot box is publicly announced.
- **The Investigation :** This stage can be on demand or required. If it is on demand and the voters or the PPs are not satisfied with the counted results of the ballot boxes, they can require investigation. In this process, the ballots in the ballot boxes that are under investigation are re-identified and compared to the old identifications. More discussion on this topic is in the next section.

V. THE INTEGRITY OF THE VOTING SYSTEM

In this section, with some games, we analyze what kind of integrity our voting system is providing. We deeply look at the actions of the cats and the dogs on our system. Also, we discuss the success probabilities of these actions.

Game 1 : The Dogs: Single Vote-Purchasing

- A dog approaches a voter outside the ballot box room before the voter casts his vote.
- The dog offers some money to the voter to cast a pre-stamped ballot and return an original ballot from the ballot box room.
- The voter agrees, takes the money, inserts the pre-stamped ballot into his pocket, goes to the casting room, takes an original one, inserts it into his pocket, and casts the pre-stamped ballot.
- He returns back to the dog, gives the original ballot, and the agreement finishes.
- The output of Game 1 is a success, if this malicious action is not revealed in the investigation step. Otherwise, the output is a failure.

To calculate the successfulness of Game 1, we assume that each ballot have 70-bit identification, i.e. there are 2^{70} different paper ballots that can be created. As noted by Bulens et al. identification space can be increased on demand. We, however, continue our analyze on 70-bit identification. Also, we assume that each ballot box contains exactly 2^{10} assigned voters, and there are 2^{20} ballot boxes. To be successful in Game 1, the malicious party must produce at least 1 ballot with the same identity as the ballots for the targeted ballot box, B_1 .

The probability that a ballot produced by the malicious party is in the set of real ballots for B_1 is given by;

$$Pr(\text{Game 1} = \text{Success}) = \frac{2^{10}}{2^{70}} = \frac{1}{2^{60}} \quad (1)$$

The malicious party must spend a lot of time and money to prepare an original ballot. Even if they are successful in producing a valid ballot for the target B_1 , there are two problems. First, the voters cannot identify the ballots. Second, they cannot get any ballot as they wanted. As a result, for a success in Game 1, there is an additional $\frac{1}{2^{10}}$ probability, which makes the probability for Game 1 to be successful $\frac{1}{2^{70}}$.

In the next game, the dogs try to purchase all of the ballots for a specific ballot box, B_2 .

Game 2 : The Dogs: Whole Ballot Box Vote-Purchasing

- **Step 1:** A **dog** approaches a voter outside the ballot box room before a voter casts his vote.
- The **dog** offers some money to the voter to cast a pre-stamped ballot and return an original ballot from the ballot box room.
- The voter agrees, takes the money, inserts the pre-stamped ballot into his pocket, goes to the casting room, takes an original one, inserts it into his pocket, and casts the pre-stamped ballot.
- He returns back to the **dog**, gives the original ballot, and the agreement finishes.
- Return to the Step 1, until all the voters' votes are purchased.
- The output of Game 2 is a success, if this malicious action is not revealed in the investigation step. Otherwise, the output is a failure.

The probability of successfully producing 2^{10} ballots that match the ballots for the ballot box B_2 can be given by;

$$Pr(\text{Game 2} = \text{Success}) = \frac{(2^{10})!}{(2^{70})^{2^{10}}} \approx \frac{1}{2^{62914}}, \quad (2)$$

as seen from the Equation 2, producing 2^{10} ballots with matching identity is very improbable. Also, note that the votes that are not casted can be a huge problem for the **dogs**. For simplicity, we assumed that all of the votes are casted. Even a single voter, who has not casted his vote, can create an additional problem for the **dogs**.

Game 3 : The Cats: Whole Vote-Stealing from a Ballot Box

- Immediately after a ballot box's seal is just opened, a **cat** performs a magical operation ².
- During this magical operation, the **cat** changes the casted ballots with the pre-stamped ballots.
- Output of Game 3 is success, if in the investigation step, this malicious action is not revealed. Otherwise the output is failure.

Assuming that every voter casted their vote, the success probability of Game 3 is equal to Game 2. If there are some voters that have not casted their votes, the success probability success is much less than Game 2.

In the investigation step, even in the case that the malicious action is successful, there is another approach to identify a malicious action; the **fingerprints and DNA** [21], [22]. The ballots, in total, at least must contain 2^{10} different fingerprints. Actually, the fingerprints on the ballots can help to identify the voter's selection! Recently, governments have started to take fingerprints of the citizens and the aliens in their country. Malicious groups within governments can use this database to identify the selection of the voters. Actually, this is a common problem for every paper based voting systems [11], [17], [23].

The next game is a very realistic malicious action on the paper ballots. During the local counting of the ballots, some of the votes are discarded due to bad stamping (or punching). Due to very close results, some parties request re-counting for some ballot boxes at the VMC and, occasionally, the results

change after re-counting. By using this knowledge, the **cats** can play on these **badly** casted votes.

Game 4 : The Cats: Single Vote-Stealing

- A malicious party A request a new counting from the VMC for a ballot box.
- The VMC accepts this request and announce the date of the counting.
- Before the counting date, the **cats** look at the votes and notice a discarded vote.
- The **cat** replaces this ballot with a new one.
- Output of the game is success, if in the investigation step, this malicious action is not revealed. Otherwise the output is failure.

The successfulness of Game 4, same as Game 1. The **cats**, however, may be able to identify the ballot's PUF. With this, they have only $\frac{1}{2^{60}}$ probability to construct a valid ballot. This game can also be played for as many times as there are badly stamped ballots.

In the next game, although it is not realistic, we will look at the probability that a malicious party somehow steals all the casted votes before counting. For simplicity, we assume that all the votes are casted.

Game 4 : The Cats: Whole Vote-Stealing

- Just before the counting process after the ballot boxes are opened, the **cats** perform magical operations.
- During this magical operation, the **cats** changes the casted ballots with pre-stamped ballots.
- Output success if in the investigation step, this malicious action is not revealed, else output failure.

The probability of successfully producing 2^{30} ballots can be given by;

$$Pr(\text{Game 4} = \text{Success}) = \frac{(2^{30})!}{(2^{70})^{2^{30}}} \approx \frac{1}{2^{62914}}, \quad (3)$$

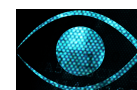
VI. CONCLUSION

In this work, we have approached the integrity and vote-selling problems of paper based voting systems by deploying paper PUF constructed with UV fibers. Our proposed solution requires only a group of honest judges. The remaining parties can be malicious. The integrity and vote-selling problems can be solved with a high probability. The cost of malicious action within the voting process becomes very improbable for any malicious party. With the increase of the identification space, the proposed solution will provide have better security.

REFERENCES

- [1] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. *IACR Cryptology ePrint Archive*, 2002:165, 2002.
- [2] Premier/Diebold (Dominion) AccuVote TS and TSx. <https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/>, 2014. [Online; accessed 17-July-2014].
- [3] Rop Gonggrijp and Willem-Jan Hengeveld. Studying the nedap/groenendaal es3b voting computer: A computer security perspective. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, EVT'07, pages 1–1, Berkeley, CA, USA, 2007. USENIX Association.
- [4] Ferguson, Louise. *UPA Voting and Usability Project*. UPA, United States, 2004-04-19.

²Malicious ballot box room or performing during bogus electricity shortage.



- [5] Scott Neumann. Norway Does A Ctrl+Alt+Delete On E-Voting Experiment. <http://www.npr.org/blogs/thetwo-way/2014/06/27/326221089/norway-does-a-ctrl-alt-delete-on-e-voting-experiment>, 2014. [Online; accessed 17-July-2014].
- [6] Michael Alvarez, Jonathan N. Katz, Charles Stewart III, Ronald L. Rivest, Stephen Ansolabehere, and Thad E. Hall. Voting: What Has Changed, What Hasn't, & What Needs Improvement. <http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement>, 2012. [Online; accessed 17-July-2014].
- [7] Philippe Bulens, François-Xavier Standaert, and Jean-Jacques Quisquater. How to strongly link data and its medium: the paper case. *IET Information Security*, 4(3):125–136, 2010.
- [8] Voting - What Is, What Could Be. <http://vote.caltech.edu/content/voting-what-what-could-be>, 2014. [Online; accessed 17-July-2014].
- [9] Roger Jardí-Cedó, Jordi Pujol Ahulló, Jordi Castellà-Roca, and Alexandre Viejo. Study on poll-site voting and verification systems. *Computers & Security*, 31(8):989–1010, 2012.
- [10] Chaum, Ryan, and Schneider. A practical voter-verifiable election scheme. In *ESORICS: European Symposium on Research in Computer Security*. LNCS, Springer-Verlag, 2005.
- [11] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.
- [12] Peter Y. A. Ryan. A variant of the chaum voter-verifiable scheme. pages 81–88. ACM, 2005.
- [13] Peter Y. A. Ryan. Prêt à voter with paillier encryption. *Mathematical and Computer Modelling*, 48(9-10):1646–1662, 2008.
- [14] Sherman AT Fisher K, Carback R. Punchscan: Introduction and system definition of a high-integrity election system. In *Proceedings of the Workshop on Trustworthy Elections 2006*, pages 1–8. Springer, 2006.
- [15] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In David L. Dill and Tadayoshi Kohno, editors, *2008 USENIX/ACCURATE Electronic Voting Workshop, July 28-29, 2008, San Jose, CA, USA, Proceedings*. USENIX Association, 2008.
- [16] Stefan Popoveniuc, Jeremy Clark, Richard Carback, Aleksander Essex, and David Chaum. Securing optical-scan voting. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Mirosław Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*, pages 357–369. Springer, 2010.
- [17] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *WPES*, pages 29–40. ACM, 2006.
- [18] Hileli Yerel Seçim 2014 Belgeleri ve Fotoğrafları. <http://hilelisecim2014.tumblr.com/>, 2014. [Online; accessed 17-July-2014].
- [19] CHP ve MHP'den Seçimde Hile Yapıldı İddiası. <http://www.bianet.org/bianet/siyaset/113469-chp-ve-mhp-den-secimde-hile-yapildi-iddiasi>, 2014. [Online; accessed 17-July-2014].
- [20] Maithili Narasimha and Gene Tsudik. DSAC: An approach to ensure integrity of outsourced databases using signature aggregation and chaining. *IACR Cryptology ePrint Archive*, 2005:297, 2005.
- [21] Paul-Jean Coulier. Les vapeurs diode employes comme moyen de reconnaître l'altération des écritures (iodine vapors used as a means of recognizing the alteration of writing. *L'anne scientifique et industrielle*, 8:157–160, 1863.
- [22] M.Kinga Balogh, Joachim Burger, Klaus Bender, eter M Schneider, and Kurt W Alta. Str genotyping and mtdna sequencing of latent fingerprint on paper. *Forensic Science International*, 137(2-3):188–195, 2003.
- [23] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46, May/June 2008.



Siber Güvenlik Ekonomisi Üzerine Literatür İncelemesi

H. Şentürk, C.Z. Çil ve Ş. Sağıroğlu

Özet— Teknolojik karmaşıklığı ve yol açtığı ekonomik zararları gün geçtikçe artan siber saldırılar ile çok sayıda siber güvenlik teknolojilerinin yatırım opsiyonu olarak bulunduğu güvenlik sektörü, siber güvenliğin ekonomik boyutu üzerine düşünmeyi gerekli kılmaktadır. Bu çalışmada; siber güvenliğin ekonomik boyutu alanında son onbeş yılda yapılan akademik çalışmalar incelenmiş, literatürdeki boşluklar ortaya konularak sonraki araştırmalara yön verilmesi amaçlanmıştır.

Anahtar Kelimeler—Siber güvenlik ekonomisi, güvenlik yatırımı, güvenlik yatırımının geri dönüşü.

Abstract— The technological complexity and increasing losses incurred by the cyber attacks as well as booming cyber security sector offering variety of tools as investment options necessitate consideration of cyber security economics. This study evaluates the academic literature on cyber security economics for the last fifteen years and aims to provide research directions by pinpointing literature gaps.

Keywords—Cyber security economy, security investment, return on security investment.

I. GİRİŞ

GÜNÜMÜZ teknolojisinin getirdiği ve IEEE standardı olan “nesnelerin interneti-internet of things” ve “her şeyin interneti- Internet of Everything” konseptleri, başta bilgisayarlar ve akıllı telefonlar olmak üzere mutfağımızdaki bulaşık makinesinden arabaya, evdeki klimadan saksıya kadar etrafımızdaki hemen her şeyin internet üzerinden birbirine bağlantısını öngörmektedir. Diğer taraftan 1990'lu yılların basit virüs yazılımlarıyla başlayan siber saldırıların, günümüzde hedef odaklı gelişmiş saldırılar da denilen APT (Advanced Persistent Threat) örneğinde görüldüğü gibi karmaşıklığını ve ekonomik etkisini artırdığı bilinmektedir. Bu durumun getirdiği en büyük zorluk, bu altyapının güvenliğinin sağlanması, bunun ekonomik yansıması ise güvenlik için gerekli optimum yatırım maliyetlerinin belirlenmesi ihtiyacıdır. Bu amaçtan yola çıkarak, bu çalışmada siber

güvenliğin ekonomik boyutu üzerine alanda yapılan akademik çalışmalar incelenmiştir.

Siber güvenliğin ekonomik boyutunun büyüklüğünü açıklayıcı olması açısından birkaç örnek vermek yerinde olacaktır.

Code Red solucan yazılımı, Temmuz 2001'de ilk ortaya çıktığında kendini her 37 dakikada çoğaltarak toplamda 2 milyar ABD doları zarara yol açmıştır. Ağustos 2003'te çıkan Blaster solucanı ise ilk haftasında yarım milyon bilgisayara bulaşmış, işletme başına 475 bin dolar maddi kayıp verdiği açıklanmıştır [1].

I Love You ve Love Bug virüslerinin, dünya çapında 10 milyar dolar, My Doom isimli truva atının 4.8 milyar dolar, Nimda solucan yazılımının ise yaklaşık 3 milyar dolar maddi zarara yol açtığı tahmin edilmektedir [2].

2005 yılında Bilgisayar Güvenliği Enstitüsü (CSI) tarafından yapılan araştırmada, katılan 639 işletmenin 2005 yılı için sızmalardan kaynaklanan maddi kaybının 130 milyon dolar olduğu açıklanmıştır [3].

2010 yılında Symantec ve Ponemon Enstitüsü tarafından hazırlanan ve 15 farklı sektörden 51 farklı firmanın katıldığı sızma maliyetleri raporunda firmaların 2010 yılı yıllık ortalama kayıp tutarının 7,24 milyon dolar olduğu rapor edilmiştir [4].

HP Ponemon Enstitüsü tarafından 2012 yılında yapılan çalışmada ise, son üç yılda haftalık başarılı siber saldırı sayısı ortalamasının 50'den 102'ye çıktığı, ortalama saldırılardan kurtarma süresinin 14'den 24 güne çıktığı, yıllık ortalama kayıp maliyetinin ise 6,5 milyondan 8,9 milyon dolara çıktığı belirtilmiştir [5].

Yukarıda belirtilen sayılardan da görüleceği üzere, siber güvenliği elektronik ve bilgisayar bilimi yanında ekonomik açıdan da ele almak gerekmektedir. Hâlihazırda bu alandaki mevcut çalışmalar yetersiz kalmaktadır [6]. Bu çalışmanın amacı; siber güvenliğin ekonomik boyutu alanında son on beş yılda dünyada yapılan akademik çalışmaların incelenmesi ve siber güvenlik ekonomisi alanında yüksek lisans ve doktora seviyesinde araştırma yapılabilecek konulara dikkat çekilmesidir.

Manuscript received by 30 July 2014

Bilg.Y.Müh. Hakan ŞENTÜRK, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara. (Tlf: 312-414-2631; e-mail: hsenturk@hvkk.tsk.tr).

Prof.Dr. Celal Zaim ÇİL, Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği, Ankara (e-mail: czaimcil@cankaya.edu.tr).

Prof.Dr. Şeref SAĞIROĞLU, Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara (e-mail: ss@gazi.edu.tr)



II. ALANA GENEL BAKIŞ

Siber güvenlik ekonomisi alanında yapılan çalışmalar, temel olarak aşağıdaki üç konuyu ele almaktadır [7]:

- Güvenlik saldırılarının/sızmaların gerçekleşme sıklığı: Saldırıların sıklığını oluşturan göstergelerin belirlenmesi.
- Güvenlik saldırılarının/sızmaların maliyeti: Bir saldırının maliyetinin tahmin edilebilmesine yönelik problemin çözümü.
- Siber güvenlik teknolojilerine yapılan yatırımlar: Belirlenen güvenlik sistemlerinin tedarik edilmesi, kurulumu, bakım ve idamesi ile kullanılmasına yönelik harcama düzeyinin belirlenmesi.

Benzer şekilde Su, siber güvenlik ekonomisi alanındaki mevcut literatür çalışmalarını aşağıdaki üç kategoride toplamıştır [3]:

- Güvenlik saldırılarının maliyet ve etkilerinin ölçülmesi
- Güvenlik teknolojilerinin fayda ve etkilerinin ölçülmesi
- Güvenlik yatırımlarının optimum seviyesinin belirlenmesi.

Bu çalışmada, yukarıda belirtilen üç kategoride Su'nun çalışmasından sonra yapılmış güncel akademik çalışmalara ilave olarak siber güvenliğin bir risk yönetimi disiplini olduğu düşüncesinden [8] yola çıkarak, "güvenlik risklerinin belirlenmesi ve ölçülmesi" konusundaki akademik çalışmalarının durumu da dâhil olmak üzere toplam dört temel alanda inceleme yapılmıştır.

III. RİSKLERİN BELİRLENMESİ VE ÖLÇÜLMESİ

İşletmelerin güvenlik risklerinin belirlenerek ölçülmesi amacıyla farklı kalitatif ve kantitatif teknikler kullanılmaktadır.

Kalitatif tekniklerden en yaygınları, ileriki bölümde açıklanacak olan Yıllık Kayıp Beklentisi metriği, Courtney, Livermore Risk Analizi Metodolojisi (LRAM), Stokastik Baskınlık teknikleridir [9]. Bu tekniklerin güçlü yanı işletmelere zafiyet altında olan varlıklarını ve değerlerini belirlemeye ve bu varlıkları korumak için gerekli olan tedbirleri almaya zorlamasıdır. Zayıf yanı ise bu değerlerin hesaplanmasındaki fazla zaman, işgücü alması vb. zorluklar ve belirsizliklerdir [6].

Risk analizinde kullanılan kantitatif teknikler ise, senaryo analizi, beyin fırtınası, hata ağacı analizi, bulanık metrikler ve uzman görüşlerine başvuru görüşme ve anket yöntemleridir [6,10]. Bu yöntemlerin zayıf yanı uzman personelinin öznel görüşlerinden faydalanılarak belirlenen risklerin genellikle düşük, orta, yüksek vb. sayısal olmayan değerlendirmeler içermesidir.

Belirlenen risklerin sayısallaştırılması amacıyla kullanılan teknikler Tablo 1.de gösterilmiştir:

TABLO 1.
RİSK SAYISALLAŞTIRMA TEKNİKLERİ [11].

Süreç Yaklaşımı	Faktör Yaklaşımı	Aktüeryal Yaklaşım
Sebeep-Sonuç	Risk göstergeleri	Ampirik kayıp dağılımları
Bayesian İnanç Ağları		
Bulanık Mantık	Sermaye Varlık	Geçmiş veri tabanı
İstatistik Kalite Kontrol ve Güvenilirlik Analizi	fiyatlandırma modeli (Capital Asset Pricing model –CAPM)	bilgileri kullanılan parametrik dağılımlar
Bağılantı	Tahminsel modeller	Aşırı-Değer Teorisi
Sistem Dinamikleri		

Siber güvenlik risk yönetimi, bilgi varlıklarının bütünlük, gizlilik ve erişilebilirlik niteliklerini tehdit eden risklerin gerçekleşme olasılığının ortadan kaldırılması veya azaltılması sürecidir. Bu süreç, seçeneklerin belirlenmesi, seçilmesi ve uygulaması olmak üzere üç adımdan oluşur. Her bir bilgi varlığına yönelik riskin ölçülmesinden sonra kabullenmek, riski transfer etmek, indirgemek ve önlemek alternatifleri arasından biri seçilerek uygulanır. Gerçekleşme olasılığı ve ekonomik değeri düşük bilgi varlığı riskleri için riskin kabullenilmesi seçilebileceği gibi, bazı durumlarda riskin transferi, diğer bir deyişle, işletme dışında bir unsurla paylaşılması (örneğin siber güvenlik sigortası yaptırmak) söz konusu olabilir.

ABD'de 2008'e kadar olan son on yıllık dönemde siber güvenlik sigortalıların yıllık prim ödemeleri 450-500 milyon ABD dolarını bulmuştur [12]. Riskin transferi amacıyla siber güvenlik sigortası kullanılmasının, hem akademisyenler hem de uygulayıcılar tarafından önerildiği, sigorta primlerinin hesaplanabilmesine yönelik ise farklı yaklaşımlar tavsiye edildiği görülmektedir [11,13,14,15].

Herath ve diğerleri, Tablo 1.de görülen aktüeryal bir yaklaşım ile copula tabanlı bir siber sigorta risk modeli ve fiyatlandırması yöntemi önermişlerdir [13]. Geçmiş yılların virüs maliyetleri kullanılarak oluşturulan modelin zayıf tarafı, yazarlarca da belirtildiği üzere, istatistikî olarak geçmiş saldırı ve maliyet bilgilerinin kullanılmasına olan bağlılıktır ki, bu tür bilgilerin bulunmasındaki zorluklar pek çok çalışmada dile getirilmiştir [13,16,27,55].

Bandyopadhyay, doktora tezinde siber güvenlik risklerinin indirgeme ve transferi amacıyla siber sigorta kullanımını incelemiş, sonraki çalışmalar için ampirik analizlerin yapılmasını önermiştir [17].

Siber güvenlik yatırımlarının getireceği risklerin indirgenmesine bağlı olan fayda, aslında bir yetkisiz sızma durumunda beklenen kaybın azaltılması olacaktır. Dolayısıyla, bu tür bir yatırım, işletmeye doğrudan bir kar getirmeyecek, ancak bir yetkisiz sızmanın gerçekleşmesi durumunda olabilecek maddi kaybın azaltılmasını sağlayacaktır. Bu nedenle, yatırımın değerlendirilmesindeki ölçüt, uygulanacak



SİBER GÜVENLİK EKONOMİSİ ÜZERİNE LİTERATÜR İNCELEMESİ

sistem çözümünün maliyetine ek olarak, işletmeye sağlayacağı beklenen maddi kaybın azaltılması yönündeki marjinal fayda olacaktır [7].

Doktora tezinde Jourdan, bilgi güvenliği uzmanlarıyla yaptığı görüşmelerden faydalanarak bilgi güvenliği risk analizi süreçlerini incelemiş, sonuç olarak risk analiz süreçlerinin dinamiklerini daha iyi anlamak ve uygulamalarını iyileştirmek yönündeki akademik çalışmaların devamını önermiştir [10].

Claunch ve McMillan, son yıllarda siber saldırılardan kaynaklanan kayıp maliyetlerinin, tıp sektörü için 2010-2011 döneminde %10 olan genel sektör ortalamasının %32 oranında artış gösterdiği istatistiğine dikkat çekerek, Wyoming Tıp Merkezi'nde gerçekleştirdikleri vaka çalışmasında işletmenin tüm varlıklarını kapsayan bir risk analizi yaklaşımıyla, ilgili tıp merkezinin optimum siber güvenlik yatırımıyla, güvenlik seviyesini önemli derecede artırabildiğini belirtmiştir [18].

IV. GÜVENLİK SALDIRILARININ MALİYET VE ETKİLERİNİN ÖLÇÜLMESİ

Güvenlik saldırılarının işletmeye olan maliyet ve etkileri finansal, operasyonel, müşteriler ve çalışanlar ile ilgili somut ya da soyut etkilere yönelik doğrudan dolaylı ya da fırsat maliyetlerini kapsamaktadır [3,19,20].

Risklerin ölçülmesinde bulunan problemler gibi, güvenlik saldırılarına ilişkin, rakamlarla ifade edilemeyen etkilerin belirlenmesi genellikle öznel değerlendirmelerle yapılabilmekte ancak bunların rakamsal değerlere dönüştürülmesinde problemler yaşanmaktadır [21]. Dolaylı maliyetlerin belirlenmesine yönelik çalışmalar, genellikle saldırı açıklanma bilgileri ile hisse senedi değerleri arasındaki ilişkilerin incelemesi üzerine olmaktadır.

Çavuşoğlu ve diğerleri, pazar değerlendirme tabanlı bir yaklaşımla, sızmaya maruz kalan işletmelerin piyasa değerinin açıklanmasının ilk iki günü içinde ortalama % 2.1 kayba uğradığı, buna paralel olarak da bilgi güvenliği firmalarının ise aynı dönemde ortalama % 1.36 değer kazandığını gözlemlemişlerdir [22].

Hovav ve D'Arcy, virüs ve hizmet dışı bırakma saldırılarına maruz kalan işletmelerin hisse senetlerinin borsadaki durumunu incelemiş, olayların açıklanmasının ardından bahse konu işletmelerin borsa senetlerinin değer kaybına uğradığını gözlemlemişlerdir [2,23]. Ayrıca, saldırıların türüne göre etkilerin de farklı olduğu görülmektedir. Campbell ve diğerleri, yaptıkları ampirik çalışmada, halka açıklanan sızmalardan gizli bilginin ifşası söz konusu olanların, işletmenin piyasa değerine negatif etkisini tespit ederken, yine halka açıklanan ancak gizli bilginin ifşa edilmediği sızmalara borsanın ve piyasanın aynı negatif etkiyi vermediğini gözlemlemişlerdir [24].

Telang ve Wattal, yazılım sektöründe faaliyet gösteren üretici şirketler üzerine yaptığı çalışmada, yazılım zafiyetlerine ilişkin haberlerin medyada çıktığı gün, şirketlerin piyasa değerlerinin %0.63 düştüğünü, yazılım zafiyetinin türüne göre etkinin de farklı olduğunu tespit etmişlerdir [25].

Wang, üç makaleden oluşan doktora tezinde, medyada çıkan sızma haberleriyle işletmelerin hisse senedi değerleri arasındaki ilişkiyi incelemiş, Campbell'ın çalışmasının sonuçlarıyla uyumlu olarak genel saldırı ve sızma haberlerinin farklı etkilere yol açtığı, ancak gizli bilgi ihtiva eden spesifik sızma haberlerinin piyasada firmanın gelecekteki başarısı üzerinde daha negatif etkiye yol açtığını tespit etmiştir. [26].

Literatürdeki pek çok çalışmanın özellikle ABD'de düzenli olarak yapılmakta olan ve çeşitli sektörlerden çok sayıda işletmenin katıldığı veri toplama çalışma sonuçlarından faydalandığı görülmüştür. Gerçekleşen sızmaların kayıp maliyetlerine yönelik istatistikî veri sağlayan bu tür çalışmaların en yaygın örnekleri, CSI/FBI, Ponemon Enstitüleri ile Verizon'un yıllık raporlarıdır.

İşletmelerin genel eğilimi, kötü reklâm olabileceği, sektördeki konumuna zarar verebileceği düşüncesiyle maruz kaldıkları siber güvenlik saldırıları ve beraberinde gerçekleşen kayıplara ilişkin bilgileri paylaşmama yönündedir. Hatta işletmelerin, olası saldırılar sonucu oluşan veri kayıplarında, müşteriler tarafından açılan davalarda işletme aleyhinde delil olarak başvurulabileceği gerekçesiyle istatistik kayıt tutmayabildikleri bilinmektedir [27].

Conrad, zafiyetler, sızma sıklığı, kayıp maliyet tahminleri gibi güvenlik modeli parametreleri kapsamına belirsizliği de katabilmek için Monte Carlo simülasyonu yöntemini kullanmıştır [3,28].

Soo Hoo, sızma olaylarının sıklığı ve sonuçların etkilerinin sağlıklı şekilde ölçülmesi amacıyla sonraki çalışmalar için;

- Risk yönetimi faaliyetini destekleyici bilgi güvenliği istatistiklerinin toplanmasına yönelik metrik ve araçların geliştirilmesi,
- Saldırı paternlerinin ve saldırganların davranışlarının gözlemlenmesi amacıyla bilgisayar ağlarının simüle edildiği yazılım araçlarının geliştirilmesi gerektiğini önermiştir [27].

V. GÜVENLİK TEKNOLOJİLERİNİN ETKİNLİĞİNİN ÖLÇÜLMESİ

Normal şartlarda, güvenlik teknolojilerinin fayda ve etkinliği, fayda-maliyet analizi ile ölçülebilir. Faydaları, korudukları bilgi varlıklarının değerleri ve indirgedikleri riskin derecesi ile, maliyetleri ise yazılım/teçhizatın tedarik maliyeti, kurulum, eğitim ve bakım-idame maliyetleri ile ölçülebilir. Ancak, seçilen güvenlik teknolojilerinin etkinliğinin ölçülmesi



konusunda problemler mevcuttur [20]. Kullanılan güvenlik teknolojilerini etkinlikleri açısından birbirleriyle kıyaslamak için mevcut formal bir metodoloji de bulunmamaktadır. Zorluklar, saldırgan profilinin ve işletmenin güvenlik politikasına uyum durumunun tahmin edilmesindeki belirsizliklerin ölçülememesinden kaynaklanmaktadır [3].

Güvenlik teknolojilerinin etkinliği, o teknolojinin ilgili riski ne kadar azaltmakta olduğunun değerlendirilmesi ile ölçülür [3,27]. Riskin azaltılması ise, riskin tamamen önlenmesi veya gerçekleşme olasılığının azaltılmasıdır. Güvenlik teknolojilerinin etkinliğinin değerlendirilmesinde, mevcut olması durumunda test ortamlarında gerçekleştirilen ürün deneme çalışma sonuçları ve geçmişte gerçekleşen olaylara ait istatistikî veriler kullanılabilir, bu tür tarihi verinin mevcut olmaması durumunda ise güvenlik teknolojilerinin etkinliğinin tahmin edilmesi için uzman görüşlerinden, işletmenin bilgi güvenliği uzman personelinden faydalanılabilir. Butler, uzman görüşlerinin varsayım ve tahminlerinin, alınan kararlara ne kadar duyarlı olduğunun belirlenebilmesi için duyarlılık analizi yapılmasının doğru yaklaşım olduğunu belirtmiştir [29].

Diğer bir konu ise, birden fazla güvenlik teknolojisinin kullanılması durumundaki etkileşimin ölçülmesidir. Belirlenen risk için kullanılacak birden fazla teknolojinin riski ne kadar azaltacağı, toplam faydanın, ilgili teknolojinin tek tek kullanıldığında alınacak faydadan büyük olup olmayacağı konularının da incelenmesi gerekmektedir [3,29].

Yatırım yapılan güvenlik teknolojileri kullanılarak oluşturulan güvenlik sistemi altyapısının teknik açıdan etkinliğinin değerlendirilmesi amacıyla ise zafiyet tarama, sızma testleri vb. amaçlı çok sayıda ürün rafta hazır şekilde bulunmaktadır. Ayrıca bu amaçla işletmeler, gerek iç denetimler gerekse de dış kaynak kullanımıyla danışman şirketlerin denetlemesi yöntemine de başvurmaktadırlar ancak bu yaklaşım sistemin geneline ilişkin değerlendirme olup, siber güvenlik teknolojilerinin bireysel olarak değerlendirilmesi konusunda yardımcı olamamaktadırlar.

Gordon ve diğerleri, siber güvenlik denetimlerinin arttığına işaret ederek, denetimlerin siber güvenlik risklerinin indirgenmesinde ve yatırım kararlarında iyileştirmeler yapılabildiğini belirtmiştir [30].

VI. GÜVENLİK YATIRIMLARININ OPTİMUM SEVİYESİNİN BELİRLENMESİ

Crume, bilgi güvenliğinin ilk kuralının, bir varlığı korumak için değerinden fazla yatırım yapmama gerekliliği olarak tanımlamıştır [31]. Bu nedenle, yapılması gereken yatırım seviyesinin belirlenebilmesi için işletmenin sahip olduğu bilgi varlıklarının değerlerinin belirlenmesi gerekmektedir. Poore, bilgi varlıklarının değerlerinin belirlenmesi aşamasında rehber olarak kullanılabilecek öneriler sunmuştur. [32].

Güvenlik yatırımlarının optimum seviyesinin belirlenmesi için önceki bölümlerde belirtilen edilen risk, saldırı ve teknoloji etkinlik ölçümlerinin sonuçlarından faydalanılarak yatırım kararları alınır. Literatürde bu alanda kullanılan üç genel yaklaşım bulunmaktadır [3].

- Karar Analizi Çerçevesi
- Oyun Teorisi
- Reel Opsiyonlar Teorisi

A. Karar Analizi Çerçevesi:

Bu yaklaşımın temelleri 1980'li yılların ortasında ABD Ulusal Standartlar Bürosu ve ABD Ulusal Bilgisayar Güvenlik Merkezi'nin önderliğinde gerçekleştirilen bir dizi bilgi güvenliği risk yönetim modelleme çalışmaya dayanmakta olup, ortaya çıkan birinci nesil siber güvenlik risk yönetim modellerinin en temeli Şekil 1.de görülen Ortak Çerçeve olmuştur [27].



Şekil 1. Ortak Çerçeve Süreç Diyagramı [27].

Ortak Çerçeve; Gereksinimler, Varlıklar, Güvenlik Endişeleri, Tehditler, Koruma Yöntemleri, Zafiyetler ve Sonuçlar olmak üzere yedi temel bileşenin tekrarlamalı bir süreç içerisinde analizini önermektedir. Ortak çerçevenin uygulama karmaşıklığı ve kaliteli verinin bulunamaması zorluklarının aşılabilmesi amacıyla, Entegre İş Risk Yönetim Çerçevesi, Değerleme-tabanlı metodolojiler, Senaryo Analizi Yaklaşımları ve En İyi Uygulamalar olmak üzere dört genel başlık altında ikinci nesil siber güvenlik risk yönetim modelleri ortaya çıkmıştır. Bu yaklaşımlar, her ne kadar veriye bağımlılık problemini kısmen aşmış olsalar da daha çok iş süreçlerine ve organizasyonel dinamiklere yoğunlaşmış, özellikle belirsizlik problemlerini aşamamıştır. 2000'li yıllardan itibaren yapılan pek çok çalışmada atıfta bulunulan Soo Hoo, doktora tezinde belirsizlikleri de içine alan karar analizi ve risk yönetimi tabanlı bir model önerisinde bulunmuştur [27].

Gordon ve Loeb, optimum yatırım seviyesinin belirlenmesi amacıyla yapılan yatırımın marjinal faydasının marjinal maliyete eşitlenme prensibine dayalı bir ekonomik model önermiş, bir işletmenin sahip olduğu varlıkların değerinin %36,8'inin optimum yatırım seviyesi olduğu sonucuna varmışlardır [33]. Willemson ise, Gordon ve Loeb tarafından



SİBER GÜVENLİK EKONOMİSİ ÜZERİNE LİTERATÜR İNCELEMESİ

önerilen model üzerinde düzeltmeler yapılarak yapılan hesaplamalarda optimum seviyenin varlık değerlerinin %50'sine çıkması gerekebileceğini iddia etmiştir [34].

Fayda maliyet analizinin, açık anahtar kriptografisi, ağ sızma tespit sistemleri vb. sistemlerin değerlendirilmesinde kullanılabildiği belirtilmiştir [35]. Xie ve Mead, fayda-maliyet analizi yöntemiyle küçük işletmelerin bilgi güvenliklerinin geliştirilmesine yardımcı olacak tahmin metodolojisi geliştirmiştir [36]. Bodin ve diğerleri tarafından, Analitik Hiyerarşi Prosesi kullanılarak çok kriterli bir karar verme modeli önerisi yapılmış [37], ancak karar seçimi alternatiflerinin belirlenmesi üzerinde durulmamıştır. Rue ve diğerleri tarafından ise farklı siber güvenlik yatırım modellerin analiz edilerek karşılaşıldığı bir çerçeve model önerisi yapılmıştır, sonraki çalışmalara için, istatistikî verilerin önerilen karar modelinde uygulanan değerlendirme sürecine dâhil edilmesini önermişlerdir [20]. Ionnidis ve diğerleri, fayda teorisini kullanarak siber güvenlik yatırımlarının doğru zamanlamasının belirlenmesi konusunda çalışmışlardır [38]. Chai ve diğerleri, güvenlik teknolojilerinin dolaylı getirisinin belirlenmesi kapsamında 1997-2006 yılları arasındaki ABD borsa verilerini temel alarak yaptıkları çalışmada, siber güvenlik yatırımı yaptıklarına dair medyada çıkan haberler sonrasında işletmelerin borsa değerlerinde aşırı yükselme olduğunu kaydetmişlerdir [39].

B. Oyun Teorisi:

Oyun teorisinin siber güvenlik yatırımlarının değerlendirilmesindeki uygulamaları kapsamında; saldırganların stratejileri arasındaki etkileşim ve sızma başarısının artırılması, karşı tarafta ise işletmenin kazancının maksimize edilmesi amacıyla yapılan yatırımların sonucu saldırıların engellenmesi, sistemdeki zafiyetlerin azaltılması ile saldırganlar üzerinde caydırıcılık etkisi vb. etkiler incelenmektedir [40].

Çavuşoğlu, oyun teorisi tabanlı bir yaklaşım kullanarak güvenlik yatırımlarını değerlendirme ve farklı faktörlerin yatırımlar üzerindeki etkisini inceleme amaçlı bir model önermişlerdir [41].

Grossklags, doktora tezinde, toplam çaba, en zayıf link, en iyi savunma, en zayıf hedef tiplerinden oluşan güvenlik oyunları siber güvenlik ve yatırım türleri ilişkilerinin ekonomik analizini yapmıştır [42].

Huan, doktora tezinde oyun teorisi ile öğrenme teorisini birleştirmiş, oyun teorisinde genellikle ele alınmadığını iddia ettiği zaman unsurunu da dikkate alan stokastik bir oyun modeli önererek yatırımların optimum seviyesinin belirlenmesi konusunda çalışmıştır [43]. Zeshuang ve Jing, oyun teorisi ile işletmelerin siber güvenlik yatırım kararlarını incelemiştir [40]. Liu ve diğerleri, bu yaklaşımla, iki işletmenin bilgi güvenliğine

ilişkin bilgi paylaşımı ve yatırım kararlarına ilişkin eğilimlerini incelemiştir [44]. Gao ve diğerleri, oyun teorisi kullanarak tüketim modellerinden Cournot ve Bertrams modellerini siber güvenlik yatırım kararlarının analizi amacıyla kıyaslamıştır [45]. Ashok ve diğerleri, enerji sektörüne yönelik kritik altyapıların geniş alan ağında izleme, koruma ve kontrolünün sağlanması amacıyla siber güvenliğinin belirlenmesinde oyun teorisi yaklaşımını kullanmışlardır [46].

C. Reel Opsiyonlar Teorisi:

İşletme varlıklarının değerlendirilmesinde kullanılan bu teoremin [47] önemli faydası stratejik kararların değerini yani esnekliği değerlendirme sürecine dâhil etmesidir [48]. Gordon ve diğerleri, siber güvenlik yatırımları için uygulanan bekle-gör politikasını ve saldırıların gerçekleşme sayısının artmasıyla orantılı olarak siber güvenliğe daha fazla yatırım yapıldığı düşüncesi bu yaklaşımı kullanarak açıklamışlardır [49]. Daneva ise önerdiği karar destek modelinde, belirlediği reel opsiyonların karar verme sürecinde gerekli esnekliği sağladığını iddia etmiştir [50]. Herath ve Herath, yığın e-posta üzerine gerçek verilerin kullanıldığı çalışmalarında reel opsiyonlar teorisi ile Bayes teoremi istatistikleri ve analizler sonrası öğrenmeyi içeren bir model önermişlerdir [51].

Ç. Kullanılan Metrikler

Bu bölümde, siber güvenlik yatırım kararlarının verilmesine yönelik kullanılan metrikler incelenecektir.

Yıllık Kayıp Beklentisi (Annual Loss Expectancy- ALE)

1979 yılında ABD Ulusal Standartlar Bürosu, "Otomatik Veri İşleme Risk Analizi Rehberi" isimli 65 numaralı Federal Bilgi İşleme Standardını yayımlayarak bilgisayar-tabanlı risklerin ölçümünde kullanılması amacıyla aşağıda açıklanan ALE metriğini önermiştir[27]:

$$ALE = \sum_{i=1}^n I(O_i) F_i \quad (1)$$

Yukarıdaki formüle;

{O₁, ... O_n} = Maddi zararlar sonucunda oluşan saldırı olay seti
I(O_i) = i olayının ABD doları cinsinden etkisi
F_i = i olayının gerçekleşme sıklığı

Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA) ise, ALE'yi benzer şekilde, Yıllık Gerçekleşme Oranı (Annual Rate of Occurrence-ARO) ile Bir Olayın Kayıp Beklentisi (Single Loss Expectancy-SLE) değerlerinin çarpımı olarak tanımlamıştır [52].

ALE metriğinin ilgi çekici yanı, riske yönelik olasılık ve sonuç niteliklerini tek bir rakamla ifade edebilme yeteneğidir.



Zayıf yanı ise, yüksek sıklığa sahip düşük etkili olaylar ile düşük sıklıklı yüksek etkili olayları birbirinden ayıramamasıdır [27]. Diğer bir eleştirilen tarafı, sadece doğrudan maliyetleri ele alması, örneğin üretimin aksamamasından kaynaklanan dolaylı maliyetlerin düşünülmemesidir [53].

İşletmelerin siber güvenlik yatırımlarını analiz etmek amacıyla Güvenlik Yatırımının Geri Dönüşü, Net Bugünkü Değer ve İç Verim Oranı metrikleri kullanılmaktadır [3,33,54,56].

Güvenlik Yatırımının Geri Dönüşü (Return on Security Investment-ROSI) :

En basit anlamda bir yatırımın geri dönüşü, aşağıdaki formülün [53] sağında görüldüğü üzere, yapılan yatırımdan elde edilen faydanın yapılan yatırım tutarına bölünmesiyle hesaplanır. Bu basit anlatımda, siber güvenlik yatırımı tutarı, somut bir sayıyı ifade eder, ancak siber güvenlik yatırımının faydasının hesaplanması kolay olmamaktadır, çünkü örneğin tedarik edilen bir güvenlik duvarının işletmeye doğrudan getirisi olmadığından, risklerden kaynaklanabilecek kayıp maliyetlerini indirgeme ya da farklı tanımlamalarla kullanılabilmektedir.

$$ROSI = \frac{R - ALE}{T} = \frac{S - T}{T} \quad (2)$$

Yukarıdaki formüle; R (recovery), bir yılda gerçekleşen saldırıların sebep olduğu kayıplardan kurtarma maliyeti; S (savings), yatırım yapıldığında önlenen kayıplardan tasarruf maliyeti; T (tool), güvenlik teknolojisinin maliyeti; ALE ise daha önce de açıklandığı gibi yıllık kayıp beklentisidir.

Aşağıdaki formüle ise ROSI, risk indirgeme oranı ile ilişkilendirilerek hesaplanmaktadır [55].

$ROSI = ((\text{Risk tutarı} \times \text{İndirgenen risk yüzdesi}) - \text{Güvenlik çözümünün maliyeti}) / \text{Güvenlik çözümünün maliyeti}$

Net Bugünkü Değer (Net Present Value-NPV)

ROSI metriğinin öznel zayıflığına ilave olarak zaman özelliği de problem teşkil etmekte, bu zayıflıklar nedeniyle işletmeler, ROI ile NPV metriklerinin kullanımına yönelmektedirler. NPV, ilgili yatırım çözümünün getirdiği para akışını bulmak ve bu rakamı mevcut zamanın para değerine dönüştürmek suretiyle çalışır. Para akışı, hesaplanan tahmini maliyetler, maliyet tasarrufları ve karlardan oluşmaktadır [3].

İç Verim Oranı (Internal Rate of Return-IRR)

Bu metrik de, NPV metriğine benzer şekilde para akışının hesaplanmasına odaklanır, ancak NPV'den farkı IRR'nin maliyet ve fayda arasındaki başa-baş noktasının bulunmasıdır [3].

Gordon ve Loeb, işletme içi yatırımların faydalarını, işletmenin diğer yatırımlarından ve faaliyetlerinden ayırd etmenin zorluğuna değinerek, gerçekleşen maliyet tasarrufları ile beklenen maliyet tasarruflarının karşılaştırıldığı gerek NPV gerekse de IRR metriklerinin yetersiz kaldıklarını belirtmişlerdir [33]. ROSI metriğinde olduğu gibi, NPV ve IRR metriklerinin hesaplanmasında da yatırım ve maliyetlere ilişkin faiz ve vergi unsurunun dikkate alınmamasının gerçek hayata uygun olmadığı, elde edilen değerlerin tam olarak gerçeği yansıtmayacağı belirtilmektedir [56].

VII. SONUÇ

Bu çalışmada, siber güvenlik ekonomisi alanında risklerin belirlenmesi ve ölçülmesi, güvenlik saldırılarının maliyet ve etkisinin ölçülmesi, güvenlik teknolojilerinin etkinliğinin ölçülmesi ve güvenlik yatırımlarının optimum seviyesinin belirlenmesi olmak üzere dört ayrı kategoride literatür incelemesi yapılmış, işletmelerin siber güvenlik yatırım kararlarını vermeleri için gerekli olan adımlara yönelik aşağıda belirtilen boşluklar tespit edilmiştir.

- Güvenlik olayları ile ilgili olarak risklerin belirlenerek ölçülebileceği “standart”, genel kabul görmüş bir model bulunmamaktadır.

- Yatırım yapılan güvenlik teknolojilerinin, riskleri ne oranda indirgediğinin, risk yönetimi açısından ne kadar etkili olduklarının belirlenmesine yönelik “standart”, genel kabul görmüş bir yöntem bulunmamaktadır.

- Siber saldırıların kayıp maliyet hesaplamaları ile, yapılan güvenlik yatırımlarının işletmeye finansal açıdan faydalarının hesaplanmasında “standart”, genel kabul görmüş bir yöntem bulunmamaktadır.

- Kullanılan finansal metriklerin farklı yazarlar tarafından farklı formüllerle siber güvenliğe uygulandığı görülmekte, dolayısıyla bu konuda da üzerinde uzlaşılmış, genel kabul görmüş bir yöntem ortaya konulmadığı anlaşılmaktadır.

- Kaliteli veriye bağımlılık nedeniyle çalışmada incelenen dört kategoride de ampirik çalışmalara ihtiyaç olduğu görülmektedir.

Sonuç olarak, siber güvenlik ekonomisi alanında yapılan çalışmalar farklı yaklaşımlar izlemekte, kaliteli verinin eksikliği ve farklı veri setleri kullandığından aynı durum için



farklı sonuçlar üretebilmekte ve sonuçta bütün bu bulgular, siber güvenlik yatırım kararlarının verilmesine yönelik bilimsel çalışmaların artarak devam etmesi gerektiğine işaret etmektedir.

KAYNAKÇA

- [1] A. Hovav ve J. D'Arcy, "The Impact of Virus Attack Announcements on the Market Value of Firms", Information Systems Security, June 2004.
- [2] M. Ünver, C. Canbay ve A.G. Mirzaoglu, "Siber Güvenliğinin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Raporu", Mayıs 2009.
- [3] X. Su, "An Overview of Economic Approaches to Information Security Management", Technical Report, June 2006.
- [4] Symantec and Ponemon Institute, "2010 Annual Study: US Cost of a Data Breach", March 2011.
- [5] HP Ponemon Study, "The Growing Cost of Cyber Crime", 2012.
- [6] S.E. Aoufi, "Economic Evaluation of Information Security, Ph.D Thesis, 2009.
- [7] J.N. Sheen, "Information Security Investment Decision by Fuzzy Economics", 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), 23-25 June 2010.
- [8] B. Blakley, E. McDermott ve D. Geer, "Information Security is Information Risk Management", Communications of the ACM, 2002, pp.97-104
- [9] R.K. Rainer, C.A. Snyder ve H.H. Carr, "Risk Analysis for Information Technology", Journal of Management Information Systems, 1991, Vol.8 No.1, pp.129-147.
- [10] J.S. Zachariah, "An Investigation of Organizational Information Security Risk Analysis", Auburn University, Ph.D Thesis, 2010.
- [11] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti ve S.K. Sadhukhan, "e-Risk Management with Insurance: A framework using Copula aided Bayesian Belief Networks", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.
- [12] H. Cylinder, "Evaluating Cyber Insurance", CPCU eJournal, Vol. 61 No. 12, December 2008.
- [13] H.S. Herath ve T.C. Herath, "Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management", Workshop on the Economics of Information Security (WEIS), 2007.
- [14] R. Böhme, "Cyber insurance Revisited" Workshop on the Economics of Information Security (WEIS), Harvard University, 2005.
- [15] R. Böhme ve G. Kataria, "Models and Measures for Correlation in Cyber-Insurance", Workshop on the Economics of Information Security (WEIS), UK, 2006.
- [16] L.A. Gordon, M.P. Loeb ve T. Sohail, "A Framework for Using Insurance for Cyber-Risk Management", Communications Of The ACM, 2003.
- [17] T. Bandyopadhyay, "Mitigation and Transfer of Information Security Risk: Investments in Financial Instruments and Technology", The University of Texas, Ph.D Thesis, 2006.
- [18] D. Claunch ve M. McMillan, "Determining the right level for your IT Security Investment", Healthcare Financial Management, pages 100-103, May 2013.
- [19] ISF, Information Security Forum, "The Standard of Good Practice for Information Security", 2007.
- [20] R. Rue, S.L. Pfleeger ve D. Ortiz "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making", Workshop on the Economics of Information Security, 2007.
- [21] Ponemon Institute Report sponsored by HP Enterprise Security, "2012 Cost of Cyber Crime Study", October 2012.
- [22] H. Çavuşoğlu, B. Mishra ve S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", Internal Journal of E-Commerce, 2004.
- [23] A. Hovav ve J. D'Arcy, "The Impact of Denial of Service Attack Announcements on the Market Value of Firms", Risk Management and Insurance Review, Vol.6, No.2, 97-121, 2003.
- [24] K. Campbell, L.A. Gordon, M. Loeb ve L. Zhou, "The Economic cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", Journal of Computer Security, pp. 431-448, 2003.
- [25] R. Telang, ve S. Wattal, "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – An Empirical Investigation", Working Paper, Carnegie Mellon University, 2006.
- [26] T. Wang, "Essays on Information Security from an Economic Perspective", Purdue University, Ph.D Thesis, 2009.
- [27] K.S. Hoo, "How much is Enough? A Risk-Management Approach to Computer Security", 2000.
- [28] J.R. Conrad, "Analyzing The Risks Of Information Security Investments With Monte Carlo Simulations", Proceedings of the 4th Workshop on the Economics of Information Security (WEIS05), June 2005.
- [29] S.A. Butler, "Security Attribute Evaluation Method: A Cost-Benefit Approach", Proceedings of the 24th International Conference on Software Engineering, New York, USA, pp. 232-240, 2002.
- [30] L.A. Gordon, M.P. Loeb, T. Sohail, C. Tseng ve L. Zhou, "Cyber Security, Capital Allocations and Management Control Systems", European Accounting Review, Vol.17, No.2, pp. 215-241, 2008.
- [31] J. Crume, "Inside Internet Security", Addison Wesley Professional Publications, 08 September 2000.
- [32] R.S. Poore, "Valuing information assets for security risk management", Information Systems Security, pp.13-23, October 2000.
- [33] L.A. Gordon ve M.P. Loeb, "The Economics of Information Security Investment", ACM Transactions on Information and System Security, 438-457, November 2002.
- [34] J. Willmson, "On the Gordon&Loeb Model for Information Security Investment", 2006.
- [35] R.T. Mercuri, "Analyzing Security Costs", Communications of the ACM, Vol.46 No.6. June 2003.
- [36] N. Xie ve N.R. Mead, "SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies", Networked Systems Survivability Program Technical Note, CMU/SEI-2004-TN-045, November 2004.
- [37] L.D. Bodin, L.A. Gordon ve M.P. Loeb, "Evaluating Information Security Investments Using Analytical Hierarchy Process", Communications ACM, pp. 78-83, 2005.
- [38] C. Ionnidis, D. Pym ve J. Williams, "Fixed Costs, Investment Rigidities and Risk Aversion in Information Security: A Utility-theoretic Approach", Workshop on the Economics of Information Security (WEIS), 2011.
- [39] S. Chai, M. Kim ve R.H. Rao, "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior", Decision Support Systems, Vol.50, pp. 651-661, 2011.
- [40] L. Zeshuang ve L. Jing, "Study on the Organization Information Security Investment-Decision Making Based on the Limited Strategy Game Theory Perspective", Second International Conference on Computational Intelligence and Natural Computing (CINC), 2010.
- [41] H. Çavuşoğlu, B. Mishra ve S. Raghunathan, "A Model for Evaluating IT Security Investments", Communications ACM Vol 47. No.7, pp.87-92, 2004.
- [42] J. Grossklags, "Secure or Insecure: An Economic Analysis of Security Interdependencies and Investment Types", University of Berkeley, California, Ph.D Thesis, 2009.
- [43] J. Huan, "Optimal Investment in IS Security: A Game Theoretical Approach", Morgan State University, Ph.D Thesis, 2009.
- [44] D. Liu, Y. Ji ve V. Mookerjee, "Knowledge Sharing and Investment Decisions in Information Security", Decision Support Systems", Vol. 52, pp.95-107, 2011.
- [45] X. Gao, W. Zhong ve S. Mei, "A Differential Game Approach to Information Security Investment Under Hackers' Knowledge Dissemination", Operations Research Letters, Vol.41, Issue 5, pp:421-425, September 2013.
- [46] A. Ashok, A. Hahn ve M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment", Journal of Advanced Research, (2014) Vol.5, pp. 481-489, 2014.
- [47] G.C. Akkaya, "Yatırım Projelerinin Değerlendirilmesinde Alternatif Bir Yöntem: Reel Opsiyonlar", Muhasebe ve Finansman Dergisi (MUFAD), Sayı 28, Syf. 172-178, Ekim 2005.



- [48] A. Değer, "Patent Değerlemesi ve Reel Opsiyonlar", Business and Economics Research Journal, Vol.2, No.1, pp.153-172, 2011.
- [49] L.A. Gordon, M.P. Loeb ve W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait and See Approach", Computer Security Journal, 19(2), 2003.
- [50] M. Daneva, "Applying Real Options Thinking to Information Security", Centre for Telematics and Information Technology (CTIT) Technical Report, 2006.
- [51] H.S. Herath ve T.C. Herath, "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit", Journal of Management Information Systems Vol. 25 Issue 3, p337, December 2008.
- [52] ENISA (European Network and Information Security Agency, "Introduction to Return on Security Investment", Deliverable, December 2012.
- [53] J.V. Brocke, G. Strouch ve C. Buddendick, "Return on Security Investments – Design Principles of Measurement Systems Based on Capital Budgeting", In Proceedings of ISTA 2007. pp.21-32, 2007.
- [54] CSI (Computer Security Institute), "Computer Crime and Security Survey", 2010.
- [55] W. Sonnenreich, J. Albanese ve B. Stout, "Return on Security Investment (ROSI) : A Practical Quantitative Model", Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.
- [56] K.K. Kommineni ve A.Y. Babu, "A Cost-Benefit Model for an Enterprise Information Security", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.2, Issue 3, February 2013.

yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş 100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.

Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.

H. Şentürk 1996 yılında Hava Harp Okulu Bilgisayar Mühendisliği Bölümü Lisans, 2002 yılında ABD Hava Üniversitesi Hava Kuvvetleri Teknoloji Enstitüsü (Ohio-ABD) Bilgisayar Mühendisliği dalında Yüksek Lisansını tamamladı. Doktora eğitimi, Kara Harp Okulu Savunma Bilimleri Enstitüsü Teknoloji Yönetimi Anabilim Dalında tez aşamasında devam etmektedir. 1998'den günümüze kadar Hava Kuvvetleri'nin çeşitli Mühabere Elektronik ve Bilgi Sistemleri kadrolarında, 2004-2007 yılları arasında NATO Program Merkezi'nde (Glons-Belçika) Analist-Programcı olarak çalıştı. İlgi alanları siber güvenlik stratejileri, siber savunma teknolojileri ve saldırı yöntemleri, kurumsal bilgi güvenliği, siber güvenlik ekonomisi ve yatırım kararlarının analizi, Ar-Ge ve teknoloji yönetimidir.

C. Z. Çil 1982 yılında Boğaziçi Üniversitesi Elektrik-Elektronik Bölümü Lisans, 1984'de Boğaziçi Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalında Yüksek Lisans, 1989 yılında Boğaziçi Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalında Doktorasını tamamladı. Hava Harp Okulu Elektronik Mühendisliği Bölümünde 1985-1994 döneminde öğretim elemanı olarak çalıştı, aynı dönemde Boğaziçi Üniversitesi Fizik Bölümünde kısmi zamanlı öğretim elemanı olarak dersler verdi. 1994-1997 döneminde NATO Havadan Erken İhbar Komuta Kontrol Sistemi Program Yönetimi Ajansı'nda (Brunssum-Hollanda) uzman test mühendisi olarak görev yaptı. 1998-2006 döneminde HAVELSAN A.Ş.'nde Savunma Sistemleri'nden sorumlu Genel Müdür Yardımcısı olarak çalıştı. 2006-2008 döneminde Kara Harp Okulu Savunma Bilimleri Enstitüsünde kısmi zamanlı öğretim elemanı olarak ders verdi. 2008 yılından itibaren Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümünde öğretim üyesi olarak çalışmakta, aynı zamanda 2009 yılından itibaren bu bölümün başkanlığını, 2013 yılı başından bu yana ise bölüm başkanlığı ile birlikte Mühendislik Fakültesi Dekanlığı görevini yürütmektedir. Dr. Celal Zaim ÇİL'in ilgi alanları katı hal elektronigi, analog ve sayısal elektronik, amorf yarı iletken ince filmler, LED ile aydınlatma sistemi tasarımı, savunma sistemleri elektronigi, ayrıca Ar-Ge ve İnovasyon Yönetimi ve Bilgi Yönetimidir.

Ş. Sağıroğlu Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü'dür. Zeki sistem kimliklendirme, tanıma ve modelleme ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları, yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50'nin üzerinde ulusal dergilerde



A Block Size Analysis for Blocked Discrete Wavelet Watermarking

Ahmet Şenol¹, Ersin Elbaşı², Kıvanç Dinçer¹, Hayri Sever¹

Abstract—Image watermarking has been an important discipline for claiming ownership, ensuring genuineness of images and fingerprinting of images. An important part of the work in this field is performed in discrete wavelet transform (DWT) domain. The watermark is embedded in coefficient values in one or all of LL, LH, HL, HH bands of first level or higher level (DWT) decompositions. In previous works, a host image is taken as a whole and firstly DWT of the whole image is found and then further level decompositions are obtained, if needed. In this paper, instead of taking DWT of the whole image, we implement the known DWT watermarking algorithm by first dividing host image into smaller blocks, namely 64x64, 32x32, 16x16, 8x8, and then taking DWT of each block independently. In addition, we divide the corresponding watermark into the same/matching number of blocks as the original image blocks. We then embed the corresponding watermark block into bands (LL, LH, HL, HH) of DWT transform of original image blocks. When we analyze the fidelity of watermarked images and similarity values of extracted watermarks for different types of block sizes and attacks, we observed that we get better results in our implementation than the known algorithm for some attack types and the results improve with smaller size blocks.

Index Terms— Block Size, Discrete Wavelet Transform, Image Watermarking, Robust Non-blind Watermarking.

I. INTRODUCTION

Millions of files are downloaded and uploaded every day on the Internet. Majority of the files exchanged on the Internet are image and video files. The ease of access to digital content on the Internet has increased all sorts of misuse including violating copyrights and tampering data without owner's permission [1]. Content owners are continuously seeking new ways for protecting their copyrighted files.

One of the main methods of protecting copyrighted content is watermarking. Image watermarking is embedding some data, called “watermark”, into the image that does not affect the quality of the image in visually detectable extent, and the watermark is extracted when necessary.

1 Computer Engineering Department, Hacettepe University, 06800 Çankaya Ankara

2 Department of Computer Engineering, Çankaya University, 06790 Etimesgut Ankara

A. Ş. Author (phone: +90-312-4175190; e-mail: asenol@kho.edu.tr).

E. E. Author (e-mail: eelbasi@cankaya.edu.tr)

K.D. Author (e-mail: kivanc.dincer@hacettepe.edu.tr)

H.S. Author (e-mail: sever@hacettepe.edu.tr).

Although a visible image watermark such as a logo can declare the identity of its producer, most watermarks in use are invisible. Image watermarking is commonly used for proving ownership, keeping track of advertisement broadcasts, putting metadata right into the image for indexing/searching and making sure that the image is not changed or disturbed (tamper detection).

There is the term “fragile watermarking”, which is used for proving the image is genuine. The watermark is embedded in such a way that the watermark is lost when the watermarked image is changed to some extent.

A successful watermark algorithm must satisfy following conditions [2]:

Fidelity: Fidelity is a criterion that the watermarked image looks like the original image, i.e. embedded watermark is not perceptible in the watermarked image. You see the original image and watermarked image in Fig.1 and Fig.2, respectively.



Fig. 1. Original Image



Fig. 2. Watermarked Image

Robustness: Robustness is the extent of durability of the watermark embedded in the original image after intentional or unintentional image processing attacks such as compression, cropping, noise, blur or filter. If the purpose is tamper detection, a fragile watermark is needed; i.e., with a slightest change in the watermarked image, watermark must deteriorate. Robustness is directly dependent on the watermarking method and domain. You see a binary image (visual) watermark in Fig.3 to be embedded in the image, and in Fig.4 you see the watermark extracted from a watermarked and attacked image. As seen, the watermark is easily recognizable regardless of the attack.

BC

Fig. 3. Binary Image Watermark embedded

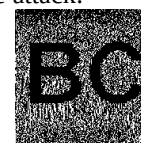


Fig. 4. Watermark extracted from watermarked and attacked document



Data Load Capacity: The amount of data that can be represented by the embedded watermark is named as “data load capacity.” Watermark detection type of watermark embedding methods help you to decide whether the watermark is present in the image or not. For example, if the watermark data load capacity is one bit: 1 indicates watermark is present, 0 otherwise. One can put much more data in images, such as binary images, or metadata images. If, for example, you put 64x64 binary logo image watermark in a 512x512 image, the data load capacity becomes 64x64. You can put 64x64 different binary images in the original image.

In all watermarking algorithms, there are two basic steps. 1) “watermark embedding” 2) “watermark detection/extraction” 3) An optional extra step named “watermark generation” [3].

If the original image is used in the detection/extraction phase of the algorithm then the algorithm is called *non-blind algorithm*. If only the original watermark is used in detection/extraction phase, it is called *semi-blind*, and if none of the two is used; it is called *blind* type watermarking algorithm.

Earliest forms of embedding watermarks in images were in the spatial domain. In spatial domain watermarking, watermark is embedded in least significant bits of an image [4]. In a typical grayscale image, 8 bits are used for one pixel that holds the luminance value of that pixel. When you change the least significant bits, overall appearance of the image doesn't change much. One can use 1 to 4 bits in each pixel of the image to hide another image or watermark.

In transform domain watermarking, the image is transferred to other domains, such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). In transform domain, image is transferred to corresponding frequency domain. The watermark is first multiplied by watermark weight values and then added to frequency values. After changing some of the frequency values, image is retransferred to spatial domain by applying reverse transform operation.

After the watermark is embedded in the image, there might be intentional or unintentional attacks that may disturb the watermark. A person that has legally obtained the image may want to resize the image, or may apply a blur filter on the image. In an air TV broadcasting, some noise may be added to image frames while they are transferred in the air. On the other hand, the person using the image without permission (pirate) intentionally tries to destroy the watermark by applying some kind of attacks.

Some of the major types of attacks against image watermarks are lossy image compression which affects watermark embedded in high frequency/textured image areas, blurring, sharpening, cropping, rotation, scaling, re-watermarking with attacker's own watermark to claim his ownership instead of the true owner, transfer operation which shifts the image left, right, down or upwards.

There are studies in the literature to avoid these types of attacks [6].

II. PREVIOUS WORK IN LITERATURE

Image watermarking began to develop in the spatial domain. Tirkel, Schyndel, and Osborne embedded watermarks of m-sequence to the least significant bit of a 8 bit gray scale image[4]. That spatial domain algorithm had a data load capacity of one bit; that is: the watermark is present or not.

Frequency domain or transform domain methods emerged to replace LSB based methods in the following studies. In 1997 Cox, Kilian, Leighton, and Shamoon [7] used the method of “spread spectrum communication” in which frequency band is very large, the message to be transmitted is spread along the frequency scale such that the signal is very weak in each frequency so that it could not be detected by hostile attacks. They made the analogy with the frequency spectra with the image transformed to frequency domain by DCT, and analogy with watermark and transmitted signal. To place a watermark of length n to an NxN image, firstly NxN DCT of the image is computed and the watermark is put in n highest magnitude coefficients of the transform matrix except the DC (lowest) component. Watermark embedding and detection processes are shown in Fig.5 and Fig.6.

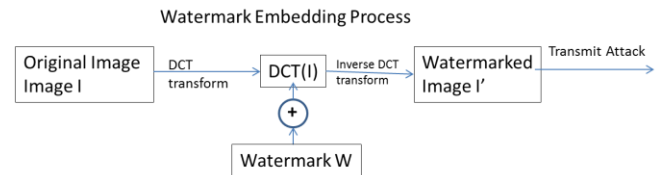


Fig. 5. Cox et al. Watermark Embedding Phase

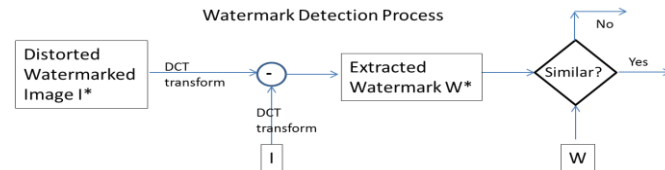


Fig. 6. Cox et al. Watermark Detection

Piva, Barni, Bartolini and Capellini used a similar method [8]. They also embedded the watermark in DCT domain where watermark is a pseudo random sequence of real numbers (PSRN) having mean 0 and variance 1. They differ from work of Cox et al. in that, instead of embedding the watermark in first 1000 DCT coefficients, they skip the first L coefficients and embed the watermark in the following M coefficients. The algorithm is semi-blind so the original image is not used in watermark detection phase. The authors skip the first L coefficients for the watermark to be not affected by high-pass filters such as histogram equalization, gamma correction. In the paper, they used L=25000, M=16000, where M is also the watermark size. The watermark is embedded in middle frequencies so that algorithm is more robust to low-pass and high-pass filters.

Correlation between the original and extracted watermark is computed as:

$$Z: \text{Correlation} = (W * V^*) / M = \frac{1}{M} \sum_{i=1}^M W_i \cdot V_i^* \quad (3)$$



where W is original watermark, V^* is the extracted watermark and M is the watermark size.

If $Z > T_z$, where T_z is correlation threshold value, then it is decided that watermark is present. T_z is calculated as:

$$T_z = \frac{\alpha}{3M} \sum_{i=1}^M |V_i^*|, \quad (4) \text{ where } \alpha = 0.2 \text{ in the paper}$$

Nikolaidis & Pitas claim that correlation detector is not optimal since data distributions of transform coefficients do not have Gaussian probability density function(pdf); instead, generalized Gaussian (GG) pdf is observed in DCT/DWT transform values[9]. They proposed a new watermark detection scheme that uses the parameter values of this pdf and pdf's parameters which are calculated from watermarked data itself. Rahman, Ahmad & Swamy propose to use pdf based on Gauss-Hermit expansion in detection of watermarks embedded in DWT sub band coefficients [10]. They claim that their detection method gives better results because this new pdf statistically matches better to the exact pdf since number of parameters calculated from higher order moments of image coefficients is more than GG or other type of pdf's.

Tao and Eskicioglu proposed a non-blind Discrete Wavelet Transform (DWT) based watermarking method[6]. In discrete wavelet transform, image is decomposed into four bands, each of which is half sized in both row and column size, which makes it a quarter of original size. Upper left band is called LL band, in which a coarser version of the original image is placed. The other bands are: on upper right band HL (horizontal detail), on lower left band LH (vertical detail), and lower right band LL (diagonal detail) high pass bands. The LL band in decomposition can be further decomposed to obtain another four bands of a lower level.

A binary image logo watermark is embedded in each four of the decomposition levels of the original image. After applying DWT transform to the image, in each of the bands (LL, LH, HL, HH), watermark embedding is done as in Eq.(5) and extraction is done as in Eq(6).

I : original $2N \times 2N$ image

W : $N \times N$ binary logo watermark image

V_{ij} : DWT coefficients in the corresponding band

V'_{ij} : watermarked DWT coefficients

V^{*k}_{ij} : watermarked and possibly attacked images DWT coefficients in band k , where $k \in \{1, 2, 3, 4\}$.

W^* : extracted binary watermark image

$$V^{k*}_{ij} = V^k_{ij} + \alpha_k W_{ij} \quad (5)$$

$$W^*_{ij} = (V^{k*}_{ij} - V^k_{ij}) / \alpha_k \quad (6)$$

Since magnitudes of DWT coefficients are larger in LL band, watermark strength constant α is a larger value than those of LH, HL, HH bands.

Visual quality of the watermarked and attacked images is measured using Peak-Signal-to-Noise-Ratio (PSNR) values.

$$PSNR = 20 \log_{10}(255/RMSE) \quad (7)$$

RMSE is square root of mean squared error between original and distorted images

$$RMSE = \sqrt{(\sum_{i,j} (I^*_{ij} - I_{ij})^2) / (N \times N)} \quad (8)$$

Many DWT-based watermarking schemes were developed thereafter[11]–[14]. Dugad, Ratakonda and Narendra proposed [11] a method similar to that of Tao and Eskicioglu's work[6]. Proposed work was also semi-blind DWT-based watermarking method, in which watermark is a binary image of the same size as the original image, watermark is embedded in LH, HL and HH bands. The watermark is embedded in only the coefficients higher than a given threshold T_1 . Adding watermark only to higher-level coefficients means embedding watermark in only the edges in an image. In the watermark detection phase, coefficients that are above a second threshold T_2 , where T_2 is far above T_1 , are chosen. Also while calculating the correlation threshold that is used to decide whether watermark is present or not, value is divided by $2M$ instead of $3M$ of Piva et al.'s work[8]. Authors state that since higher level coefficients are preserved despite much degradation, correlation value will be higher than that of [8]. This could give their method more fidelity by increasing deciding threshold value.

$$T_z = \frac{\alpha}{2M} \sum_{i=1}^M |V_i^*|, \quad (9)$$

Lai & Tsai embedded watermark into the singular values of the singular value decomposition (SVD) that is applied to the DWT bands of the original image[15].

Proposed Work: The proposed work pursues the method of Tao and Eskicioglu [6] that it is a DWT-based non-blind algorithm that embeds the watermark in all bands (LL, LH, HL, HH) of DWT transform. The difference is that, instead of taking DWT of whole image and embedding the whole watermark in first level decomposition bands, the original image is split into 64×64 blocks, and DWT of each block is taken separately. Watermark binary image is also split into 32×32 blocks, and this 32×32 part of watermark is embedded in first level DWT decomposition bands of 64×64 original image block. In each image block, a watermark block that is half size both in length and width of image block is embedded in first level decomposition LL, LH, HL, HH bands.

Similarly, the algorithm is run with the original image split into 32×32 , 16×16 , 8×8 blocks, obtained watermarked images and their PSNR values, also saved the extracted watermarks and their quality ratios.



PSNR values between the original image and watermarked image are calculated to compute the fidelity performance of the algorithm which measures to what extent the watermarked image looks like the original one. PSNR is described in Eq (7). Similarity ratio (SR) values are calculated between extracted watermark and embedded watermark. SR is calculated as in Eq (10).

$$SR = S / (S + D) \quad (10)$$

S: number of matching pixels in compared images

D: number of different pixels in compared images

Watermark Embedding and Extraction Algorithm for 64x64 image blocks is given below. In the same way, algorithm can be run for 32x32, 16x16, 8x8 sized blocks by changing block size values.

Watermark Embedding Algorithm:

1. Divide Original Image in 64x64 equal parts, Ipo
2. Divide watermark binary image W into 32x32 parts Wp
3. For each 64x64 part of original image block Ipo
 - a. $(Ipt_{LL}, Ipt_{LH}, Ipt_{HL}, Ipt_{HH}) = DWT(Ipo)$, transform
 - b. Embed 32x32 corresponding watermark part Wp into each of $Ipt_{LL}, Ipt_{LH}, Ipt_{HL}, Ipt_{HH}$
 - i) $Ipt_{LL}'_{ij} = Ipt_{LL}_{ij} + \alpha Wp_{ij}$ where $\alpha=8$ for LL band, $\alpha=2$ for other bands
 - c. $Ipw = IDWT(Ipt_{LL}', Ipt_{LH}', Ipt_{HL}', Ipt_{HH}')$, Obtain watermarked image part Ipw
 - d. Combine watermarked image blocks Ipw's to obtain watermarked image Iw

Watermark Extraction Algorithm:

1. Divide watermarked and possibly attacked Image in 64x64 equal parts, Ip*
2. Divide original Image in 64x64 equal parts, Ipo
3. Take $(Ipt_{LL}^*, Ipt_{LH}^*, Ipt_{HL}^*, Ipt_{HH}^*) = DWT(Ip^*)$
 $(Ipt_{LL}, Ipt_{LH}, Ipt_{HL}, Ipt_{HH}) = DWT(Ipo)$
4. For each 64x64 block of watermarked and original image block Ip*, Ipo
 - $Wp_{LL}^* = (Ipt_{LL}^* - Ipo_{LL})/coll$; where Wp_{LL}^* : Extracted Watermark part values in LL band, $coll=8$ for LL band.
 - $Wp_{LLb}^* = Wp_{LL}^* > 0.5$; where Wp_{LLb}^* : Extracted Watermark part as binary image in LL band
 - $Wp_{LH}^* = (Ipt_{LH}^* - Ipo_{LH})/coll$; $coll=2$ for HL

$$Wp_{LHb}^* = Wp_{LH}^* > 0.5;$$

$$Wp_{HL}^* = (Ipt_{HL}^* - Ipo_{HL})/coll; coll=2 \text{ for HL}$$

$$Wp_{HLb}^* = Wp_{HL}^* > 0.5;$$

$$Wp_{HH}^* = (Ipt_{HH}^* - Ipo_{HH})/coll; coll=2 \text{ for HH}$$

$$Wp_{HHb}^* = Wp_{HH}^* > 0.5;$$

5. Combine extracted watermark parts Wp^* 's to obtain extracted watermark W^* for each band LL, LH, HL, HH.

Since DWT coefficient values are larger in LL bands than in other three bands, watermark strength α is 8 for LL band, 2 for the other three bands.

A

Fig. 7. Second binary watermark image, namely the capital letter A, the same size as BC watermark

III. EXPERIMENTS

The algorithm was run by dividing the image into 512x512(whole image), 64x64, 32x32, 16x16, 8x8 image blocks, taking DWT of each block separately and embedding the watermark part into each of the first level DWT decomposition bands LL, LH, HL, HH. Watermarked images were saved for each case. Then most common attacks were applied to watermarked images. Those attacks were: Jpeg compression by %75, %50, %25 image quality, 3x3 blur filter, Gaussian noise attack with mean zero and variance 0.001, scale-rescale by 0.5 and 2, histogram equalization, intensity adjustment from range [0 0.8] to [0 1], gamma correction, re-watermarking. The original image used is seen in Fig.1. The binary watermark logo image is an image that has letters BC next to each other as seen in Fig.3. The second watermark embedded for attacking is seen in Fig.7. Watermarked and attacked images were also saved. The watermarked and attacked images and their corresponding PSNR values are seen in Fig.8 for the case when original image is divided into 8x8 image blocks. Only the watermarked images that are subjected to compression attacks are given.

The watermark extraction phase is run for each image block size case. The extracted watermarks and their similarity ratios are given in Fig.9. Again, only watermarks extracted from LL and LH bands for compression, rotate, scale, crop and re-watermark attacks are given. For each type of attacked image, extracted watermark from first DWT decomposition band of that attacked image is listed in the same column, as rows correspond to 64x64, 32x32, 16x16, 8x8 block size cases as seen in Fig.9. The extracted watermark's similarity ratio (extracted watermark quality) increases as the image is divided into smaller size blocks before embedding the watermark. The coarser watermarks are extracted when the



A BLOCK SIZE ANALYSIS FOR BLOCKED DWT WATERMARKING

image is divided into 64x64 parts, and the best results are obtained when the image is divided into 8x8 parts. The similarity ratios for each type of attack and for each size of blocks can be seen in the tabular form in Table I. Tao & Eskicioglu results are given as columns in Table I next to 8x8 block size result column. In this work we applied the same algorithm where Tao applied using same cover image and watermark. Experimental results show that our blocked watermarking method gives better results in embedding and in extraction phases after some common attacks than Tao algorithm. We do not compare directly with Tao's numerical results because we do not know some parameters such as scaling factor.

When we look at the algorithm in image fidelity aspect, although algorithm applied with smaller blocks gives much better extracted watermarks, it has no drawbacks compared to ones with larger blocks in fidelity aspect. PSNR values are all the same for every different block size. The only type of attack that PSNR values differ is the Gaussian Noise attack. This is because every time Gaussian attack is called, a noise that is formed by completely different values is applied on the watermarked image; so different PSNR values are reasonable.

We reached better results when we increased watermark strength $\alpha = 12$ for LL band, $\alpha = 5$ for LH, HL, HH bands, but inserted watermark began to be noticeable and image began to deteriorate. Also instead of comparing extracted watermark values with 0.5 when transforming it to binary image, we can compare with 0.45 or 0.4 to get a better-extracted image.

We must also mention a drawback that although the best results are obtained with 8x8 block size, only one level of DWT decomposition is possible for this block size. The second drawback is the extra CPU time needed as smaller block sizes are chosen. CPU time vs. block size graphs are given in fig.10 for embedding and extraction phases. For real time systems, execution time may be a problem but it could be tolerable in other type of systems.

IV. CONCLUSION

In Tao paper [6], binary pattern has been embedded in four bands of Discrete Wavelet Transform (LL, LH, HL and HH). Test results show that embedding the watermark in lower frequencies is robust to a group of attacks, and embedding the watermark in higher frequencies is robust to another set of attacks. Only for re-watermarking and collusion attacks, the watermarks extracted from all four bands are identical.

In this research work instead of using Tao's algorithm, we divided cover image into 512x512, 64x64, 32x32, 16x16 and 8x8 pixel blocks. We embedded binary watermark into each block using first level decomposition of DWT. Experimental results show that our method blocked watermarking gives better results in embedding and in extraction phases after some

common attacks than Tao's algorithm. The drawback of using smaller blocks is that computational overhead increases compared to using larger image sub blocks. We conclude that, blocked watermarking can be used successfully in cases where one can tolerate computational overhead.

REFERENCES

- [1] W. Bender, N. Morimoto, and A. Lu, "Techniques for data hiding," vol. 35, pp. 313–336, 1996.
- [2] V. M. Potdar, H. Song, and C. Elizabeth, "A survey of digital image watermarking techniques," 2005 3rd IEEE Int. Conf. Ind. Informatics, INDIN, vol. 2005, pp. 709–716, 2005.
- [3] N. Nikolaidis and I. Pitas, "Digital Image Watermarking: an Overview," pp. 1–6, 1999.
- [4] R. G. Van Schyndel, a. Z. Tirkel, and C. F. Osborne, "A digital watermark," *Proc. 1st Int. Conf. Image Process.*, vol. 2, pp. 86–90, 1994.
- [5] I. J. M. L. . B. J. A. Cox, *Digital Watermarking*. Academic Press, 2002, p. 542.
- [6] P. Tao, A. M. Eskicioglu, and I. Science, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain," pp. 1–12.
- [7] I. J. Cox, S. Member, J. Kilian, F. T. Leighton, and T. Shamon, "Secure Spread Spectrum Watermarking for Multimedia," vol. 6, no. 12, pp. 1673–1687, 1997.
- [8] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," *Proc. Int. Conf. Image Process.*, vol. 1, pp. 520–523, 1997.
- [9] A. Nikolaidis, I. Pitas, and S. Member, "Asymptotically Optimal Detection for Additive Watermarking in the DCT and DWT Domains," vol. 12, no. 5, pp. 563–571, 2003.
- [10] S. M. M. Rahman, M. O. Ahmad, and M. N. S. Swamy, "A New Statistical Detector for DWT-Based Additive Image Watermarking Using the Gauss – Hermite Expansion," vol. 18, no. 8, pp. 1782–1796, 2009.
- [11] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," *Proc. 1998 Int. Conf. Image Process. ICIP98 (Cat. No.98CB36269)*, vol. 2, pp. 1–5, 1998.
- [12] N. V Dharwadkar, "An Efficient Non-blind Watermarking Scheme for Color Images using Discrete Wavelet Transformation," *Int. J. Comput. Appl. (0975 – 8887) Volume 2 – No.3, May 2010*, vol. 2, no. 3, pp. 60–66, 2010.
- [13] O. Jane and E. Elbasi, "A new approach of nonblind watermarking methods based on DWT and SVD via LU decomposition," *Turkish J. Electr. Eng. Comput. Sci. doi10.3906/elk-1212-75*, pp. 1–13, 2012.
- [14] T. Minamoto and R. Ohura, "A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic," *Appl. Math. Comput. 226 306–319 Contents*, vol. 226, pp. 306–319, 2014.
- [15] C. Lai and C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," vol. 59, no. 11, pp. 3060–3063, 2010.





Fig. 8. Original, Watermarked and Attacked Images for 8x8 image block sizes and embedded watermark

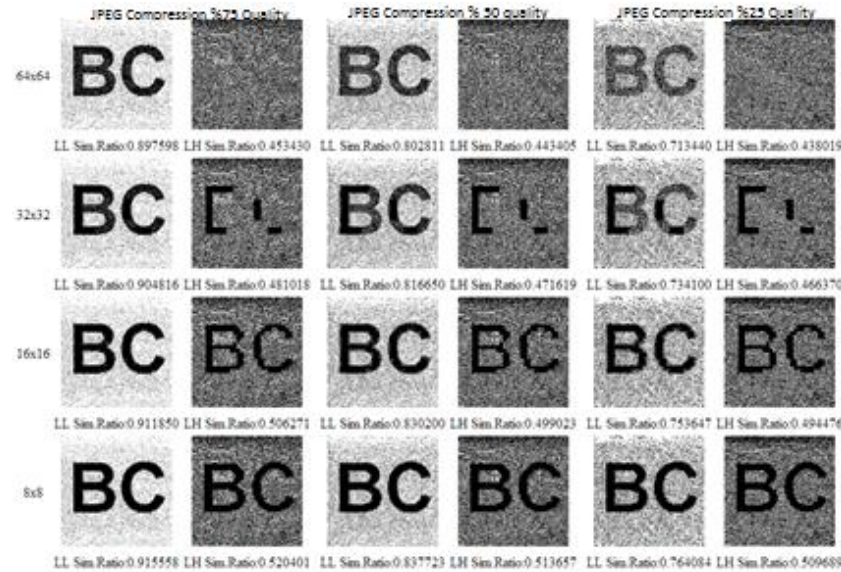


Fig. 9. Extracted watermarks from the bands LL, LH, HH for the cases images divided into 64x64, 32x32, 16x16, 8x8 image blocks

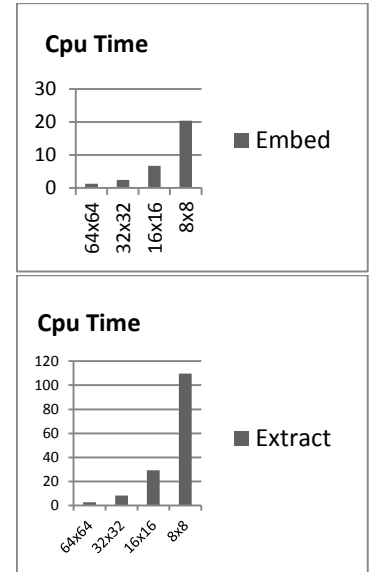


Fig.10. CPU time vs. Block Size Graphs for Embed & Extract Phases



Fig. 9. Continued

Table I. Similarity ratios for extracted watermarks from LL and LH bands for attack types

	LL						LH					
	512x512	64x64	32x32	16x16	8x8	Tao&Esk	512x512	64x64	32x32	16x16	8x8	Tao&Esk
JPEG 75	0,898	0,898	0,905	0,912	0,916	0,92	0,453	0,453	0,481	0,506	0,52	0,619
JPEG 50	0,803	0,803	0,817	0,83	0,838	0,84	0,443	0,443	0,472	0,499	0,514	0,6
JPEG 25	0,713	0,713	0,734	0,754	0,764	0,747	0,438	0,438	0,466	0,494	0,51	0,595
FILTER	0,772	0,772	0,79	0,805	0,815	0,822	0,373	0,373	0,4	0,427	0,442	0,596
GAUSS	0,685	0,688	0,709	0,727	0,737	0,717	0,545	0,547	0,576	0,608	0,62	0,563
SCALE-RESCALE	0,75	0,75	0,773	0,795	0,807	0,7795	0,425	0,425	0,453	0,481	0,496	0,604
HISTOGRAM EQ.	0,627	0,627	0,664	0,7	0,718	0,421	0,635	0,635	0,664	0,692	0,706	0,662
INTENSITY ADJ	0,801	0,801	0,867	0,932	0,966	0,197	0,747	0,747	0,765	0,785	0,795	0,799
GAMMA	0,199	0,199	0,199	0,199	0,199	0,803	0,827	0,827	0,836	0,848	0,854	0,863
ROTATE-ROTATE	0,766	0,766	0,776	0,784	0,789	0,91	0,458	0,458	0,482	0,506	0,52	0,654
CROP	0,586	0,586	0,586	0,586	0,586	0,996	0,7	0,7	0,717	0,725	0,731	0,913
REWATERMARK	0,864	0,864	0,915	0,952	0,977	0,905	0,864	0,864	0,915	0,952	0,977	0,905
TOTAL	7,878	7,881	8,149	8,39	8,526	8,0615	6,208	6,21	6,51	6,798	6,954	7,475

MOBILE OPERATING SYSTEMS AND SECURITY VULNERABILITIES

Mobile Operating Systems and Security Vulnerabilities

M. Alkan, S. K. Şenol, G. Uçtu

ABSTRACT

In this study the Mobile Operating Systems have been examined, security vulnerabilities have been investigated and mobile operating systems security levels have been explained by comparison. The security weaknesses are explained by examining the condensation and the level of safety between the versions of the operating systems. Mobile security issues to be kept in mind by users, risks, threats, forward measures to be taken are explained.

Key Words : *Information security, mobile operating system, security vulnerabilities*

I. INTRODUCTION

Operating systems are the system software that are responsible for running the basic system and application programs which built upon managing and controlling the hardware. Mobile operating systems are the operating system used in mobile devices such as the smart phone, tablet, PDAs. Currently mobile operating systems used to provide personal computer performance and enriched features such as phone capability, touch screen, Bluetooth, Wi-Fi, GPS, photography, audio and video recording for mobile devices.

The development of mobile operating systems is one of the important stages of development of mobile devices. The first cell phone was developed in 1973. Until 1992, embedded systems were used for control operations of mobile phones. IBM Simon (1993), combined mobile phone and PDA with the touch screen and e-mail features; was the first smart phone that we use. Palm Company in 1996 realized Palm OS operating system for the PDA branded Palm Pilot 1000 PDA. In 2000; Symbian has been developed as first modern mobile operating system for the mobile phones. In 2007, IOS operating system with Apple iPhone phones and in 2008 with a version of Android 1.0; Android operating system is released [1].

RIM Blackberry and Windows Mobile operating systems, which was developed before the IOS and Android operating systems has continued the activity for a while. Over time the use of IOS and the Android operating system has increased and today have become the most widely used mobile operating systems. According to the data obtained by IDC (International Data Corporation), on the first quarter of 2014 the market share of mobile operating systems are as shown in the following graphs and tables [2].

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
Q1 2014	81.1%	15.2%	2.7%	0.5%	0.6%
Q1 2013	75.3%	17.1%	3.2%	2.9%	1.5%
Q1 2012	59.2%	23.0%	2.0%	6.3%	9.5%
Q1 2011	36.1%	18.3%	1.2%	13.6%	30.8%

Source: IDC, 2014 Q1

Fig.1. The mobile operating system market share between the years 2011-2014

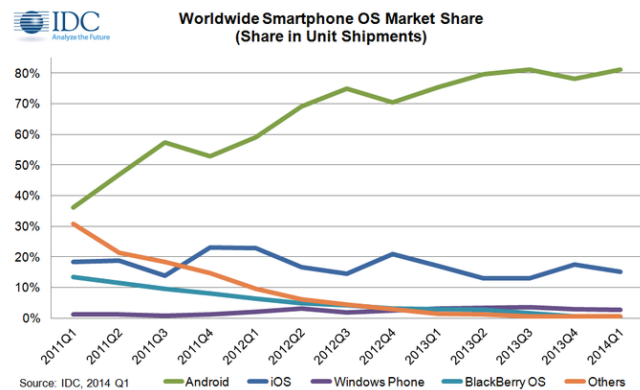


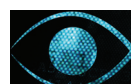
Fig.2. The graphic of mobile operating system market share between the years 2011-2014

In the last four years, the percentage of the use of the Android operating system increased more than double, while the percentage of iOS and Windows Phone maintained approximately, there was a decrease in BlackBerry OS and other operating systems. According to IDC reports percent market share, the most preferred mobile operating system Android OS, while Apple iOS is following him. In this study, four operating system in the chart above, will be discussed.

II. DEVELOPMENT OF MOBILE OPERATING SYSTEMS

A. Android Operating System

On 6 November 2007, under the leadership of Google, with the participation of 47 technology companies, such as HTC, Sony, T-Mobile, Texas Instruments, the Open Handset Alliance (OHA) was established [3]. The aim is to develop royalty-free technology which is based on open standards for mobile devices. Android operating system is an open source operating system, developed by Google and the OHA for mobile devices, based on the Linux operating system. It was developed in the Java language. This version includes features such as, camera support, Wi-Fi, Bluetooth, folders, web



MOBILE OPERATING SYSTEMS AND SECURITY VULNERABILITIES

browser, YouTube, alarm clock, voice dialing and alerts. The android operating system versions developed till this day are as follows [4].

- Android 1.1 Astro 9 February, 2009; It is designed for mobile phones only. Aims the system error correction of previous version and develop the API.
- Android 1.5 Cupcake, 30 April 2009; Ability to customize the widgets, animated screen and keyboard that can predict the text features were added.
- Android 1.6 Donut, 16 September 2009; screen resolution has been increased. Making accurate translation, advanced android market, multiple deletions in the gallery, voice dialing features are added.
- Android 2.0 / 2.1 Eclair, 29 October 2009; HTML 5 and Bluetooth 2.1 support have been added. Virtual keyboard, moving wallpapers, and digital zoom features have been added.
- Android 2.2, 20 May 2010; 720p screen resolution, USB connectivity, Wi-Fi feature of the browser, Flash Player 10.1 support was added.
- Android 2.3 Gingerbread on 6 December 2010; multi-camera and multi-touch support, video calling feature has been added. 7
- Android 3.0 / 3.1 / 3.2 Honeycomb February 2011; was developed only for tablets, android operating system was made compatible with the tablets.
- Android 4.0 Ice Cream Sandwich, 19 October 2011; face detection and file sharing with NFC features added.
- Android 4.1 Jelly Bean, 9 July 2012; The ability to open two applications at the same time, smooth sliding screen feature has been added. Energy efficiency was achieved.
- Android 4.2 Jelly Bean Plus, 29 October 2012; added features for multi-user and capturing 360-degree panoramic photo.
- Jelly Bean Android 4.2.2 Plus, 11 February 2013; heating and freezing problems have been fixed.
- Android 4.3 Jelly Bean, 24 July 2013; parental control, smart Bluetooth and Wi-Fi technology added. With this release application permissions could be controlled
- Android 4.4 KitKat, 31 October 2013; So many changes have been made on visual interface.

B. iPhone Operating System (IOS)

IOS is a mobile operating system designed for Apple's iPhone, which is also used later for iPod touch and iPad. IOS is a closed source operating system based on MacOS X operating system and has been developed in C language.

On 9 January 2007, first iPhone was announced and the first version was released on 29 June 2007. After this date, the IOS versions have been developed as follows [5]:

- IOS 1.x; On 29 June 2007 iOS 1.0 was released, then has been updated 8 times (1.0.1, 1.0.2, 1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5). With those updates new features have been added, such as safari security improvement, the recycling of elements deleted from the phone, custom ring tones, high audio quality, EDGE and GPRS support, new encryption

system. With the last update on July 15, 2008 the iPod Touch security update has been realized.

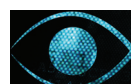
- iOS 2.x; Was released on 11 July 2008. Later, 2.0.1, 2.0.2, 2.1, 2.2.1 update was carried out in the form of 5 pieces. With this update, vulnerabilities of the old versions are closed.
- iOS 3.x; On 9 June 2009 was launched along with the iPhone 3GS version and 7 updates (3.0.1, 3.1, 3.1.2, 3.1.3, 3.2, 3.2.1, 3.2.2) was carried out. In this release, copy-and-paste feature and MMS support has been added. Also WebKit support has been added and security errors are fixed. iPad support is provided with 3.2 update.
- iOS 4.x; has been introduced on 21 June 2010. It is the first iOS version, supporting all apple devices. 16 updates are made as 4.0.1, 4.0.2, 4.1, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.3, 4.3.1, 4.3.2, 4.3.3
- iOS 5.x; Presentation was made on 6 June 2011 and was released on 21 October 2011. On this version iCloud cloud database system features have been added. 2 updates were performed as 5.0.1 and 5.1.1.
- iOS 6.x; Presentation was made on 11 June 2012 and was released on 29 September 2012. As 6.0.1, 6.0.2, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6 9 updates were performed.
- iOS 7.x; Was released on 10 June 2013 and was released on 18 September 2013. As 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.1, 7.1.1, 7.1.2 9 updates were performed.
- iOS 8.x; Presentation was made on 2 June 2014, and was released on 17 September 2014.

C. Windows Mobile Operating System

Windows mobile operating system is a mobile operating system developed by Microsoft Corporation for mobile devices. It is based on Windows CE and has been developed in C++.

The first version of Windows mobile operating system which designed for mobile computers was Pocket PC 2000 operating system and launched in April of 2000. Despite having limited functions; it was a preferred choice for pocket PCs. Its functions enriched and made compatible with mobile phones harmonized with Pocket PCs and 2002 version has been released in 2001 October. In June of 2003 for Pocket PC, Windows Mobile name had been used instead, and giving more weight to the mobile phones as a mobile operating system has continued on his way. With the name of the Windows Mobile operating system released versions are as follows [6].

- Windows Mobile 2003 June 2003
- Windows Mobile 2003 SE, March 2004; some of the vulnerabilities of Windows Mobile 2003 version have been fixed and ActiveSync feature added
- Windows Mobile 5, May 2005; With this release, a new system has been enhanced, also persistent memory support is provided.
- Windows Mobile 6, February 2007; Windows Live Messenger has been added.
- Windows Mobile 6.5, May 2009; was developed to fix the old version errors.



MOBILE OPERATING SYSTEMS AND SECURITY VULNERABILITIES

Microsoft Company began to face some problems and receive criticism with the current versions. Received so many complaints about being useless, development difficulties and the distribution channels. To eliminate this problem, Microsoft Corporation has developed Windows Phone. The user interface and application architecture was redesigned [7]. Hardware changes made to this new operating system, prevented to resume compatibility with the Windows mobile operating system applications. The versions of the Windows Phone operating system are as follows [8].

- Windows Phone 7, 29 October 2010;
 - Windows Phone 7.5, Mango, 27 September 2011; The mobile version of Internet Explorer 9, multitasking support for third-party applications are added.
 - Windows Phone 7.5, Tango, 28 June 2012; Errors fixed, low-equipped device configuration has been developed.
 - Windows Phone 7.8, 1 February 2013
- On June 20, 2012, Microsoft Corporation announced that they changed the mobile operating system to the Windows NT, rather than to Windows CE kernel. This modification was to ensure compatibility between Windows 8 and Windows Phone.
- Windows Phone 8, 29 October 2012; It is compatible with Windows 8. High screen resolutions are supported. The Start screen is renovated.
 - Windows Phone 8.1, 14 April 2014; Word Flower keyboard also supports Turkish, notification area, display buttons are added features.

D. Blackberry Operating System

BlackBerry operating system is the java-based mobile operating system produced by RIM (Research in Motion) for BlackBerry mobile devices. Versions developed as follows [9].

- BlackBerry 1.0, February 1999; has been released with BlackBerry 580 pager. Include features: To be able to send and receive mail, telephone and messaging.
- BlackBerry 3.6, March 2002; was released with BlackBerry 5810 smartphone.
- BlackBerry 5.0, 4 August 2008; was released with the BlackBerry Bold smartphone, then began to be used also in other BlackBerry devices.
- BlackBerry 6.0, April 2010; includes WebKit-based browser.
- BlackBerry 7.0, August 2011; there is no compatibility with previous versions. Previous versions of BlackBerry devices with version 7.0 cannot be updated.
- BlackBerry 7.1, 2012; version 7.0 update with innovations like calling over Wi-Fi and Wi-Fi hotspot features.
- BlackBerry 10, it was announced in 30 January 2013. BlackBerry 10 mobile operating system developed for use in next-generation BlackBerry devices, QNX-based operating system is designed.

III. MOBILE OPERATING SYSTEM SECURITY

The operating system, armed with one of the main roles in mobile communications, has important functions at the point to provide mobile security. Mobile operating systems also contain similar security activities. However, these application methods vary. In general, the security measures used in operating system, 'sandbox' function allowing you to work independently of each files and an approval mechanism, the 'digital signature' is a function. However, some of these received measures to create a more secure system, has prepared the ground for the emergence of security weaknesses. as the 'Jailbreaking' in IOS and abuse of the permit system in Android OS.

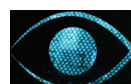
A. Sandboxing

Sandboxing process is separation of each software package by the core on the application level. Thus application access to sensitive information stored units, the private area of another application, hardware such as camera and GPS has become controlled [10].

As IOS, sandboxing process is accomplished by layered IOS architecture. 3rd party applications and system resources are operated in different layers. Thus, access to system resources of the application software is restricted [11]. Applications can be accessed to the protected resources using registered APIs. Application developers are submitted for Apple's approval before releasing their applications. Deemed appropriate applications are approved by Apple and allowed to access protected resources using registered API's. Applications not approved by Apple rejected .Approved applications are dealt via the Apple's official app store, Apple Store.

Sandboxing in Android operating system is provided with particular virtual machine process called Dalvik [12]. Android runtime layer is the layer that 3rd Party applications are written [13]. Developed applications in this layer are added to the virtual machine and each single user as if the virtual machine is operated separately. Thus sorting of developed applications other system resources are provided [11]. Application's access to system resources that needed to be interact, built on permissions in order to fulfill their functions. Application developers, prepares a description that applications needs to access which system resources to fulfill their function and seek permission from users for access. These permissions must be approved by the user before installing applications on mobile devices. As the Android operating system does not process any approval, distribution of application is carried out more freely. Application developers are free to share applications on the platform they want.

Sandboxing function is also performed by the virtual machine on the BlackBerry operating system. Applications can be distributed with 3rd party channels without approval. However, only approved applications can be distributed on the official app store 'App World'.



MOBILE OPERATING SYSTEMS AND SECURITY VULNERABILITIES

B. Digital Signature

Digital signature application is a system which is a security measure and an approval mechanism, just like sandboxing, exists in the operating system but used in different situations.

In the Android operating system, developers assigns signature. The goal here is not to give corporate approval to application, but provide continuity of updates. Signature system is used to determine who developed the application and confirm that updates made by the same developer.

In the process of IOS, Apple makes signing itself. When proper Applications that are submitted by the developers for approval and received the approval by Apple and signed; both they were allowed access to system resources and distribution is made. Unsigned applications will not be distributed.

On BlackBerry operating system, the signature application is used to keep track of restricted APIs. With BlackBerry operating system certain APIs are limited. Users should purchase signing key from RIM if they need to use limited APIs. Unique keys are created for each user [11].

C. Jailbreaking

Apple's goal of providing a more secure operating system and taken around the IOS with thick walls, have been exceeded by malicious attackers, as well as iOS users. Apple follows a rigid policy about distributing the applications via the official store. Some iOS users executing jailbreak process to achieve a freer life beyond this conservative approach.

Jailbreaking allows descending the operating system roots and provides the opportunity to make changes here with the patches and changes in the operating system [14], so it is a rooting process. Thus, by removing restrictions on the installation of unapproved applications, the operating system will become freer but more vulnerable. IOS's approval mechanism is a kind of 'chain of trust' which allows to run only safe and competent programs [15]. However, the jailbroken devices can undermine the trust chain. And make the device clear to every application that is authorized or unauthorized, malicious or not.

By the jailbreaking process performed in the IOS;

- Provides access to the operating system
- Obtain the opportunity to install applications and themes not approved by Apple
- Limitations on the mobile device are removed.

Rooting, operation down to the roots of the system, although not as intense as in IOS, is a condition encountered also on Android operating system. By the rooting process on Android operating system;

- obtain access opportunity to the Flash memory chip
- Applications to run faster
- The device or carrier applications can be changed
- The device can be converted to Wi-Fi hotspot

In some versions of the BlackBerry operating system, a jailbreak tool called 'Dingleberry' can be used for rooting process, but BlackBerry 10 does not allow jailbreaking [16].

D. Permission System

Basic security system used in Android operating system is permission application. In theory, it is a very robust security method, but it is weakened by users and application developers who abuses system [17].

Application developers as they have developed their practices when determining what permissions you need, sometimes unconsciously permissions are not needed, can add to the list. Selected extra permissions without required examination or using the same permission list of another application causes weakness in the system [18]. Request of permissions not necessary for the development of the application program, can be done in a conscious way by malicious people, with evil intentions, hiding behind innocent application to perform malicious activities. In both cases, consciously or unconsciously, causes a security weakness.

Literally the creation of a safe permitting system based on users. Because these systems, users are in the decision making process. Users needed to carefully review the allow lists and make a decision required by them. These permissions in the Android operating system can be handled in three categories [19]

- Normal: Low-risk permits. It can be annoying but they are not harmful to the user. For example, 'set wallpaper' permission, gives you to change the background image on the mobile device.

- Dangerous: Access to private information, or lead to financial losses are allowed. For example, permission to send SMS/MMS messages or access e-mail accounts.

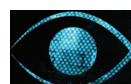
- Signature/system: The most dangerous are the permissions that are required to arrange access. For example, delete application permissions. Those are more difficult to obtain.

In order to make accurate decisions, users must have a minimum knowledge about the permissions and which category they belong. Also they are required to have much interest to examine the permissions before downloading the application. Otherwise, by accepting all the permissions requested, without passing through an assessment, they bypass the security system and has made devices become open to any attack.

IV. CONCLUSION

Since the first developments of Mobil operating systems, the development of new versions and updates are done to get more functional and safer operating system. At this point, the mobile operating systems try to provide a balance between security and usability according to their corporate principles.

On the one hand, the iOS operating system draws clear boundaries with red lines trying to achieve a more robust security system, on the other side, Android operating system, based on freedom and leave the security option and responsibility to the users. Users are the ones who will make the choice. In addition, users have the opportunity to use the secure platform in a possible free form thanks to their technical skills, security perceptions and awareness. Also they can use the platform that removes many limitations, as safest



MOBILE OPERATING SYSTEMS AND SECURITY VULNERABILITIES

as possible. Both platforms can provide the ideal conditions for this infrastructure.

REFERENCES

- [1] www.wikipedia.org/wiki/mobile-operating-system
- [2] www.idc.com/prodserv/smartphone-os-market-share.jsp
- [3] www.wikipedia.org/wiki/open_Handset_Alliance
- [4] [www.wikipedia.org/wiki/Android_\(işletim-sistemi\)](http://www.wikipedia.org/wiki/Android_(işletim-sistemi))
- [5] www.wikipedia.org/wiki/IOS_version_history
- [6] mobilişletimsistemleri.wikispace.com
- [7] P. Grundström, "Mobile Development for Iphone and Android", *B.S. thesis*, Sweden, 2010.
- [8] en.wikipedia.org/wiki/Windows_Phone_version_history
- [9] www.wikipedia.org/wiki/BlackBerry_OS
- [10] T. Vidas, D. Votipka, N. Christin, "All Your Droid Are Belong To Us: A Survey of Current Android Attacks", *Carnegie Mellon University*, 2011.
- [11] D. Barrera, P. Van Oorschot "Secure Software Installation on Smartphones", *Carleton University*, 2010.
- [12] J. Joseph, "Mobile OS-Comparative Study", *Journal of Engineering Computers & Applied Sciences (JEC&AS)*, 2013.
- [13] I. Thakur, G.S. Jain, "Countermeasures for Security Vulnerability in Android", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, June. 2013.
- [14] S. Salerno, A. Sanzgiri, S. Upadhyaya, 'Exploration of Attacks on Current Generation Smartphones', *Procedia Computer Science*, 2011.
- [15] Grimes, Galen A. "Are Apple's Security Measures Sufficient to Protect Its Mobile Devices?", *Wireless Telecommunications Symposium (WTS)*, 2012. IEEE, 2012.
- [16] A. Antuk, "BlackBerry Z10 Research Primer". *SEC Consult Vulnerability Lab*, Vienna, May. 2013.
- [17] S. Mansfield-Devine, 'Android architecture: attacking the weak points', *Network Security 2012.10 (2012)*: pp.5-12, 2012.
- [18] Z. Fang, W. Han, Y. Li, "Permission Based Android Security: Issues and Countermeasures", *Computers & Security 43 (2014)*: pp.205-218, 2014.
- [19] AP. Felt, E. Chin, S. Hanna, D. Song, D. Wagner, "Android Permissions Demystified". *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011.

Mustafa ALKAN



Graduated from Erciyes University, Faculty of Engineering, Department of Electronic Engineering. Studied as research assistant at the same university. He received the Master and PhD Degree in Erciyes University. He served as head of Electronic Department from 1994 to 2001. Became an Associate

Professor in 1998. He was Deputy Chairman of The Information and Communication Technologies Authority between 2001 and 2012. Became a professor in 2012. Prof. Alkan has been serving as Head of Department on Gazi University, Technology Faculty, Electric-Electronic division.

He had more than 100 works published in the field of electronics and IT in national and international journals. He got project studies on Information Security, Cryptography, Internet Domain Names, IPv6, Cyber Security, Electronic Signatures, Registered Electronic Mail Systems. He has carried out tasks such as National Coordination Committee of the World Summit on Information Society and Electronic Signature Coordination Committee. He is co-chair of several National and International Conferences in the field of ICT.

Sümeýra KAVRUK ŞENOL

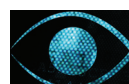


She was born in Ankara in 1980, graduated from the Malatya İnönü University. Faculty of Engineering, Department of Electrical and Electronic Engineering in 2002. She received the Master Degree at Malatya İnönü University, Electrical and Electronic Engineering. Worked for a private company for a while. Started her PhD on Gazi University, Technology Faculty in 2013.

Göksel UÇTU



He was born in Mersin in 1989. He received the Electronic and Electronics Engineer degree from TOBB ETU in 2011 and master of science degree from Middle East Technical University (METU) Telecommunication option in 2014. He is currently working towards his Ph.D. degree in the Electrical and Computer Engineering Department at TOBB ETU in Ankara and research assistant at Gazi University, Faculty of Technology. His research interests include green communication, energy harvesting, energy efficiency, convex optimization and software defined radio.



Güvenli İnternet

S. Özeren

Özet — Bu çalışmada Türkiye’de yürütülmekte olan Güvenli İnternet uygulamalarının kapsam ve etkinliği incelenmiştir. İnternet ortamındaki risk ve tehdit unsurlarını tanımlayan kavramların açıklanmasının ardından Türkiye’de uygulanan siber güvenlik politikaları incelenmiş ve güvenli İnternet uygulamaları, diğer ülkelerdeki uygulamalarla kıyaslanmıştır. Güvenli İnternet konusunda Avrupa Birliği mevzuatı ve uluslararası sözleşmeler çerçevesinde Türkiye’nin bulunduğu konum değerlendirilmiştir.

Anahtar Sözcükler — Bilgi Güvenliği, Siber Güvenlik, Güvenli İnternet, İnternet Güvenliği.

Summary – In this study, the scope and effectiveness of secure Internet applications have been investigated that is being conducted in Turkey. After the announcement of the notions identify the risks and threats in the Internet environment, the Cyber Security policies implemented in Turkey are examined and Internet applications have been compared with the practices in other countries. The location of Turkey was evaluated within the framework of the European Union legislation and international conventions about the Internet Safety.

Keywords - Information Security, Cyber Security, Internet Safety, Internet Security.

I. GİRİŞ

BİLİŞİM ve mobil iletişim teknolojileri geliştikçe günlük yaşamımızdaki süreçler İnternet ortamına entegre olmaktadır. Günümüzde vatandaşlar, firmalar ve devletler arasındaki pek çok ilişki İnternet teknolojileri üzerinden yürütülmektedir. Akıllı telefonların yaygın kullanımıyla birlikte nüfusun büyük bir çoğunluğu 24 saat kesintisiz İnternet bağlantısına sahip olmuştur.

İnternet teknolojilerinin yaygın kullanımının doğal bir sonucu olarak devletler özellikle çocuk istismarlarını engellemek ve çocukları zararlı içeriklerden korumak amacıyla uluslararası sözleşmelere taraf olmaya ve ulusal İnternet politikaları geliştirmeye başlamıştır.

S. Özeren TEDER ve İnternet Geliştirme Kurulu Başkanı’dır. (Tel: 3124660411; Faks: 3124660418; e-Posta: serhat.ozeren@teder.org.tr).

II. İNTERNET TEKNOLOJİSİ

İnternet, dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır [1]. Türk Dil Kurumu, İnternet sözcüğüne karşılık olarak “genel ağ” ifadesini önermiştir. İnternet, çok protokollü bir ağ olup birbirine bağlı bilgisayar ağlarının tümü olarak da tanımlanabilir. Binlerce akademik ve ticari ağla devlet ve serbest bilgisayar ağının birbirine bağlanmasıyla oluşmuştur. Bilgisayarlar arasında bilgi TCP/IP protokolleri aracılığıyla transfer edilmektedir.

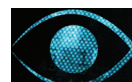
İnternet’in kökeni, kesintisiz, sağlam ve özel bir bilgisayar ağı kurmak isteyen Amerika Birleşik Devletleri hükümeti tarafından 1960 yılında başlatılan araştırmalara dayanmaktadır.

1980’lerde Ulusal Bilim Vakfı tarafından yeni bir ABD omurgasının finansmanı için toplanan özel fonlar, dünya çapında katılım ve birçok özel ağın birleşmesini sağlamıştır.

1990’larda uluslararası bir ağın yaygınlaşması ile internet, modern insan hayatının temelinde yer almıştır. Günümüzde günlük yaşamımızdaki pek çok süreç İnternet üzerinden yürütülmektedir.

İnternet üzerinden ağ sayesinde iletişim kuran bilgisayar sistemleri olan askeri iletişim sistemi Semi-Automatic Ground Environment (SAGE) ve ticari havayolu rezervasyon sistemi olan Semi-Automatic Business Research Environment (SABRE) 1950’lerin başında çalışmaya başlamıştır. 1960’larda ise ‘the Advanced Research Projects Agency (ARPA)’, ABD’nin savunma sistemi için ‘the Advanced Research Projects Agency Network (ARPANET)’ün tasarım finansmanı olmaya başladı. 1960’larda oluşturulan projeler sayesinde 1969’da İnternet o dönemin zirvesine ulaşmıştır. Bu tarihten sonra da ARPANET bildiğimiz modern İNTERNET olarak hayatımızdaki yerini aldı. 1970’li yılların başında Amerikan üniversitelerine bu projeden yararlanma imkânı verilmesinin ardından e-posta (SMTP) ve NNTP uygulamaları yaygınlık kazanmaya başlamıştır. Bu uygulamaları FTP ve HTTP protokolleri izlemiştir [2].

İnternet iletişimi TCP/IP (Transmission Control Protocol / Internet Protocol) adı verilen bir protokol kümesi kullanılarak sağlanmaktadır. Bu protokollere örnek olarak, dosya alma/gönderme protokolü (FTP, File Transfer Protocol), elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol), TELNET protokolü verilebilir. Web sayfalarına bağlanmak için kullanılan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır. TCP/IP



protokolü aynı zamanda, diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok farklı tipte bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır [3].

III. SİBER GÜVENLİK

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımları, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük ve gizliliklerdir. (ITU – T X.1205 sayılı Tavsiye Kararında yer alan ve uluslararası alanda kabul gören tanımdır) [4].

A. Siber Güvenlik Konusunda Bakanlıklar Düzeyindeki Çalışmalar

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) arasında Siber Güvenlik konusunda 3 Mayıs 2012 tarihli bir protokol imzalanmıştır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Bilim Sanayi ve Teknoloji Bakanlığı arasında Siber Güvenlik konusunda 14 Ağustos 2012 tarihli bir protokol imzalanmıştır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile TÜBİTAK arasında Ulusal Siber Güvenlik Teknoloji Geliştirme Programı Konusunda 14 Ağustos 2012 tarihli bir “Danışmanlık Hizmetleri Alımı Sözleşmesi” imzalanmıştır.

Bakanlar Kurulu’nun, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı, 20 Ekim 2012 tarihli Resmi Gazete’de yayımlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Siber Güvenlik Kurulu’nun 1’inci toplantısında 20 Aralık 2012 tarihinde onaylanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Bakanlar Kurulu tarafından 20 Haziran 2013 tarihinde kabul edilmiştir.

Siber Olaylara Müdahale Ekiplerinin (SOME) Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 11 Kasım 2013 tarihli Resmi Gazete’de yayımlanmıştır.

655 sayılı KHK, 5809 sayılı Elektronik Haberleşme Kanunu ve 5651 sayılı Kanun’la ilgili değişiklikler 02 Aralık 2013 tarihli Bakanlar Kurulu toplantısında görüşülmüştür. Değişiklik talepleri Siber Güvenlik Çalışmaları ve Siber Güvenlik Kurulu’nun varlığı ve işleyişi, yer sağlayıcılara yönelik hapis cezası uygulamasının kaldırılması, yer sağlayıcıların sınıflandırılması ve teşviki, yer sağlayıcılar için

faaliyet belgesi yerine bildirim usulü getirilmesi başlıklarında değerlendirilmiştir.

Adalet Bakanlığı Siber Güvenlik Kanun Taslağı ilgili kurumların görüşlerine gönderilmiştir [5].

Milli Savunma Bakanlığı Genelkurmay Muhabere Elektronik ve Bilgi Sistemleri Başkanlığı tarafından konuya ilişkin olarak, Ekim 2012 tarihinde başlatılan süreç içerisinde ilgili makamlar ile koordine edilerek söz konusu mutabakat muhtırası hazırlanmıştır. 20 Haziran 2013 tarihinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’nda icra edilen 2’nci Siber Güvenlik Kurulu’nda alınan karar doğrultusunda, Türkiye Cumhuriyeti Hükümeti ile NATO Siber Savunma Yönetim Kurulu arasında siber savunma alanında işbirliğine yönelik olarak hazırlanan “NATO Siber Savunma Mutabakat Muhtırası”nı imzalamaya, Türkiye Cumhuriyeti adına Millî Savunma Bakanlığı yetkilendirilmiştir. Bu kapsamda; 12 Temmuz 2013 tarihinde Dışişleri Bakanlığı’nda, 22 Kasım 2013 ve 27 Kasım 2013 tarihlerinde Millî Savunma Bakanlığı’nda; Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK katılımı ile icra edilen toplantılar neticesinde söz konusu mutabakat muhtırası güncellenerek uzlaşma ile nihai hale getirilmiştir. “NATO Siber Savunma Mutabakat Muhtırası”nın, Türkiye Cumhuriyeti Hükümeti ile NATO Siber Savunma Yönetim Kurulu arasında imzalanması için gerekli işlemlerin ve sürecin başlatılması aşamasına gelinmiştir [6].

IV. GÜVENLİ İNTERNET

Güvenli İnternet, teknik güvenlik ve içerik güvenliği olarak iki açıdan değerlendirilmektedir. İngilizcede teknik güvenlik “security” kavramıyla, içerik güvenliği ise “safety” kavramıyla tanımlanmaktadır. Güvenli İnternet terimi Türkiye’deki mevzuat çerçevesinde “Internet Safety” teriminin Türkçe karşılığı olarak kullanılmaktadır.

V. TÜRKİYE’DE GÜVENLİ İNTERNET HİZMETİ

Güvenli İnternet Hizmeti, altyapısı erişim sağlayıcılar tarafından oluşturulan ücretsiz, talebe bağlı ve alternatif bir İnternet erişim hizmetidir.

Güvenli İnternet Hizmeti’ne ilişkin çalışmalar, Anayasa’nın “Ailenin korunması ve çocuk hakları” başlıklı 41. Maddesi ve “Gençliğin korunması” kenar başlıklı 58. Maddesi hükümlerine dayanmaktadır. Ayrıca bu Anayasal hükümlerin yanında Elektronik Haberleşme Kanunu’nun Tüketici ve Son Kullanıcı haklarını düzenleyen hükümleri ile bu kanun uyarınca çıkarılan Tüketici Hakları Yönetmeliği’nin “İnternetin Güvenli Kullanımı” başlıklı 10. maddesi de uygulamanın kapsamını belirlemiştir. Yönetmelik, İşletmecilere İnternetin Güvenli Kullanımına yönelik ücretsiz alternatif hizmeti sunma yükümlülüğü getirmiştir.

Bu hizmet kullanıcıların bireysel tercihlerine dayalı olarak talep etmeleri halinde alabilecekleri ve kullandıkları profiller arasında her an geçiş yapabilecekleri ve Güvenli İnternet Hizmeti dışına çıkabilecekleri bir işleyişi öngörmektedir.

Güvenli İnternet hizmetiyle aileler İnternetin olumsuz içeriklerinden olan pornografik sitelerden, uyuşturucu ticareti yapan sitelerden, şiddet içeren sitelerden, ırkçılık ve nefret suçları üzerine yayın yapan sitelerden, suç işlemeyi anlatan sitelerden, terör propagandası yapan sitelerden talebe bağlı ve ücretsiz olarak korunma imkanına kavuşmaktadır.

Mevcut filtreleme hizmetlerinden faydalanamayan kullanıcıların kolayca kullanabileceği bir hizmettir. Çocuk veya Aile profilden birini tercih eden kullanıcı karşılaştığı sorunu yine kullanmakta olduğu profil ile ilgili olarak geri bildirimde bulunma ve bu çerçevede tedbir alınmasını talep etme hakkına sahip olmaktadır.

Güvenli İnternet Hizmeti süreci ile 5651 sayılı Kanun çerçevesindeki erişim engelleme tedbir kararları birbirinden bağımsız konulardır. 2012 yılı Mayıs ayı verilerine göre Güvenli İnternet Hizmetini kullanan abone sayısı yaklaşık 1 milyon, bu aboneler arasında çocuk profilini kullananların oranı ise %14 olarak hesaplanmıştır [7].

VI. AVRUPA ÜLKELERİNDE GÜVENLİ İNTERNET

Güvenli internet hizmetinin etik anlayışın temel çerçevesini, Avrupa Konseyi Siber Suç Sözleşmesi'nin reşit olmayanlara ilişkin düzenlemesi, Çocukların Cinsel Sömürü ve İstismara Karşı Korunmasına Yönelik 201 sayılı Sözleşmesi'nin ilgili hükümleri ve BM Çocuk Haklarına Dair Sözleşme oluşturmaktadır. [8].

Dünyadaki İnternet içerik düzenlemelerine kıyasla Avrupa'da yapılan İnternet filtreleme, Avrupa'nın demokratik geleneği ve özgür ifade için verdiği mücadele göz önünde bulundurulduğunda dikkat çekici olmaktadır.

Filtreleme; devlet tarafından emredilen, ülke içerisinde barındırılan yasadışı içeriğin kaldırılması (uyar-kaldır), yurtdışında barındırılan içeriğe erişimin kısıtlanması, yasadışı içeriğe yönelik arama motorlarında sonuçların filtrelenmesi gibi çeşitli şekiller alabilmektedir. Birçok durumda, İnternet Servis Sağlayıcıları, arama motoru veya içerik sağlayıcı tarafından yapılan filtreleme "gönüllü" olarak adlandırılmakta ancak kamu otoritelerinin bu alanda yasama yapmaksızın oluşturdukları baskılar ile "zorunlu gönüllü" olarak sistem işletilmektedir.

Filtre edilen yasadışı içeriğin kapsamı genel olarak çocuk pornografisi, ırkçılık, nefreti ve terörü besleyen materyaller, telif hakları ve kumar sitelerinden oluşmaktadır. Bununla birlikte gerçek hayatta suç olan fiiller çevrimiçi ortamda da suç sayıldığı için başvurular üzerine mahkemelerce farklı konularda da filtreleme kararları alınabilmektedir.

AB düzeyinde, İnternet kullanımının izlenmesi konusunda İnternet Servis Sağlayıcıların genel bir yükümlülükleri olmadığı gibi, yasadışı içeriğin sorumluluğundan da korunmaktadırlar. Ancak, kendilerine bu tür içerik bildirildiğinde filtreleme yapmak zorundadırlar. Bu nedenle, üye ülkelerdeki filtrelemenin derecesi, hükümetlerin, kolluk kuvvetlerinin, sivil toplum kuruluşlarının, yasadışı içeriği tanıma ve rapor etme yönündeki kamuoyu bilincine göre değişmektedir.

Geçen on beş yılda, AB düzeyinde İnternet düzenleme konusunda ortak politikalar ve uygulamalar ortaya koyma çalışmaları devam etmektedir. Bunlar bölgesel ticaretin ve rekabetin gelişmesi, İnternet suçlarının ve terörizm ile mücadelenin bir gereği olarak görülmüştür. Diğer taraftan, yasadışı içerik hususunda İnternet Servis Sağlayıcıların sorumluluğu ve verilerin korunması hususunda yükümlülükleri öne çıkmıştır.

Avrupa'da bölgesel düzenlemeye ilişkin yaklaşım ilk olarak Avrupa Konseyi'nin, Komisyon'dan, 1 Nisan 1996'da "İnternetin hızlı gelişiminin neden olduğu problemlere ilişkin bir özet" istemesi ile başlamıştır.

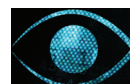
Bu talebe Komisyon, "İnternette Yasadışı ve Zararlı İçerikler" başlıklı bir rapor ve "Görsel-işitsel hizmetlerde küçüklerin ve insan onurunun korunması" başlıklı bir bilimsel çalışma ile cevap vermiştir. Bu belgelere dayanılarak, Ocak 1999 – Aralık 2002 arasında uygulamaya konulan "İnternetin Güvenli Kullanımının Desteklenmesi Harekat Planında (Action Plan on Promoting Safe Use of the Internet) ifadesini bulan "AB düzeyinde İnternetin kendi kendine düzenlenmesi için ortak çatı" taslağı hazırlanmıştır. Safer Internet Action Plan, düzenleme gerektirmeyen inisiyatifleri destekleyerek gerçekleştirmeyi amaçlamaktadır.

Bu kapsamda hem endüstriyi hem de internet kullanıcılarını, uygun, öz denetim sistemlerini uygulamak noktasında cesaretlendirmek, teknik çözümleri hareketlendirmek, aileleri ve öğretmenleri internet üzerinden zararlı ve yasadışı içeriklerle ilgili bilgilendirmek ve deneyimleri paylaşmak hedeflenmektedir.

Bu hedefler için dört hareket noktası belirlenmiştir.

1. Daha emniyetli bir ortam oluşturmak
 - Avrupa İhbar Merkezleri ağı oluşturmak (INHOPE)
 - Gönüllü düzenleme ve Prensipler Kararlarını (Code of Conduct) teşvik etmek
2. Filtreleme ve izleme programlarını geliştirmek
 - Filtreleme ve izlemenin faydalarını göstermek
 - İzleme programlarına dair uluslararası anlaşmaları kolaylaştırmak.
3. Bilinçlendirme Aktivitelerini cesaretlendirmek
 - Bilinçlendirme Aktiviteleri için yer sağlama
 - Geniş çaplı Bilinçlendirme Aktivitelerini cesaretlendirme
4. Destek faaliyetleri
 - Yasal suçlamalara değer vermek
 - Benzer uluslararası inisiyatiflerle işbirliği yapmak

İnternet Action Plan ilk defa tasarlandığı 1999 yılından bu güne kadar yasadışı ve zararlı içerikten korunmayı yasal ve düzenleyici bir çerçeveye oturtmaya yönelik bir dizi girişimler ve gelişmeler yaşanmıştır. Avrupa Konseyi'nin daha sonraki kararları ile Güvenli İnternet Programları uzatılmış ve halihazırda 2009-2013 yıllarını kapsayan (A multi-annual community programme on protecting children using the Internet and other communication technologies: İnternet ve Diğer İletişim Teknolojilerini Kullanan Çocukları Korumaya İlişkin Yıllara Sari Topluluk Programı) devam etmektedir.



A. İngiltere’de Güvenli İnternet Çalışmaları

Müstehcen içeriği düzenleme hareketi AB düzeyinden önce ülkeler düzeyinde ve İnternet Servis Sağlayıcılarca gönüllü uygulanacak filtre uygulamaları ile başlamıştır. Bu uygulamada en belirgin model, İngiltere’deki uygulama olmuştur. İngiltere’deki en büyük İnternet Servis Sağlayıcı olan BT, Haziran 2004 de İçişleri Bakanlığı işbirliği içerisinde “Cleanfeed” projesini uygulamaya koymuştur.

Projeye göre BT, dünyanın herhangi bir yerinde barındırılan çocuk istismarı (1978 tarihli Çocukların Korunması Kanununda belirtildiği şekliyle) görüntüsü taşıyan İnternet içeriğini filtrelemektedir. Bu içerikler, bir sivil toplum örgütü olan Internet Watch Foundation (IWF) tarafından bir liste halinde derlenmektedir. Üst düzey yöneticileri, emekli polis teşkilatı mensuplarından oluşan ve bünyesinde hukukçu barındırmayan IWF, Sexual Offences Act 2003’de yer alan düzenlemeler ve İngiltere’deki 52 polis teşkilatı ile imzalamış oldukları iyi niyet anlaşmaları sayesinde, çocukların cinsel istismarına yönelik yayınları inceleyip işlem sürecini tetikleyebilmektedir. IWF tarafından oluşturulan kara liste, İnternet Servis Sağlayıcılara, mobil operatörlere, içerik sağlayıcılara ve arama motorlarına verilmektedir. Bu içeriklere ulaşmak istenildiğinde bir hata mesajı ile karşılaşmaktadır.

İngiltere dahilinde barındırılan içerik için ise uyar kaldır yöntemi ile erişim sağlayıcılardan ve içerik sağlayıcılardan kaldırılması istenmektedir.

Her ne kadar bu sistemin esası “gönüllü” ise de İngiltere hükümeti tarafından 2007 yılının sonuna kadar bütün İnternet Servis Sağlayıcıların benzer bir sistem uygulaması istenmiştir.

İsveç, Norveç, Danimarka, Finlandiya ve İtalya gibi diğer ülkelerde de benzer programlar uygulanmaktadır.

B. Norveç’de Güvenli İnternet Çalışmaları

Eylül 2004’de, engelleme sistemi farklı bir türde gönüllü olarak Telenor İSS tarafından Norveç’te hayata geçirilmiştir. Kullanılan engelleme yöntemi de DNS zehirlenme olarak bilinen DNS kara listesidir. DNS kara listeyi kullanarak, belirli bir web sayfasını veya site içerisindeki alt alan sayfalarını engellemek mümkün değildir. Sitenin (domain) tamamına erişim engellenmektedir.

C. Danimarka’da Güvenli İnternet Çalışmaları

29 Ocak 2008 tarihinde Danimarka’da bir mahkeme tarafından Danimarka’daki İnternet servis sağlayıcılara popüler bir dosya paylaşım servisi olan Pirate Bay sitesi için erişim engelleme kararı gönderilmiştir. Kamuoyunda geniş çaplı tartışmalara neden olan bu kararın ardından Danimarka yargısı, söz konusu sitenin sahibi hakkında ceza davası açmıştır.

Danimarka Güvenli İnternet Merkezi, üç bağımsız organizasyonun işbirliği ile çalışmalarını yürütmektedir. Cyberhus isimli bir yardım hattı aracılığıyla çocuk ve gençler için danışmanlık hizmeti verilmektedir. Red Barnet isimli bir diğer hat üzerinden ise yasadışı içerik şikayetleri alınmaktadır.

2012 yılının ilk ayında 2 bin 522 adet ihbar alınmış ve ülke genelinde 506 İnternet sitesi hakkında yasal işlem başlatılmıştır.

D. Diğer Avrupa Ülkelerinde Güvenli İnternet Çalışmaları

İsveç, Finlandiya, Hollanda ve İsviçre gibi ülkelerde özellikle çocuk cinsel istismarı objelerine yönelik benzer tedbirler alınmış, bazı kara listeler hazırlanmış ve bazı ülkelerde DNS engelleme yoluna gidilmiştir.

İlk filtreleme çalışmaları çocuk pornosu gibi sınırlı alanlarda kalırken bu günlerde yetişkin pornografisi, online kumar, bahis, ırkçılık, kamu otoritelerine hakaret, saldırgan içerikler gibi alanlar için de filtreleme uygulamaları olduğu gözlenmektedir.

E. Avusturalya’da Güvenli İnternet Çalışmaları

Avrupa dışındaki ülkelerden Avusturalya’da 31 Mart 2010 tarihi itibarıyla, İnternet Servis Sağlayıcılar web sayfalarına erişimin engellenmesinde filtreleme sonucu düzeyini uygulamak için kanun veya başka bir yonteme bağlı kalmadan gerçekleştirmeye başlamışlardır. Bu İnternet Servis Sağlayıcılardan bazıları bu filtreleme işlemini birkaç yıldır gönüllü olarak uygulamaktadır.

Bütün bu uygulamalara rağmen 2007 Kasım ayında seçilen Avustralya Federal İşçi Hükümeti yapılanları yetersiz bulmuştur. Bu konuda hükümet, sonucu tabanlı filtreleme sistemi ile bir devlet kurumu tarafından hazırlanacak bir kara liste ile erişim engellenmesi yolunu tüm İnternet Servis Sağlayıcılara uygulamada konusunda bir plan oluşturmaktadır.

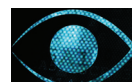
F. Kanada’da Güvenli İnternet Çalışmaları

Kanada’da 23 Kasım 2006 tarihinde 8 İnternet Servis Sağlayıcı çevrimiçi çocuk cinsel istismarına karşı yeni bir gönüllü girişim başlatmıştır. Bu tarihlerde engellenen site sayısının 500-800 arasında olduğu bildirilmiştir.

VII. NEFRET İFADELERİNE İLİŞKİN DÜZENLEMELER

AB genelinde politik karışıklık sebebiyle yapılmış olan bir filtreleme söz konusu olmamakla birlikte ulusal kimliği ve resmi kurumların saygınlığını korumaya yönelik filtrelemelere rastlanılmaktadır. 2002 yılında İsveç’te, İsveç Mahkemelerini şiddetle eleştiren ABD’de barındırılan 3 adet web sitesine erişimin engellenmesi istenmiş, tepki gösteren İnternet Servis Sağlayıcı yetkilileri hakkında yasal soruşturma başlatılmıştır.

Avrupa ülkeleri, etik politikalarını internete de uyarlayarak nefret ifadelerine karşı harekete geçmişlerdir. 2000 yılında Fransa’da, iki Anti Semitist STK tarafından mahkemeye taşınan bir davada, mahkeme Yahoo’yu, Nazi hatıraları ihtiva eden bir açık artırma sitesine erişim sağladığı için sorumlu tutmuş, ya bu siteye Fransa’dan erişimin imkansız kılması ya da ceza ile karşı karşıya kalınacağını bildirmiştir. Yahoo, davayı, Fransız yargı kararlarının ABD’de geçersiz olduğu iddiasıyla ABD bölge mahkemesine taşımış, mahkeme 2001



Kasım ayında Yahoo lehinde karar vermiş, devam eden süreçte Ocak 2006'da dava düşmüştür.

Benzer şekilde, yine Aralık 2000'de, Alman Federal Mahkemesi, Nazileri öven bir materyalin nerede barındırıldığına bakılmaksızın Alman kanunlarına göre sansürlenmesi gerektiğine karar vermiş, 2002 yılında 78 İnternet Servis Sağlayıcıya Neo-Nazi içerik taşıyan iki yabancı sitenin yayınlarının durdurulması talimatı verilmiştir.

Diğer Avrupa ülkelerinde de ırksal nefreti besleyen materyalleri yasaklayan mevzuat bulunmakta olup bu mevzuat, Avrupa Konseyi'nin Siber Suç Sözleşmesi ile senkronize edilmiştir. Bu duruma göre, yasadışı içerik söz konusu olduğunda, uyarı verilmesi durumunda, sitenin yurt içi veya dışında barındırıldığına göre, İnternet Servis Sağlayıcılar ya ilgili içeriği kaldıracak ya da siteyi kapatacaklardır.

AB üyesi ülkeler, İnternet ve diğer elektronik ağlar üzerinden medya veya diğer yayınlar tarafından yapılacak hakaret veya iftira durumunda uygulanacak basitleştirilmiş bir çatinın gerekliliğini ifade etmektedirler. Bu gereklilik Şubat 2007'de Avrupa Parlamentosu'nda tekrar ifade edilmiştir.

Ülkeler düzeyinde ise özellikle İngiltere'de, "Hakaret" in web sitesi kapatma nedeni oluşturması eleştirilere sebep olmaktadır.

VIII. FİKRİ HAKLARA İLİŞKİN DÜZENLEMELER

Fikri haklar konusunda ise iki direktif bulunmaktadır. Bu direktifler 9 Nisan 2001'de kabul edilmiş olan "Bilgi Toplumunda Telif Hakları ve İlgili Haklar" ve 8 Haziran 2000'de kabul edilmiş olan "2000/31/EC sayılı Elektronik Ticaret Direktifi"dir. Yasama konusunda ortak bir platform oluşturma çabaları, üye ülkelerin kültürel yapılarına ve mevcut mevzuatına verilen önemden ötürü yavaş yavaş yol izlemektedir.

Pek çok Avrupa ülkesi, telif hakları ihlallerine karşı, ABD'de uygulanan uyarı kaldır yöntemine benzer internet filtreleme yöntemleri kullanmaktadır. Avrupa'da telif hakları ihlallerine karşı İnternet Servis Sağlayıcılar ve arama motorları temsilcilerinin sorumlu tutularak gözaltına alındığı, para cezasına çarptırıldığı veya sitelerinin kapatıldığı örnekler bulunmaktadır.

IX. SONUÇ

Türkiye'de yürürlükte bulunan Güvenli İnternet uygulamaları, diğer ülkelerindeki güvenli İnternet çalışmalarıyla aynı etik çerçeveye sahiptir. ABD ve AB ülkeleri başta olmak üzere bütün devletlerde çocukların zararlı içeriklerden korunması amacıyla çeşitli düzenlemeler yapılmaktadır. Türkiye'de yürürlükte bulunan güvenli İnternet uygulamalarının ve güvenli İnternet hizmetinin isteğe bağlı ve ücretsiz oluşu, kullanım kolaylığı, aktif geribildirim kanallarının bulunması ve özellikle kullanıcıları banka hesap bilgileri ve şifreleri çalmaya yönelik zararlı İnternet sitelerinden uzak tutma konusundaki güçlü yönleri, sistemi emsallerinden daha avantajlı duruma getirmektedir. Ayrıca güvenli İnternet hizmeti kullanıcı sayısındaki artış trendi,

Güvenli İnternet kullanımı konusunda kullanıcılardaki bilinç düzeyinin gelişmekte olduğunun önemli bir göstergesidir.

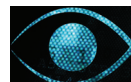
KAYNAKLAR

- [1] Merriam Webster's Dictionary & Thesaurus, 2008
- [2] Elektrik Mühendisliği Dergisi 442. Sayı Mayıs 2011
- [3] http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/55.html
- [4] http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php
- [5] Siber Güvenlik Kurulu, Ulaştırma Denizcilik ve Haberleşme Bakanlığı 3. Raporu.
- [6] Siber Güvenlik Kurulu, Milli Savunma Bakanlığı 3. Raporu
- [7] Çocuk ve Aile Profil Kriterleri Çalışma Kurulu 4. Raporu
- [8] Çocuk ve Aile Profil Kriterleri Çalışma Kurulu 1. Raporu

S. Özeren İTÜ'de Uçak Mühendisliği eğitimi alan Serhat Özeren, yüksek lisansını GYTE de elektronik bilim uzmanı olarak yapmaktadır. Techno Tower isimli konsorsiyumun, Erenet ve Eresoft'un kurucularından olan Özeren, aynı zamanda TEDER ve İnternet Geliştirme Kurulu'nun Başkanıdır.

1989 yılında iş hayatına başlayan Özeren 1993 yılında Erenet adı altında Bilgi Teknolojileri alanında faaliyet göstermeye başladı. 2002 yılında TEDER'i kuran Özeren o yıldan bu yana TEDER'in Yönetim Kurulu Başkanlığını yürütmektedir. TEDER Yönetim Kurulu Başkanı Serhat Özeren 12 Şubat 2008 tarihinde Devlet Planlama Teşkilatı'nda gerçekleştirilen seçimde e-Dönüşüm Türkiye Danışma Kurulu Başkanı seçilmiştir. Yine Telekomünikasyon sektörünün önde gelen derneklerinden TÜTED'in de Yönetim Kurulu Başkan Yardımcılığı görevini yürütmektedir. Aynı zamanda İTÜ Geliştirme Vakfı Okulları yönetim kurulu Başkanı ve İTÜ Geliştirme Vakfı mütevelli heyeti üyesidir.

MOBİSAD ve TUBİSAD üyesi olan Özeren, Türkiye Kurumsal Yönetim Derneği üyesi ve C5 Elektronik Yönetim Kurulu üyesi de yapmaktadır.



Mobil Yaşamda Siber Güvenlik Yaklaşımı

K. G. Gökce, E. Şahinaslan, S. Dincel

Özet— Bilişim teknolojilerinin ve özellikle internetin hayatımızdaki önemi her geçen gün artmaktadır. Sosyal ağların kullanımının yaygınlaşması, hemen hemen her şeyin internet üzerinden yapılması ve bilgiye kolay erişimin artık lüks değil bir ihtiyaç olması mobil cihazların kullanımını da hızla artırmıştır. Bilgiye tek bir tıkla erişilmesi ve mobil teknolojilerle birçok işlemin daha hızlı ve kolay gerçekleşmesi hem kullanıcıların beklentilerini değiştirmiş hem de kurumların hizmet anlayışının teknolojik olarak farklılaşmasına neden olmuştur. Klasik ve geleneksel yöntemlerin yerini artık globalleşen dünyada mobil cihazlar ve mobil uygulamalar almaya başlamıştır. Mobil cihazların internet erişimi için kullanımının hızla artmasına paralel olarak bu cihazları hedef alan siber saldırı ve tehditlerde artmaktadır.

Bu çalışmada giderek artan mobil yaşam sonucu ortaya çıkan siber güvenlik sorunları ve alınabilecek önlemler belirlenecektir.

Anahtar Kelimeler - mobil cihaz, mobil güvenlik, siber güvenlik, siber tehdit ve saldırı

Abstract— The importance of information technologies and especially the internet is increasing in our lives each and every day. The usage of mobile devices is increasing rapidly with the spread of social networks usage, almost everything done over the internet and the need of easy access to the information that is no longer be a luxury. One click access to information and many process done faster and easier with mobile technologies are the reason for change both user expectations and technological differentiation in institution's services offered. Classic and traditional method are replaced with mobile devices and mobile applications in globalizing world. The cyber attacks and threats for mobile devices targeted have been increasing with rapidly increasing usage of them for internet connection. In this study, the cyber security issues resulting from increasing mobile life and actions need to be taken are determined.

Key Words- cyber threat and attack, cyber security, mobile device, mobile security

I. GİRİŞ

Dijital ağların giderek yaygınlaşması ve birbiri ile bağlantılı hale gelmesiyle birlikte globalleşen dünyamızda teknoloji her alanda hızla yerini almaya devam etmektedir. Sanayiden sağlığa, kamu ve özel sektörde birçok kurum ve kuruluş hizmet ve ürünlerini internet üzerinden sunmaktadır. Sosyal ağların, bulut bilişimin, mobil cihazların kullanımının hızla artması, hayatımızda vazgeçilmez hale gelmesi bilgilere hızlı ve kolay erişimi sağlamaktadır. Günümüzde bu hızlı ve kolay iletişimi sağlama noktasında hem kullanıcılar hem de

kurumlar tarafından en yaygın kullanılan teknoloji mobil cihazlardır.

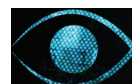
İstatistiklere bakıldığında, dünya nüfusunun yaklaşık %35'i internet kullanıcısı iken %26'sının ise sosyal ağlarda hesabı bulunmaktadır. Mobil cihaz kullanıcılarının sayısı ise oldukça yüksek olup %93'lük bir orana sahiptir. Mobil cihazların kullanım yaşı düşerken bir yandan da kişi başına düşen mobil cihaz sayısı artmaktadır. Türkiye'deki kullanım oranına bakıldığında ise nüfusun %84'ünün mobil cihaz kullanıcısı olduğu görülmektedir [2].

Bu gelişmelere bakarak bilişim hizmetlerinin hızla mobil cihazlara kaydığını söyleyebiliriz. İnternete erişim için daha birkaç yıl öncesine kadar ağırlıklı olarak kullanılmakta olan kişisel bilgisayarlara (dizüstü, masaüstü bilgisayar) olan eğilim giderek azalmaktadır. Tablo 1'deki verilere bakıldığında 3 yıl içinde mobil telefon sayısının, bilgisayar ve tablet sayısından oldukça fazla olduğu görülmektedir. 2015 yılında ise bilgisayar sayısında düşüş yaşanırken tablet ve mobil telefon sayısında artış olmaktadır. Bu da ilerleyen zaman içinde mobilleşmenin artacağını, geleneksel dizüstü ve masaüstü bilgisayar kullanımının ise azalacağını açıkça göstermektedir.

TABLO I
SEGMENTLERE GÖRE DÜNYA ÇAPINDAKİ CİHAZ SEVKİYATI
(MİLYON TÜRÜNDE) [1]

Cihaz Tipi	2013	2014	2015
Geleneksel Bilgisayarlar (Dizüstü, Masaüstü)	296.1	276.7	263.0
Tablet	195.4	270.7	349.1
Mobil Telefonlar	1,807.0	1,895.1	1,952.9
Diğer Ultramobil Cihazlar (Hybrid ve Clamshell)	21.1	37.2	62.0
Toplam	2,319.6	2,479.8	2,627.0

Mobil cihazlar hem sektörel olarak finastan sağlığa birçok alanda yaygın olarak kullanılmakta hem de uygulama olarak artırılmış gerçeklikten video konferans özelliğine kadar geniş çapta hizmet sunmaktadır. Bu özelliklerin yanında mobilitenin günlük yaşamımızda yaygın olarak kullanımı göz önüne alındığında kurum ve şirketlerin iç ve dış uygulamalarını, müşteriye sunduğu hizmetleri mobil platforma taşımaları kaçınılmaz olmuştur. Mobil cihaz ve uygulamalar vasıtası ile kişisel ve kurumsal verilere kolaylıkla erişilebiliyor olunması da bu cihazları çok çeşitli siber güvenlik tehditlerinin hedefi



haline getirmiştir. Mobil cihazlar bir yandan hayatı kolaylaştırırken diğer yandan da güvenlikle ilgili birçok kaygıyı da doğal olarak ortaya çıkarmaktadır [3].

İnternete erişim için mobil cihazların kullanımının artmasıyla birlikte mobil cihazlara ve cihazların kullanıcılarına yönelik siber saldırılarda artmaktadır. Kötü amaçlı mobil yazılım sayısında giderek yükselen bir artış olduğu bilinmektedir. Cihazlara yerleşen bu kötümcul yazılımlar, bilgi çalmak veya farklı siber saldırı yöntemleri ile kişi ve kurumlara büyük çapta zarar vermek, itibar kaybına uğratmak amacı ile kullanılmaktadır.

Sadece bilginin değil aynı zamanda dijital ortamların, elektrik, elektronik ve bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirlik bileşenlerinin korunması amacıyla oluşturan siber güvenlik yaklaşımının mobil cihazlar için neler sunduğu ilerleyen bölümlerde ayrıntılı olarak incelenecektir.

II. SİBER GÜVENLİK

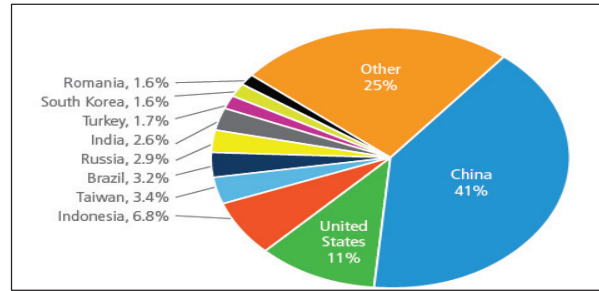
Siber güvenlik tanım olarak şu şekilde ifade edilmektedir; siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür [5].

Kurum, kuruluş ve kullanıcıların varlıklarının korunması konusunda bilgi güvenliğindeki 3 temel unsur olan gizlilik, bütünlük, erişilebilirlik bileşenlerine dikkat edilmelidir. Gizlilik, varlığı sadece iş ihtiyacı için ilgili olan kişilerin görmesi, kullanması anlamına gelmektedir. Yapılacak herhangi bir siber saldırıda bilginin yetkisiz kişilerin eline geçmesi varlığın gizliliğinin de ihlali anlamına gelmektedir. Bilginin bütünlüğünün korunmasındaki amaç ise herhangi bir bilişim sistemleri vasıtasıyla saklanan verinin yetkisiz kişiler tarafından değiştirilmesini veya bozulmasını önlemektir. Varlığın bilgi güvenliği bileşenlerinden biri olan erişilebilirlik ile de kast edilen bilgiye ihtiyaç duyulduğunda erişilebilmesidir [5]. Meydana gelebilecek olan siber saldırılar sonucu bilgiye, veriye olan erişim engellenebilmekte kişi, kurum ve kuruluşları zor duruma düşebilmektedir.

Siber saldırı çeşitleri çok fazla sayıda olmakla beraber sürekli yeni saldırı türlerinin meydana gelmesi de kaçınılmazdır. Siber saldırı türleri genel hatları ile 5 başlık altında toplanabilir[7]:

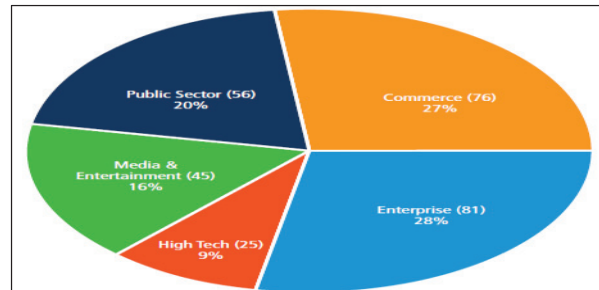
1. Servis Dışı Bırakma Saldırıları (DDOS, DOS)
2. Zararlı Yazılımlar
 - i) Bilgisayar Virüsleri
 - ii) Solucan
 - iii) Truva atı
 - iv) Tuş kaydedici
 - v) Reklam yazılımları
 - vi) Casus Yazılımlar
3. Oltalama
4. İstenmeyen E-Posta
5. Trafik Dinlenmesi

Siber güvenlik konusunda yeterli olmasada gün geçtikçe daha fazla çalışma yapılmaktadır. Kurumlar siber saldırıların hedefi olmamak ve bu saldırıları önceden tespit edebilmek için önemli yatırımlar yapmaktadırlar. Yine de dünya üzerinde önemli birçok özel kurum ve devlet kurumu çok ciddi siber saldırılara maruz kalabilmektedir. Aşağıdaki grafikte kaynak IP adresine göre kendisinden en fazla saldırı gerçekleşen ülkeler gösterilmiştir. Araştırmaya göre siber saldırıların %41'i Çin kaynaklı olup, Türkiye %1,7 ile 9.sırada yer almaktadır. Siber saldırılara ev sahipliği yapması açısından Türkiye'nin durumu maalesef pek parlak görünmemektedir [6].



Şekil 1. İnternet Saldırıların Kaynağı Olan Ülkelerin Yüzdesel Dağılımı [6]

Yine aynı araştırmaya göre, DDoS saldırıların sektörel olarak dağılımına bakıldığında ticaretten, medya&eğlence sektörüne birçok alanda yaygın olarak siber saldırıların yapıldığı görülebilmektedir. Grafiğe göre en fazla saldırı yatırım sektörüne düzenlenirken en az saldırılar ileri teknoloji ile ilgili çalışma yapan sektörlerle düzenlenmektedir [6].

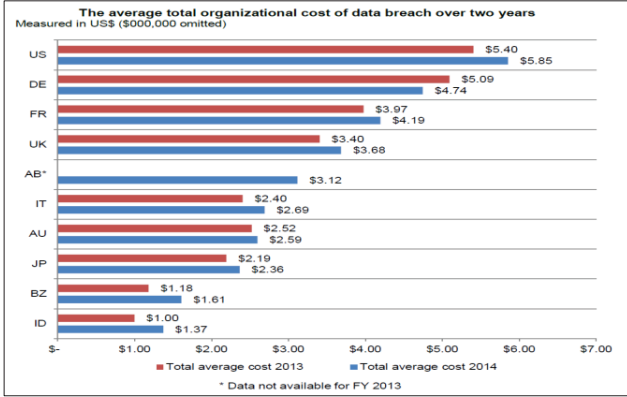


Şekil 2. 2014 Yılındaki DDOS Saldırıların Sektörlere Göre Dağılımı [6]

Kurumlarda siber güvenliği sağlamanın ilk şartı olarak en üstten en alta kadar tüm çalışanların bilgi güvenliği farkındalığının yüksek seviyede olması ve siber güvenliğinin sağlanabilmesi için zaman, kaynak, bütçe konusunda üst yönetimin gerekli desteği sağlaması gerekir. Özellikle günümüzde tüm sektörlerde teknolojinin, internet altyapısının yoğun olarak kullanılması her bir sektör ve kurumu siber saldırılar konusunda açık hedef haline getirmektedir.

Siber saldırıları diğer saldırılardan ayıran en önemli fark, siber silahların ucuz maliyetlerle tahmin edilemeyecek boyutlarda zararlara yol açmasıdır. Hacker olarak adlandırılan siber savaşçılar bir bilgisayar ve bir e-posta ile hedefteki sistemi rahatlıkla ele geçirebilmektedir. Siber saldırıları tespit etmek ve sistemi eski haline döndürmenin maliyeti ise oldukça yüksektir.

Şekil 3' de belirtildiği üzere 2014 yılında yapılan bir araştırmaya göre 10 farklı ülkede yer alan şirketler için siber saldırı sonucu oluşan veri kayıplarının ortalama toplam organizasyonel maliyeti aşağıda gösterilmiştir. 5.85 milyon dolar ile Amerika birinci sırayı alırken, 4.74 milyon dolarlık bir maliyetle Almanya takip etmektedir. En az ortalama olarak toplam maliyete sahip olan şirketler ise sırasıyla Brezilya ve Hindistan ülkelerine aittir. Maliyetlerin yüksek olması siber güvenlik konusunda alınması gereken önlemlerin artırılması gerektiğini açıkça göstermektedir.



Şekil 3. İki Yıl İçindeki Ortalama Toplam Organizasyonel Veri İhlal Maliyetleri [8]

III. MOBİL GÜVENLİK TEHDİTLERİ

Mobilleşme bilgi teknolojilerinin gelişmesiyle birlikte giderek yaygınlaşmış, kurumsal hizmet ve süreçleri kolaylaştırması ile de her alanda hızla yayılmaya başlamıştır.

Mobil çözümlerden daha iyi bir şekilde yararlanabilmek için son zamanlarda birçok inovasyon ortaya çıkmıştır. Donanım alanında Apple'ın iPad cihazları, işletim sistemlerinde Google'ın Android yazılımı, sosyal iletişim alanında Skype gibi yazılımlar ve 4G, LTE gibi ağ teknolojileri bu inovatif teknolojik gelişimlere örnek olarak verilebilir. [9]

Kişiler ve kurumlar sürekli gelişen ve değişen mobil teknolojilere hızla adapte olup mobil cihazların kullanımı yaygınlaşırken mobil cihazlardaki güvenlik riskleri kişiler ve kurumların en büyük endişeleri arasında yerini almaktadır.

Mobil cihazlardaki Bluetooth, kızılötesi, Wi-Fi gibi kolay erişilebilirliği sağlayan birçok özellik, saldırganlar için mobil cihazları masaüstü ve dizüstü bilgisayarlara göre daha cazip hale getirmiştir. Mobil cihazlara ait aşağıdaki özelliklerde herhangi bir açıklık olması durumunda mobil cihazlar siber saldırıya maruz kalabilir: [10]

- SMS
- Wi-Fi
- Bluetooth
- Kızılötesi (Infra-red)
- USB
- Ağ tarayıcı

- Email sunucusu
- Third party applications
- İşletim sistemi açıklıkları
- Fiziksel erişim

Mobil cihazlar küçük boyutlarına rağmen birçok özelliği içinde barındırdığından bazı fiziksel ya da teknolojik açıklıklara sahiptirler.

A. Fiziksel Mobil Açıklıklar

Mobil cihazların boyut olarak ufak olması ve kolay taşınabilmesi, cihazların kolaylıkla çalışmasına ya da kaybolmasına sebebiyet vermektedir [4,8]. Böyle bir durumun meydana gelmesi cihaz içindeki kritik verileri tehlikeye atmaktadır. Özellikle böyle bir durumda oluşabilecek zararı en az seviyeye indirebilmek için iş amaçlı kullanılan kurumsal telefonların uzaktan yönetilebiliyor olması, otorizasyon ve şifreleme kurallarına dikkat edilmesi önemlidir.

Telefonların kimlik numarası niteliğinde olan IMEI numarası biliniyor ise herhangi bir sebeple çalınan ya da kaybolan telefon kolaylıkla açılabilir. IMEI numaralarının güvenli bir şekilde güçlü erişim kontrol mekanizmaları ile saklanması ise mobil operatörlerin sorumluluğundadır [11].

Ayrıca dışarıdayken örneğin bir yerde sıra beklerken arkamızda bekleyen kişi telefona girdiğimiz şifreyi ya da telefonda baktığımız gizli içerikteki bilgileri rahatlıkla görebilir [4]. Böyle bir zafiyeti engellemenin tek yolu, kullanıcıların farkındalık seviyesini artırmak, onları bilgilerin korunması noktasında bilinçlendirmektir.

B. Teknolojik Mobil Açıklıklar

Telefonun teknolojik özellikleri (SMS, Bluetooth, GPS gibi) kullanılarak yapılabilecek saldırılara örnek olarak bahsederek, hacker telefonun

SMS, E-mail: Saldırgan, SMS veya e-mail özelliğini kullanarak mesajları kendine yönlendirebilir, kritik bir bilgiyi öğrenmek için mesajları, e-mail hesabını inceleyebilir [4,10]

İşletim sistemi zafiyetleri: Mobil cihazların işletim sistemindeki açıklıklar konuşmaların saldırgan tarafından dinlenmesine, kaydedilmesine neden olabilmektedir [4, 10].

Lokasyon bilgisi: Günümüzde birçok akıllı cihaz GPS özelliği sayesinde lokasyon bilgisini ulaşılabilir hale getirmektedir [8]. Hacker denilen kişiler bu bilgiyi kullanarak cihazın lokasyon bilgisini rahatlıkla öğrenebilmekte, başka kaynaklardan elde ettiği bilgi ile ilişkilendirebilmektedir [4].

C. Mobil Uygulama Açıklıkları

Farklı amaçlar için kullanılan birçok uygulama kolaylıkla erişilebilir amaçla mobil cihaz üzerine kullanıcılar tarafından indirilmektedir. Bu uygulamaların çoğu çok fazla sayıda güvenlik riski ve mobil ajan içermektedir [4,11]. Bazı işletim sistemleri uygulamaları mağazalarında uygulamaları yayınlamadan önce güvenlik açıklıklarını kontrol ederken bazılarında ise böyle bir kontrol bulunmamaktadır. Bu durumda kullanıcıların uygulamaları mobil cihazından indirirken daha dikkatli olması gerekmektedir.

D. Güvenli Olmayan Ağların Kullanılması

Mobil cihazlar üzerinden internet erişimi için güvenilir olmayan ağların kullanılması birçok saldırıya davetiye çıkarmaktadır. Mobil cihazlar ile kablosuz erişimi sağlayan cihaz arasındaki verilerin dinlenebilmesi saldırganlar için oldukça kolay olmaktadır [4,11].

VPN gibi güçlü şifreleme teknolojileri kullanılarak güvenilmeyen ağların sebep olabileceği riskler azaltılarak, verinin gizlilik, bütünlük, erişilebilirlik bileşenlerinin korunması sağlanabilir [4].

E. Sosyal Medyanın Kullanılması

Sosyal medya erişim ve kullanım açısından pek çok güvenlik riski içermektedir. Özellikle mobil cihazlar üzerinden sosyal medya uygulamalarına erişildiğinde genel olarak cihazların güvenlik ayarlarının kullanıcıların kişisel verilerini paylaşmaya yönelik olarak ayarlandığı bilinmektedir [12]. Sosyal medya üzerinde gezinirken ya da herhangi bir paylaşımda bulunulurken Wi-fi ve GPS aracılığı ile konum bilgileri kolaylıkla başkaları ile paylaşılabilir. Ayrıca sosyal ağ uygulamaları mobil cihazın üzerinde sürekli olarak açık bulunduğundan bazı zararlı uygulamalar sosyal ağlardaki verilerinizi kolaylıkla ele geçirebilmektedir [13].

Mobil cihazlarda sosyal medya güvenliğinin sağlanabilmesi için yapılması gereken en önemli 2 madde şu şekilde sıralanabilir [10]:

- Wi-Fi, GPS, Bluetooth, hücresel veri gibi fonksiyonlar sadece ihtiyaç anında aktif hale getirilip sonrasında pasif edilmeli. Böylece mobil cihazımızı sürekli bir hedef haline getirmekten kurtarabiliriz.
- Mobil cihaz üzerine indirilen sosyal ağ uygulamaları konum bilgisi ya da fotoğraflarımıza sürekli erişmek istediğinde izin verilmemeli, yine ihtiyaç olduğunda aktif hale getirilmelidir.

F. Zararlı Yazılımlar

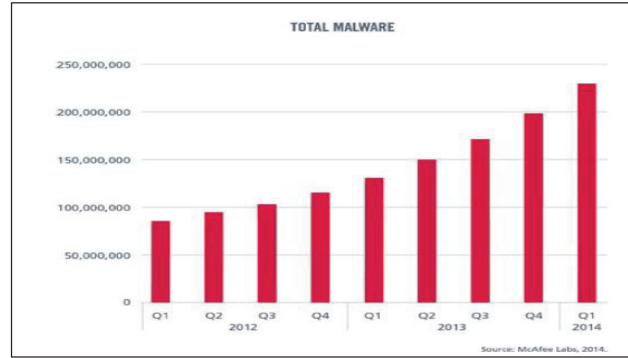
İnternette indirilen dosyalar, mesajlaşma servisleri, bluetooth gibi iletişim kaynakları mobil cihazlara zararlı yazılım ya da virüs bulaşma riskini artırmaktadır [11].

McAfee Labs tarafından yapılan araştırmaya göre Şekil 4'teki grafiğe bakıldığında 2012'den 2014'e kadarki süreçte zararlı mobil yazılımların sayısı giderek artmıştır. Bu artıştaki en önemli etmenler arasında mobil cihaz kullanım sayısının artması ve internete erişim için kablosuz erişimin kullanılmasının yaygınlaşması sayılabilir [14].

Zararlı yazılımların cihazlara bulaşması durumunda yapılabilecek potansiyel saldırılar aşağıdaki şekilde sıralanabilir [15]:

- Yerine geçme: Zararlı yazılım sayesinde cihaz üzerinde adeta uzak masa üstü erişimi sağlanarak mobil cihaz üzerinden bilgiler alınabilir.
- Veri akışını kesme: Cihaza doğru olan her türlü veri akışı kesilebilir.

- Bilgi hırsızlığı: Cihaza yerleşen zararlı yazılım tüm bilgileri toplayarak cihazdan dışarı gönderebilir.
- Arka kapı (Backdoor): Zararlı yazılım cihazda korunmasız bir arka kapı oluşturarak diğer ataklara açık hale getirir.
- Servisi kötüye kullanma: Cihaza yerleşmiş yazılım, servisi çok amaçlı kullanarak, kullanıcının fazla ücret ödemesine yol açar.
- Erişilebilirlik: Cihaz üzerindeki zararlı yazılım diğer cihazlarla etkileşimi sağlayarak farklı verilere erişim sağlayabilir.
- Şebekeye giriş: Cihaz üzerindeki zararlı yazılım farklı bir kimlik doğrulamaya gerek kalmaksızın şebekeye erişebilir.
- Solucan (Wormable): Cihaz üzerindeki zararlı yazılım, son derece rahat çoğalan solucanlar olabilir ve diğer cihazlara doğru hızla yayılır.



Şekil 4. 2012 Yılından 2014 Yılı'nın İlk Çeyreğine Kadar Mobil Zararlı Yazılımların Toplam Sayısı [14]

G. Kurumlar için Yeni Endişe: Kendi Cihazını Getir (BYOD (Bring Your Own Device))

Mobil cihazların kullanımının artmasıyla birlikte iş hayatında da yeni ihtiyaçlar ortaya çıkmaktadır. Eskiden mobil cihazlar kurumlarda sadece e-maillere erişme, acil çağrılara cevap verme gibi temel iş ihtiyaçları için kullanılmaktaydı. Fakat günümüzde mobil cihazların kullanımının artması ve kolay taşınabilmesi ile birlikte bu cihazların kişisel bilgisayarların sunduğu neredeyse tüm hizmetleri sağlaması akıllı telefonların ve tabletlerin kurumsal amaçlı kullanım isteğini artırmaktadır. Çalışanların kurum tarafından verilen yeni bir cihazı kullanmak yerine kendi akıllı cihazını aynı zamanda iş için kullanmak istemesi "Kendi Cihazını Getir (BYOD)" konseptini gündeme getirmiştir [16]. "Kendi Cihazını Getir" yeni bir teknoloji değildir, sadece bir kurum politikası olarak ifade edilebilir. Bazı şirketler bunu yasaklama yoluna giderken, bazıları ise veri güvenliği politikası izleyerek çalışanların kendi cihazlarıyla kurumsal ağa bağlanmasına izin veriyor.

Bu uygulamanın avantajları olduğu gibi pek çok güvenlik riski de bulunmaktadır. En büyük risk, her türlü saldırıya açık olan

mobil cihazlar kurumsal ağına içine dahil edildiğinde kurumsal verilerin güvenliğinin sağlanmasının çok kolay olmamasıdır.

Erişim politikalarının tüm rol ve sorumluluklar için açıkça belirlenmesi, kurumsal veri güvenliğinin korunması konusunda çalışanların farkındalığının artırılması, antivirüs, VPN gibi teknik olarak alınması gereken önlemlerin alınması, “Kendi cihazını getir” uygulamasının başarılı bir şekilde hayata geçmesi için kurumların alması gereken güvenlik önlemleri arasında sıralanabilir. Ayrıca kurumlar mobil cihazları uzaktan kontrol edebilmek ve çalınma, kaybolma durumlarında cihaza uzaktan müdahale ederek verilere erişilmesini önleyebilmek için Mobile Device Management (MDM) teknolojilerinden de yararlanabilirler. Aynı zamanda MDM sayesinde mobil cihazlara sadece güvenilirliğinden emin olunan uygulamaların yüklenmesine izin verilmektedir. Böylece kurumlar hem kendi yerel ağlarını ve verilerini hem de çalışanlarının ve müşterilerinin verilerini korumuş olurlar.

H. Mobil İletişim Operatörlerinden Kaynaklanan Kısıtlar

Mobil operatörler hücresel mobil telefon haberleşmesi için gerekli sistemi sağlarlar. Abonelere ait son derece kritik verilerin iletimi, saklanması mobil operatörlerin sorumluluğunda olduğu için operatörler birçok ulusal ve uluslararası kuruluş tarafından iletişim güvenliğinin sağlanması konusunda düzenleme ve denetimlere tabi tutulmaktadır. Mobil operatörlerden kaynaklanabilecek muhtemel tehditler aşağıdaki şekilde sıralanabilir [17]:

- Şebeke kaynaklarının ve verinin tahrip edilmesi
- Suistimal, sisteme izinsiz giriş ve müdahale
- Hırsızlık, veri veya diğer kaynakların çalınması veya kaybı
- Yetkisiz erişim
- Şebekelere erişimin engellenmesi, kesinti

Yukarıda bahsedilen zaafiyetlerin önüne geçmek için operatörler, kişisel verilerin işlenmesine, saklanmasına ve iletimine ilişkin güvenlik gerekliliklerini belirlemeli ve sundukları hizmetin güvenilirliğini sağlanmaya yönelik tedbirleri almalıdır [20].

IV. MOBİL GÜVENLİK İÇİN YAPILMASI GEREKENLER

Kullanıcıların alması gereken önlemleri ve kurumların mobil güvenlik konusunda izlemesi gereken politikalar ayrı başlıklar altında incelenecektir.

A. Kullanıcıların Dikkat Etmesi Gereken Kurallar

Kişisel mobil cihazların siber tehditlere karşı korunabilmesi için yapılması gerekenler aşağıdaki gibi sıralanabilir [17]:

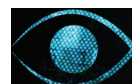
- Mobil cihaza erişebilmek ve kullanmak için şifre oluşturulmalı, cihaz belirli bir süre kullanılmadığı durumlarda otomatik olarak kilitlenecek şekilde limit süresi ayarlanmalı. Bu şekilde yetkisiz kişilerin mobil cihazdaki kişisel verilere erişimi engellenebilir.

- Cihazı herhangi bir saldırı ve bozulmadan koruyabilmek için işletim sisteminin ve yüklenen uygulamalara ait yazılımlar güncel tutulmalı.
- Şüpheli e-mail ya da sms yoluyla gelen linklere tıklanmamalı. Bu linkler zararlı yazılımların cihaza yüklenmesine sebep olabilir.
- Web sitelerinde telefon numarası istenildiğinde ilgili kurum tarafından istenildiğine ve güvenilir olarak saklanacağına emin olunmadığı sürece telefon numarası yazılmamalı. Saldırganlar kullandıkları zararlı yazılımlar sayesinde telefon numaralarını web sitelerinden toplayarak bu numaralara karşı saldırı düzenleyebilmektedir.
- Truva atı ya da zararlı kod içeren uygulamalardan korunabilmek için mobil cihaz üzerine güvenilirliğine emin olunan uygulamalar yüklenmelidir.
- Mobil cihazlar için özel geliştirilmiş antivirüsler kullanılarak zararlı yazılımlara karşı mobil cihazlardaki verilerin korunması sağlanabilir.
- Wi-fi, bluetooth, kızılötesi gibi fonksiyonlar sadece ihtiyaç anında aktif hale getirilmeli. Böylelikle bu özellikler kullanılarak yapılan saldırılardan korunma sağlanabilir.
- Güvenilmeyen kablosuz ağlarla internete bağlanılmamalı.
- Cihazda bluetooth teknolojisinin kullanılması halinde açık ve keşfedilir özelliği devre dışı bırakılmamalı. Bu özellik kullanılarak yapılabilecek saldırılar bu şekilde engellenebilir.
- Sosyal ağ uygulamaları kullanılırken dikkatli olunmalı, bilinmeyen uygulamaların konum bilgisine ve fotoğraflara erişimine izin verilmemeli.
- Cihazınızda jailbreak (yazılım kırma) veya root (sistem tüm yetkilerini kullanacak hale getirme) özellikleri aktif hale getirildiğinde normalde izin verilmeyen zararlı yazılım içeren uygulamalarda dahil olmak üzere istenilen programları yükleme, silme gibi birçok hakka sahip olmaktadır. Özellikle yetkin olmayan, bilgi güvenliği konusunda farkındalığı düşük kullanıcılar tarafından bu özelliklerin aktif hale getirilmesi kötü niyetli yazılımlara karşı korumayı ortadan kaldırmaktadır.
- Cihazınızın çalınma ve kaybolmalara karşı Find My Phone ya da benzer ayarlamalar yapılmalı. Böylelikle cihazın harita üzerinde konumu ve çalınma/kaybolma durumu kolaylıkla öğrenilebilir.
- Çalınma, yağmalanma, kaybolma veya her ne suretle olursa olsun, mobil cihazların sahibinin rızası dışında elden çıkması durumlarında tüketiciler telefonla Bilgi Teknolojileri ve İletişim Kurumunun Bilgi ve İhbar Merkezine ihbarda bulunarak cihazlarının elektronik haberleşme şebekesinden hizmet almasını engellenmesini sağlayabilir [19].

B. Kurumların Yapması Gerekenler

Kurumsal verilere kişisel ya da kurum cihazıyla erişilmesine izin verildiğinde iç ve dış tehditlere karşı alınması gereken önlemler aşağıdaki gibi sıralanabilir:

- Mobil cihaz ve uygulamalara erişim için kurum şifre



politikaları baz alınarak güçlü şifre kullanımı sağlanmalı, kullanıcıların düzenli aralıklarla şifre değiştirmesini sağlamak için gerekli ayarlamalar yapılmalıdır.

- İlgili tüm birimlerin görüşü alınarak mobil cihazlar vasıtası ile erişilen kurumsal veriler ve uygulamalar iş gereksinimleri doğrultusunda belirlenmeli. Böylece yetkisiz kişilerin ihtiyacı olmayan veriye erişmesi engellenebilir.
- Her bir rol ve sorumluluk için erişim yetkileri, kullanıcı hakları açıkça belirlenmeli ve yazılı hale getirilmelidir.
- Mobil cihazların taşınabilirlik özelliği sebebiyle kurum dışında kullanılması durumunda birçok güvenlik zaafiyeti oluşabilmektedir. Kullanıcı kaynaklı zaafiyetleri azaltabilmek için mobil cihaz kullanıcılarının uyması gereken kurallar belirlenmelidir.
- Mobil cihaz vasıtası ile kurumsal verilere erişen çalışanlara gizlilik ve güvenlik sözleşmesi imzalatılarak gizli verilerin yetkisiz bir şekilde kullanılması engellenebilir.
- Kullanıcıların güvenlik konusundaki farkındalığını yükseltmek amacıyla düzenli olarak eğitimler verilmelidir. Bu sayede çalışanların dikkatsizliği ya da bilgi eksikliğinden kaynaklanan veri kaybının önlenmesi sağlanabilir.
- Mobil cihaz ve uygulamalara erişim ile ilgili kurallar belirlenirken sadece BT birimlerinin değil, kurumdaki ilgili tüm birimlerin görüşü alınmalıdır.
- Kötü niyetli yazılımların kurum verilerine ve kurum ağına vereceği zararı önleyebilmek için mobil araçlar üzerine üçüncü parti imzasız, güvenilir olmayan yazılımların yüklenmesine izin verilmemelidir.
- Zararlı yazılım ve virüsler mobil cihazlara bulaşarak kurumsal verilerin gizlilik, bütünlük, erişilebilirlik bileşenlerini bozabilir. Bu durumu önleyebilmek için uygun antivirüs yazılımları kullanılmalı ve sürekli güncellenmelidir.
- Mobil cihazın yeni çıkan açıklıklara karşı korunabilmesi için işletim sisteminin düzenli olarak güncellendiğinden emin olunmalı.
- Mobil cihaz kurum ağına bağlanırken iletişim güvenliğinin sağlanması adına kurum ağı ile operatör ağı arasında sanal özel ağ oluşturulabilir ya da uygulamaya erişmeden önce mobil cihaz kurum ağına sanal özel ağ ile bağlanabilir [11].
- Mobil cihazlar vasıtasıyla erişilen kurumsal uygulamalarda yapılan işlemlerin denetim izleri alınmalı, kritik işlem ve uygulamalara ait izler düzenli olarak raporlanıp incelenmelidir.
- Cihazların kaybolması, çalınması durumunda ya da verilerin güvenliğinin tehlikeye girdiği durumlarda cihaza kolaylıkla müdahale edebilmek için merkezi bir yönetim konsolu uygulanmalıdır. Böylece lokasyon izleme, veri temizleme, şifre/PIN değiştirme ve güçlü kullanıcı yetkilendirmesi gibi fonksiyonlar uzaktan kontrollü bir şekilde yapılabilir.

V. SONUÇ

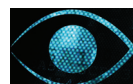
Hemen hemen herkesin bir veya daha fazla mobil cihazının olduğu ve bu cihazların insanların hayatında vazgeçilmez bir parça haline dönüştüğü bilinmektedir. Artık çoğumuz en kritik bilgilerimizi kişisel bilgisayarlardan çok, akıllı telefon ve tabletlerde taşımaktayız. Sadece kişisel veriler değil en mahrem kurumsal verilere bile mobil cihazlar vasıtasıyla tek bir tıkla kolaylıkla erişebilmemiz alınması gereken güvenlik önlemleri için daha fazla araştırma yapılması gerektiğini açıkça göstermektedir.

Mobil cihazların kolay taşınabilme, erişilebilirlik özelliği ve içerdiği bazı teknolojilerin doğru kullanılmadığı takdirde bir takım güvenlik zaafiyetlerine sebebiyet vermesi mobil cihazları saldırganlar için hedef haline getirmiştir. Gittikçe daha fazla zarara sebep olan siber tehditler mobil cihazları bilgisayarlardan bile daha yüksek oranda etkilenmektedir [14].

Bilinen tüm güvenlik açıklıklarına rağmen kişi ve kurumlar mobil cihazların sağladığı avantajlardan dolayı bu cihazları kullanmaktan vazgeçmemektedir. Mobil cihazları etkileyen siber saldırıların sayısının artması kullanıcıların güvenlik konusundaki farkındalığını da artırmasına sebep olmuştur. Vazgeçilemeyen ve gittikçe hayatımıza daha fazla dahil olan cihazları güvenli bir şekilde kullanabilmek için tüm güvenlik riskleri, iç ve dış tehditler, kullanıcı dikkatsizlikleri belirlenip her bir risk için ayrı bir aksiyon ve önlem planı oluşturulmalıdır.

Kullanıcı ve kurumların alması gereken güvenlik önlemlerinin yanı sıra mobil iletişim operatörlerine de mobil güvenliğin sağlanması konusunda çok büyük görevler düşmektedir. Veri, kurumsal ağdan çıktıktan sonra kontrol operatörlerin sorumluluğunda olduğundan erişim ve iletişim altyapı hizmetleri ve uygulamalara ait tüm risk ve tehditler operatörler tarafından belirlenmeli, gerekli kontroller sağlanmalıdır. Haberleşme güvenliğinin sağlanması, verinin gizlilik, bütünlük, erişilebilirlik bileşenlerinin tam olarak korunduğunun garanti edilmesi, erişim kontrolü ve kimlik denetimi gibi tedbirlerin alınması oluşabilecek güvenlik açıklıklarının önüne geçilmesi için hayati önem arz etmektedir. Abone ve kullanıcılara ait iletişim bilgileri, trafik verileri, konum bilgisi gibi gizli verilerin saklanması, korunması, imhası ile ilgili kurallar AB Mevzuatı Veri Koruma Direktifi'nde de açıkça belirtilmiştir. Veri Koruma Direktifi'ne göre operatörler tarafından saklanan verilerin kaybolması, değiştirilmesi, depolanması, işlenmesi, ifşa edilmesi, belirtilen verilere erişilmesine karşı uygun teknik ve idari tedbirler alınması gerektiği belirtilmiştir. Yine mobil operatörlerin düzenli denetimi ve teftişi ile ilgili çalışmalar ülkemizde Bilgi Teknolojileri Kurumu kontrolünde gerçekleştirilmektedir [21].

Mobilleşmenin her alanda yaygınlaşmasıyla birlikte pazarlama stratejisi olarak mobil iletişimin kullanılması işletmeciler için kaçınılmaz olmuştur. SMS gibi haberleşme vasıtaları



sayesinde bir anda çok sayıda müşteriye ulaşabilme imkanı çok cazip görülmekle birlikte müşterileri rahatsız etmemek ve istemedikleri sürece onlara mesaj yollamamak gerekmektedir. Bunların yanı sıra milyonlarca kişinin iletişim bilgilerini elinde bulunduran mobil operatörlerin bu bilgileri müşterinin bilgisi ve izni olmadan kullanması, üçüncü kişilere ifşa etmesi ve bu yollarla haksız kazanç elde etmesi ise hukuka ve dürüstlük kurallarına aykırıdır [21].

Son zamanlarda ülkemizde ve dünya genelinde yaygın olarak görülen telefon dinlemelerinin ifşasında veri gizliliğini sağlamakla yükümlü olan operatörlerin ve diğer kurumların görevlerini yerine getirmediği ve gizli olarak korumaları gereken bilgilerin dışarı sızmasına sebebiyet verdikleri ortaya çıkmıştır. Yasal olmayan yollarla usulsuz bir şekilde yapılan telefon dinlemeleri ile ilgili operatörlerin herhangi bir zaafiyetinin olup olmadığının tespiti ile ilgili soruşturmaların açılmasındaki sorumluluk ülkemizde Bilgi Teknolojileri Kurumu'na aittir. Kurallara uymayan ve zaafiyete sebebiyet veren mobil operatörlerin cezalandırılması ile ilgili örnekler ise geçmiş zamanlarda meydana gelmiştir [21].

Bazı özel yasal takip durumlarında ilgili yargı kararları ve yetkilendirmeler ile telefon dinleme hakkına sahip olan istihbarat birimlerinin yetkileri de belli kurallar çerçevesinde belirlenmiş olup, yetki sorumsuzluğu gibi bir durum söz konusu değildir. Ülkemizde Milli İstihbarat Birimi görev ve sorumluluklarının dışında hareket eden kişilerle ilgili olarak konuyu açıkça şu şekilde ifade etmiştir: "Teknik takip sırasında elde ettiği bilgileri şahsi amaçlarla kullanmaya kalkan veya teşkilatın dışına çıkaran personel teşkilat yasa gereği devlet sırrını ifşa etmekten yargılanır ve yapılabilecek suistimallere karşı kurulan kontrol sistemi sayesinde bilgi sızdıran mutlaka yakalanır." [22]. Yine Alman Federal Anayasa Mahkemesi, istihbarat birimlerinin teknik araçlar yoluyla yaptıkları yetkisiz erişimleri ve dinlemeleri yasaklamıştır [21]. Ulusal ve uluslararası birçok yasa ile kişilere ait verilerin korunması düzenlenmiş olsa bile hem yetkisini farklı amaçlar için kullanan personeller ve kurumlar hem de saldırganlar tarafından giderek artan teknolojik imkanlar kullanılarak kullanıcıların dinlemesinin ve bunun servis edilmesinin önüne geçmek maalesef çok kolay görünmüyor. Özellikle son zamanlarda Wikileaks belgelerinin ortaya çıkması ve birçok NATO ülkesinin birbirini dinlediği gerçeği siber güvenlikle ilgili uluslararası geçerliliği olan, daha ciddi ve yaptırımı yüksek önlemler alınması gerektiğinin bir zorunluluk olduğunu açıkça göstermiştir.

Mobil yaşamda siber güvenliğin sağlanabilmesi için ilgili tüm tarafların hem hizmet alan hem hizmet veren kurumlarla birlikte denetleyici, düzenleyici kurumların koordineli olarak çalışması önemlidir. Mobil güvenlikle ilgili yetki ve sınırların net olarak çizilmesi, zaafiyet durumlarındaki ceza ve yaptırımların artırılması da oluşması muhtemel siber saldırılar için caydırıcı olabilir.

Bu çalışmada kişilerin mobil cihazlar üzerinde yer alan hem kendilerine ait özel bilgileri hem de kurumlara ait bilgileri koruması konusunda yapması gerekenlerden bahsedildi.

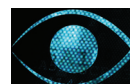
Ayrıca mobil cihazlar vasıtası ile kurumsal verilere erişilmesine izin veren kurumların alması gereken önlemler ve yapılması gereken kontroller açıkça belirtilmiştir.

KAYNAKÇA

- [1] <http://www.gartner.com/newsroom/id/2692318>
- [2] We Are Social, "Global Digital Statistics 2014"
- [3] Hekim, H ve Başbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4, 135-158
- [4] National Institute of Standards and Technology. "Guidelines for Managing the Security of Mobile Devices in the Enterprise (SP 800-124)." <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
- [5] http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php
- [6] Akamai, "Akamai's State of The Internet Q1 2014 Report" http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114
- [7] <http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf>
- [8] Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis" <http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF>
- [9] Kietzmann, J., Plangger, K., Eaton, B., Heiligenberg, K., Pitt, L., & Berthon, P. (2013). Mobility at work: A typology of mobile communities of practice and contextual ambidexterity. The Journal of Strategic Information Systems, 22(4), 282-297.
- [10] Verizon, "Mobile devices and Organizational Security Risk", http://www.verizonenterprise.com/resources/whitepapers/wp_mobile-devices-and-organizational-security-risk_en_xg.pdf
- [11] Birliği, k. B. İ. M. Y. Mobil Uygulamalarda Güvenlik.
- [12] Tunca, Sosyal ağlarda güvenlik - 1: Akıllı telefon ve tablet güvenliği, 6 Mayıs 2012. [Çevrimiçi]. Available: <http://dijitalekojoloji.blogspot.com/2012/05/sosyal-aglarda-guvenlik-1-akll-telefon.html>. [Ağustos'ta erişilmiştir].
- [13] Yıldırım, N., & Varol, A. (2013). Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması (Security On Social Network: A Case Study Done At Bitlis Eren and Fırat Universities). TÜRKİYE BİLİŞİM VAKFI BİLGİSAYAR BİLİMLERİ ve MÜHENDİSLİĞİ DERGİSİ, 7(7).
- [14] McAfee. "McAfee Labs Threat Report" <http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf>
- [15] Wayne Jansen, Karen Scarfone Guideliness on Cell Phone and PDA Security Recommendations of the National Institute of Standards and Technology
- [16] Disterer, G., & Kleiner, C. (2013). BYOD—Bring Your Own Device. HMD Praxis der Wirtschaftsinformatik, 50(2), 92-100.
- [17] Özcan, S. , Mayıs 2009, Yeni Nesil Şebekelere (NGN) Düzenleyici Yaklaşım ve Türkiye Önerileri, Sadullah Özcan, Uzmanlık Tezi, Bilgi Teknolojileri İletişim Kurumu
- [18] Cyber Threats to Mobile Phones, US-CERT United States Computer Emergency Readiness Team, By Paul Ruggiero and Jon Foote, 2011 Carnegie Mellon University, Produced for US-CERT
- [19] <https://tuketici.btk.gov.tr/>
- [20] http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSEKIGKHak_Yon_Konsolide_Metin_2013.pdf
- [21] Şahin, O. , Haziran 2011, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Osman Şahin, Uzmanlık Tezi, Bilgi Teknolojileri İletişim Kurumu
- [22] <https://www.mit.gov.tr/2937.pdf>

Keyser Gülnur GÖKCE – 1989 yılında Ankara'da doğdu. Yeditepe Üniversitesi Endüstri Mühendisliği'nde lisans eğitimini tamamladıktan sonra, Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri'nde yüksek lisansına devam etmektedir. Aynı zamanda Bank Asya'da Bilgi Güvenliği, BT Risk ve Uyum Müdürlüğü'nde uzman olarak çalışmaktadır. Araştırma ve çalışma konuları arasında siber güvenlik, BYOD, PCI DSS bulunmaktadır.

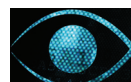
Dr. Ender ŞAHİNİSLAN – 1972'de doğdu, evli ve üç çocuk babasıdır. Trakya Üniversitesi Bilgisayar Mühendisliği Lisans, Gebze Yüksek



Teknoloji Enstitüsü Bilgisayar Mühendisliği bölümünde ‘Yazılımda Kalite Modellerinin Değerlendirilmesi’ adlı çalışmayla Yüksek Lisans, Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde ‘Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi’ adlı çalışmayla doktora programını tamamladı.

1996 yılında Gazi Üniversitesi’nde başladığı çalışma hayatına Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Araştırma Görevlisi, Maltepe Üniversitesi Öğretim Görevlisi, Sabancı Üniversitesi Bilgi Teknolojileri Birimi’nde Uygulama Sorumlusu olarak devam etti. 2004 yılında Bank Asya Yazılım Geliştirme Müdürlüğü’nde başladığı göreve, Organizasyon Kalite ve Sistem Geliştirme Müdürlüğünde devam etti halen Bilgi Güvenliği, BT Risk ve Uyum Müdürü olarak çalışmaktadır. ISO 27001 LA, ITIL Fv3 ve CRISC sertifikalarına sahiptir.

Said Dincel – 1985 doğumlu, Beykent Üniversitesi Yönetim Bilişim Sistemleri bölümünden mezun oldu. Bank Asya, Bilgi Güvenliği BT Risk ve Uyum Müdürlüğü’nde Bilgi güvenliği uzmanı olarak çalışmaktadır. Veri tabanı ve merkezi log yönetimi, log analizi, bilgi güvenliği ihlal olayları inceleme ve çözümleme, sızma test proje yönetimi başlıca çalışma alanlarını oluşturmaktadır. Halen İstanbul Şehir Üniversite’sinde, Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans eğitimini sürdürmektedir.



Çok Katmanlı Görüntü Steganografi

E. Avcı, T.Tuncer, F.Ertam

Özet—Bir steganografik metodu değerlendirebilmek için örtü verideki değişim ve örtü verinin taşıma kapasite ele alınmalıdır. Steganografik metotlarda en temel amaç kapasiteyi arttırmak ve örtü verideki değişimi azaltmaktır. Ancak kapasiteyle örtü verisindeki değişim ters orantılı olduğu için bu iki amaç aynı anda gerçekleşemez. Örtü verisindeki değişimi sabit tutup kapasiteyi arttırmak için çok katmanlı steganografi kullanılmaktadır. Bu çalışmada çok katmanlı görüntü steganografi ele alınacak ve çok katmanlı olmayan metotlarla karşılaştırılacaktır.

Anahtar Kelimeler—Görüntü Steganografi, Bilgi Güvenliği, Çok katmanlı steganografi, Veri Gizleme

Multi-Layered Image Steganography

Abstract— Change of the cover object and capacity of the cover object should be addressed in order to appreciate a steganographic method. The main purpose of steganographic methods is increasing capacity and reduce the changes of cover object. However, capacity is inversely proportional to the change in cover object, these two goals cannot be realized simultaneously. Multi-layer steganography is used for change of the cover object was kept constant in order to increase capacity. In this study, a multi-layered image steganography will be discussed and this method will be compared with non-multi-layered methods.

Keywords—Image Steganography, Information Security, Multi-Layer Steganography, Information Hiding

I. GİRİŞ

Bilgi gizleme teknikleri eski çağlardan günümüze kadar kullanılan tekniklerdir. Bu tekniklerin temel amacı, gönderilecek verileri güvenilir bir kanal oluşturup o kanal vasıtasıyla aktarabilmektir. Günümüz dijital dünyasında birçok bilgi gizleme tekniği geliştirilmiştir ve geliştirilmeye devam edilmektedir [1]. Bilgi gizlemenin en önemli alt dallarından biri olan steganografi dijital medya verilerinin korunması için kullanılmaktadır. Steganografi; hem bilimsel olarak bilgi gizlemenin alt dalı hem de bilgiyi saklama sanatı olarak adlandırılır [8]. Steganaliz ise gizli iletişim kanalları

Engin Avcı, Fırat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği Bölümü 23100 Elazığ, Türkiye (e-posta: enginavci@firat.edu.tr).

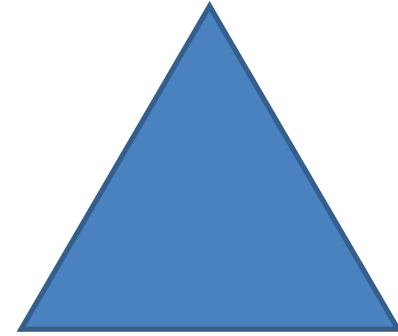
Türker Tuncer, Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü 23100 Elazığ, Türkiye (e-posta: turkertuncer@firat.edu.tr).

Fatih Ertam, Fırat Üniversitesi Bilgi İşlem Daire Başkanlığı, 23100, Elazığ, Türkiye (e-posta: faith.ertam@firat.edu.tr)

dinleyip, yapılan iletişimi ele geçirmek için yapılan saldırıları ve analizleri içermektedir.

Bir steganografik sistem farklı bakış açılarıyla değerlendirilmektedir. Bunlar bilgi gizlenen örtü verisi (cover object) ne kadar değiştiği, bilgi saklama kapasitesinin ne kadar olduğu ve sistemin dayanıklılığının ne kadar olduğudur [2]. Bir steganografik sistemin başarımını değerlendirmek için bu üç kritere bakılması gerekmektedir. Bu kriterleri steganografi ve steganaliz alanında çalışmaları olan bilim insanı Jessica Fridrich ortaya atmıştır ve Fridrich üçgeni şekil 1’de belirtilmiştir.

Kapasite



Dayanıklılık

Taşıyıcıdaki Değişim

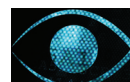
Şekil 1. Fridrich Üçgeni

Günümüzde birçok steganografik metot vardır ve bu metotların başarımının ölçülmesi için yukarıdaki üçgen referans alınmalıdır.

Her steganografik yöntem algoritmik olarak farklı metotlar izlediği için farklı analiz metotları geliştirilmiştir. Bundan dolayı her metodun kendine özgü bir steganaliz metodu bulunmaktadır [4].

Bu makalede çok katmanlı görüntü steganografiden bahsedilecektir. Temel amaç görüntünün içerisine veri ve o verinin içerisinede aynı algoritmayla veri gizlemektir. Veri gizleme ve çıkarma işlemleri ilerleye bölümlerde ayrıntılı bir şekilde anlatılacaktır.

Çalışmanın 2. Bölümünde görüntü steganografi, üçüncü bölümde çok seviyeli katmanlı steganografi, dördüncü bölümde geliştirilen uygulama ve 5. ve son bölümde sonuç ve öneriler yer alacaktır.

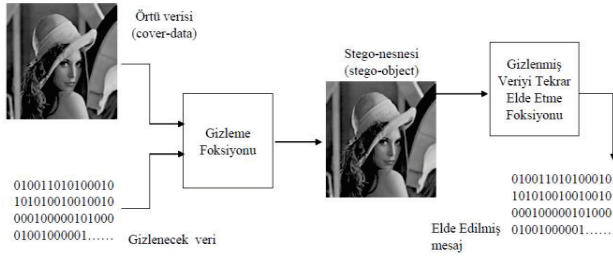


II. GÖRÜNTÜ STEGANOGRAFI

Steganografi tekniğinin en sık uygulandığı medya formatları görüntü formatlarıdır ve günümüzde yaygın şekilde kullanılmaktadır. Yaygın kullanılmasının en önemli sebeplerin biri ise kapasitedir.

Dijital görüntülerin dağıtımı kolay ve internette hemen hemen her sayfada bulundukları için steganografik iletişim açısında sıkça kullanılabilecek dosyalardır.

Görüntü dosyalarına steganografinin uygulanabilmesi için ön şart resmin dijitalleştirilmesidir. Piksel değerleri alındıktan sonra hangi gizleme fonksiyonunun kullanılacağı seçilir. Gizleme fonksiyonu seçildikten sonra gömülecek verinin boyutu, tipi ve örtü nesnesinin neresine gömüleceği hakkındaki bilgiler alınarak Steganografi anahtar oluşturulmalıdır. Anahtar istenilirse şifrelenir. Ardından gömülecek veri gizleme fonksiyonu kullanılarak örtü nesnesine gizlenir ve Stego resmi veya steganogram oluşturulur.



Şekil 2. Görüntüler için kullanılan steganografik sistem diyagramı

Herhangi bir steganografik sistemin kabul edilebilmesi için Fridrich üçgeninde gösterilen üç temel şartı sağlaması gerekmektedir. Bunlar algılanabilirlik, sağlamlık ve kapasitedir. Algılanabilirlik; taşıyıcı nesnenin (Stego-object) içerisinde bilgi olup olmadığının sezilmesidir. Eğer bir sistemde bilgi varlığı ne kadar az sezilirse o sistem o kadar güvenilirdir. Sağlamlık koşulunda ise gizli verinin ne kadarlık kısmı iletim hattında bozulmadan alıcı tarafa iletebildiğinin ölçütüdür. Gizli veri iletim kanalındaki gürültü ve saldırılardan ne kadar az etkilenmişse sistem o kadar sağlamdır. Kapasite ise örtü verisinin (cover data) ne kadarlık bilgi taşıyabileceğiyle ilgilidir. Örtü verisi ne kadar çok bilgi taşırsa o kadarlık kapasiteye sahip demektir. Örneğin steganografinin elinde here piksele bir bitlik bilgi saklayabileceği bir gizleme fonksiyonu olsun ve anahtar resme gömülmesin, böyle bir steganografik sistemin kapasitesi aşağıdaki gibi gösterilmiştir.

$$S = mnk \quad (1)$$

$$B = 8b \quad (2)$$

$$K = \frac{S}{B} \quad (3)$$

S resmin piksel sayısı veya kaç byte' tan oluştuğu temsil etmektedir. m satır sayısı, n sütun sayısı ve k katman sayılarını sembolize etmektedir. Her pikselin bir baytlık bilgi taşıdığı düşünülecek olursa formül 1 resmin kaç baytlık resim olduğu

bilgisini vermektedir. Eğer resim RGB formatında ise k 3 değerini alacaktır, gri seviyeli bir resim ise k değeri 1 olacaktır. 1 baytın 8 bit olduğu formül 2' te gösterilmiştir. Gizleme fonksiyonun özelliği ve eldeki bilgilerden yola çıkılarak formül 3' deki kapasite denklemi elde edilmiş olur.

Kusursuz bir steganografik sistemin oluşturulması için algılanabilirlik, sağlamlık ve kapasite ölçütlerinin maksimize edilmesi gerekmektedir fakat taşıyıcının kapasitesi arttıkça algılanabilirliği artmakta ve algılanabilen bir sistem kabul edilmez bir hal almaktadır. Aynı zamanda kapasitesi arttırılan bir steganografik sistemde sağlamlıktan bahsetmekte zor olacaktır. Çünkü taşınan veri iletim kanalında gerçekleşen kayıp ve saldırılardan doğrudan etkilenecektir. Bu 3 ölçütü mükemmel kullanabilen bir saklama fonksiyonu halen geliştirilememiştir ve bu sebepten dolayı ölçütlerde kabul edilebilir kıstaslar konularak gizleme fonksiyonları değerlendirilmeye çalışılmaktadır. Bu ölçütlerin en iyi sağlandığı veriler görüntü verileri (resim ve videolar) olduğu için Görüntü Steganografi çok sık kullanılmaktadır[5].

Görüntü steganografide en sık kullanılan metotlar ise aşağıda verilmiştir

- En önemsiz bit değiştirme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [2]

III. ÇOK KATMANLI STEGANOGRAFI

Çok katmanlı steganografik yöntemler taşıyıcının kapasitesini ve güvenliğini arttırmak amacıyla ortaya atılmıştır[6]. Örneğin taşıma kapasitesi 10 Kb olan bir örtü verisinin kapasitesini 12 Kb' e çıkarılmak amaçlanmıştır. Çok katmanlı steganografinin bir diğer avantajı ise kapasiteyi artırırken taşıyıcıdaki değişim yok denecek şekilde artmaktadır veya hiç artmamaktadır[7]. Çok katmanlı steganografinin matematiksel modeli aşağıdaki gibidir.

$$s = \log_{\left(\frac{b}{e}\right)}(MNk) \quad (4)$$

$$C = \sum_{n=1}^s \left(\frac{MNk}{\left(\frac{b}{e}\right)^n} \right) \quad (5)$$

$$C' = \frac{MNk}{\left(\frac{b}{e}\right)} \quad (6)$$

$$K = \frac{C-C'}{C'} 100 \quad (7)$$

$$r = \frac{C}{MNk} 100 \quad (8)$$

s seviye sayısını, b piksel değerlerinin kaç bitle ifade edildiğini, e bir piksele gömülecek bit sayısını, M resimdeki satır sayısını, N sütun sayısını, k katman sayısını, C' tek katmanlı steganografi kullanılarak yapılan gizlemede örtü verisinin kapasitesini, C çok katmanlı steganografi kullanılarak

yapılan gizlemede örtü verisinin kapasitesini, K kazancı ve r ise gizlenmiş verinin örtü verisine olan oranını ifade etmektedir.

TABLO I. Tek Seviyeli ve Çok Seviyeli (Soğan) Steganografi Veri Gizleme Kapasiteleri (LSB Tekniği, b=8, e=1)

Çok Katmanlı Steganografi Kullanılarak Elde Edilen Kazançlar (LSB Tekniği, b=8, e=1, 1 bpp)				
Boyut	64X64	256X256	512X512	1536X1536
Seviye	4	5	6	7
Kazanç (%)	14.2578	14.2822	14.2853	14.2857

Yukarıdaki tabloda LSB tekniğinin çok katmanlı uygulamasının kazanç değerleri verilmiştir. Sadece 2 seviyeli steganografi de dahi bant genişliğindeki artış %12.5 olarak gerçekleşmiştir. Çok katmanlı steganografi daha karmaşık olmasına rağmen, kapasiteyi ciddi şekilde arttırmaktadır.

Çok katmanlı görüntü steganografi yönteminin en büyük avantajlarından biride bant genişliği artmasına rağmen, resimdeki değişimin hemen aynı kalmasıdır.

Resimlerin bozulma oranı PSNR (Peak Signal Noise Rate) ve MSE (Mean Square Error) metrikleriyle hesaplanmaktadır. PSNR' nin yüksek çıkması resimdeki bozulmanın az olduğunu göstermektedir [9].

$$MSE = \frac{1}{MN} \sum_{i,j} (P_{i,j} - \bar{P}_{i,j})^2 \quad (9)$$

$$PSNR = 10 \cdot \log \cdot \frac{Max(P_{i,j}^2)}{MSE} \quad (10)$$



Şekil 3. Karşılaştırma İçin Kullanılacak Resimler

Şekil 3' teki resimlere önce klasik LSB yöntemi kullanılarak veri gömülmüştür, ardından ÇOK KATMANLI GÖRÜNTÜ STEGANOĞRAFI kullanılarak veri gömülmüş ve kapasitesi (bant genişliği) artırılmıştır. İki seviyeli ÇOK KATMANLI GÖRÜNTÜ STEGANOĞRAFI yapısı kullanılmıştır ve bant genişliği %12.5 artırılıp PSNR sonuçları aşağıdaki tabloda verilmiştir.

TABLO II. PSNR değerleri

Görüntü	LSB (%100 Kapasite- 1 bpp)	LSB (%114 Kapasite, 1.14 bpp)	4 katmanlı görüntü steganografi (%114 Kapasite)
rice	48.3568	44.8572	48.3648
adam	48.1875	36.7469	48.1263
cameraman	48.3374	44.6697	48.3600
football	48.3126	36.7448	48.3356

Tablo 2' de görüldüğü gibi PSNR sonuçları birbirine çok yakındır. Ortalama PSNR değişim miktarı %0.059 olarak gerçekleşmiştir. Bu oran ise çok küçük bir orandır ve bu oran ihmal edilebilir.

Yukarıdaki verilerden yola çıkacak olursak, çok katmanlı görüntü steganografi yöntemiyle gerçekleştirilen veri gizlemelerde örtü verisinin kalitesi bozulmadan bant genişliği (kapasite) artırılmıştır.

Fakat klasik yöntemler kullanılarak taşıyıcı kapasitesi artırılmaya çalışıldığında, PSNR değişim miktarı ortalama %15.6275 olarak gerçekleşmiştir. Klasik yöntemlerle kapasite artırıldıkça, taşıyıcı resmin kalitesi düşmektedir. Klasik yöntemlerde, resmin kalitesi ile kapasite arasında negatif korelasyon vardır. Çünkü yukarıda ki uygulamada resmin kapasitesi %14 artırıldı fakat resmin kalite metriği olan PSNR ise %15 değer kaybetmiştir.

IV. SONUÇ

Bu çalışmada çok katmanlı steganografiden bahsedilmiş olup, tek katmanlı steganografiye göre avantajlarından bahsedilmiştir. Özellikle bant genişliğini taşıyıcı kapasitesini artırması önemli bir özellik olarak görülmüştür.

Örneğin tek katmanlı steganografik bir modelin karmaşıklığını O(n) olarak kabul edersek, aynı modelin 2 katmanlı uygulamasının karmaşıklığı O(nlogn) olarak karşımıza çıkacaktır. Ancak kapasite arttıkça örtü verisindeki bozulma artmaktadır. Çok Katmanlı metotlar kullanılarak örtü verisinde ki değişim sabit tutularak kapasite artırılabilir.

Bu yöntem özellikle onion routing (soğan yönlendirme) ve çok seviyeli güvenlik uygulamalarında da kullanılabilir. Soğan yönlendirme de taşıyıcı (soğan) birden fazla mesaj taşımaktadır ve bu mesajlar çeşitli anahtarlarla şifrelenmiştir. İlgili anahtara sahip olan kullanıcı soğanı deşifre ederek ilgili mesajı elde edebilmektedir. Soğanın oluşturulabilmesi için çok katmanlı steganografi kullanılabilir. Örtü verinin altında gizlenecek alt örtü veriler sayesinde, birden fazla mesaj taşınabilir. Ayrıca çok seviyeli güvenlik uygulamalarında da bu metot kullanılabilir.

Modelin performansını arttırmak için paralel programlama metotlarına başvurulabilir. Örneğin threadler kullanılarak modelin performansı artırılabilir. Ayrıca gömülü sistemlerde uygulaması yapılarak analiz edilebilir.

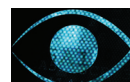
KAYNAKLAR

- [1] Katzenbeisser, S., Petitcolas, F.A.P., 2000., Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, INC. 685 Canton Street Norwood, MA 02062.
- [2] Şahin, A., 2007. Görüntü Steganografide Kullanılan Yeni Metotlar ve Bu Metotların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
- [3] N. Baykal, T. Beyan, “Bulanık Mantık Uzman Sistemler ve Denetleyiciler”, Bıçaklar Kitabevi, 2004.
- [4] Al-Najjar A.J. (2008) The Decoy: Multi-Level Digital Multimedia Steganography Model. In Proc. of 12th WSEAS International Conference on Communications, Heraklion, Greece, July 23-25, 2008
- [5] Şahin Mesut A., Mesut A., Saklı M.T., “Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri”, III Ağ ve Bilgi Güvenliği Sempozyumu, Ankara-Türkiye, Feb 2010
- [6] Fraczek W., Mazurczyk W., Szczypiorski K., “Multi-Level Steganography: Improving Hidden Communication in Networks”, Warsaw University of Technology, Apr 2012
- [7] Al-Najjar A.J. ,The Decoy: Multi-Level Digital Multimedia Steganography Model. In Proc. of 12th, 2008
- [8] Popa, R., An Analysis of Steganographic Techniques, Master Thesis, Department of Computer Science and Software Engineering, Faculty of Automatics and Computers, The Politehnica University of Timisoara, 1998.
- [9] Sayood K., Introduction to Data Compression, Morgan Kaufman Publishers, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA, 1996.

Engin Avcı, F.Ü. Yazılım Mühendisliği bölümünde çalışmaktadır. Doç. Dr. Engin Avcı görüntü işleme ve bilgi güvenliği alanında çok sayıda uluslararası yayına sahiptir

Türker Tuncer, F.Ü. Adli Bilişim Mühendisliği Bölümünde Araştırma görevlisi olarak çalışmaktadır, Yazılım Mühendisliği Bölümünde doktora öğrencisidir, bilgi güvenliği ve yazılım güvenliği alanında çalışmaktadır.

Fatih Ertam, Fırat Üniversitesi Enformatik Bölümünde okutman olarak görev yapmakta ve Bilgi işlem biriminde ağ ve sistem yöneticiliği görevini yürütmektedir. Yazılım Mühendisliği bölümünde doktora öğrencisidir, ağ güvenliği alanında çalışmaktadır.



Use of Massively Multiplayer Online Games for Intelligence Gathering, Recruitment, and Training Purposes

B. Korkmaz, M. E. Tuzcu, and S. Sözer

Abstract—Game has always been an indispensable part of human life. Since the early days of mankind, different types of games evolved hand in hand with civilization. The advent of personal computers in the 1970s, the spread of the internet in the 1990s, and the emergence of broadband connections as of the 2000s, brought about a revolution in the game industry in the form of what is called Massively Multiplayer Online Games (MMOGs). In this paper, it will be attempted to emphasize the importance of MMOGs in the light of the opportunities they provide for non-gaming purposes like intelligence gathering, recruitment, and training by states or non-state actors.

Index Terms—intelligence, Massively Multiplayer Online Game, recruitment, terrorism, training

I. INTRODUCTION

SINCE the beginning of civilization, power and security have been inseparable and vital elements for the equation of human existence. Situations of power maximization appear to be the most secure moments in political history. Power has been defined in various ways by different scholars, strategists and politicians throughout history. However, Morgenthau seems to have made the most accurate definition for today's cyber-driven world [1]. He defines power as the ability to control other people's minds and actions. Accordingly, in today's world, individuals, institutions or states, should assess all plausible scenarios concerning the factors that shape the mindsets of people they interact with, in order to prevent breaches in their defensive structures. This indicates a new security paradigm based on a broader definition of warfare.

In 1989, near the end of the Cold War, William S. Lind and several other military experts proposed the concept of "fourth generation warfare" in an attempt to explain the new security environment [2]. While the first three generations of warfare were centered on military doctrines, the fourth generation's focus has shifted towards the non-military aspects of power

struggle, they argue. In this type of warfare, opponents aim to exert force through mostly indirect means such as propaganda, financial manipulation, provocation, or other sorts of subversive activity. When military conflict is unavoidable, it usually happens in an asymmetric fashion, where proxies such as insurgent groups and terrorist organizations are employed against military and/or civilian targets.

Arguably, the most crucial factor that brought about this qualitative shift towards a more inclusive conception of warfare has been the spread of the internet. With its pervasive impact, the internet has been transforming societies across national borders in every aspect, unifying and diversifying people in unpredictable ways so that they become a "network society," whose dynamics and actions cannot be effectively controlled by local authorities [3].

With its diffuse and non-hierarchical structure, the internet constitutes an invaluable platform for real time economic and social interaction on a global scale. However, the same platform can be used for both legal and illegal activities. In the last two decades, it has been understood that "cybercrimes" such as hacking, identity theft, and denial-of-service attacks are only a small fraction of what the internet provides for actors with criminal intent. Today, it is known that cyberspace is being effectively used by terrorists, drug traffickers, money launderers etc., for communication or other purposes.

Moreover, even perfectly legal use of internet-based social media platforms may have a drastic impact on national security, as has been recently seen in massive protests and uprisings around the world. In 2011, during the Egyptian revolt, a protester in Cairo was quoted as saying, "we use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world," effectively summing up internet's function in a fourth generation "battlefield" [4]. As Kendircioğlu et al. emphasize, "interdependent and interconnected networks and devices using information and communication technology, [offer] perfect tools for irregular actors to gain or erode popular support and question the legitimacy of the opponent" [5]. Hence, the effects of widespread internet use among their citizens, have become a major concern for nation-states.

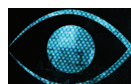
Recently, in addition to all that has been said above, yet another way of exploiting the internet for political and/or criminal purposes has come to the forefront, but in a rather

Manuscript received September 15, 2014.

Burak Korkmaz is a master's student at Turkish War Academy – Strategic Research Institute (e-mail: burakorkmaz@yahoo.com).

Mehmet Efe Tuzcu is a founding partner of Vizör Strategic Consulting Services (e-mail: metuzcu@hotmail.com).

Sema Sözer is a PhD candidate at Istanbul University Forensic Sciences Institute (e-mail: sozer.sema@gmail.com).



unexpected medium: Massively Multiplayer Online Games (MMOGs), where millions of people from around the world meet and interact in Virtual Worlds (VWs), using identities of their choosing. This topic drew much attention when, in 2013, Edward Snowden leaked secret documents concerning NSA's and GCHQ's activities in two popular MMOGs. However, as early as 2008, it was already known that American intelligence was about to start a program that aims to collect intelligence from such games [6].

As counter-intuitive as it may seem at first, MMOGs may have a substantial value from a national security perspective in today's world of fourth generation warfare, both as sources of opportunities and threats, depending on who utilizes them, and how. In this paper, it will be attempted to emphasize the importance of this subject matter in the light of relevant technical and scientific knowledge. It will be shown that MMOGs constitute a fertile ground for gathering intelligence on individual or groups of players, for finding and engaging potential recruits, and for indoctrinating and training them.

II. THE CONCEPT OF GAME FROM A FUNCTIONALIST PERSPECTIVE

A. Definition of Game

Regarding "game" merely as a pastime carries the risk of mistakenly putting it in contrast with what count as "serious" activities. As a matter of fact, "game" is such a significant part of life that philosophers had to put a great effort to understand and define it. Since Ludwig Wittgenstein, many thinkers have come up with their own definitions of "game," and the discussion still continues today. Arguably, even a predator that plays with its prey can be considered as involved in a game, hence the expression "cat-and-mouse game." In that broader sense, game can be said to exist everywhere in nature, where there is intelligent life. The more intelligent the animal is, the more complex the games become. Therefore, man-made games are much more complex than others found in the animal world.

The complexity of man-made games is a function of game rules. In fact, without rules, it is not possible to talk about a sensible game. Thus, for Bernard H. Suits, "to play a game is to engage in activity directed towards bringing about a specific state of affairs, using only means permitted by rules, where the rules prohibit more efficient in favor of less efficient means, and where such rules are accepted just because they make possible such activity" [7]. As such, games can be categorized in several ways as to their structures and tools required for playing. There are games of chance, competitive games, board games, video games, role playing games, single or multiplayer games, turn-based or real time games etc. Despite their differences, all such games are based on certain rules, which makes having rules a defining characteristic of "game."

Jane McGonigal identifies three more traits shared by all games: a goal, a feedback system, and voluntary participation [8]. Players need a goal to find a sense of purpose in playing the game. In cases of losing one's purpose in real life, the sense of purpose in games can become a plausible substitute,

which may partially explain why some games are dangerously addictive for certain populations, as will be explained below. Secondly, the feedback system, in the form of scores, levels, points etc., keeps players on track by motivating them towards the goal, and enabling them to assess their success rate. This trait also makes it possible to gain experience by trial and error. Finally, voluntary participation entails that all players are fully aware of, and willing to accept the goal, the rules and the feedback system of the game. Being able to take the challenge intentionally, and to quit at any time, differentiates the game from real life, as a safe and enjoyable activity.

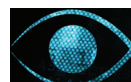
B. Functions of Game

The prevalence of games among intelligent life forms can be explained by their multiple functions. First and foremost, games serve as a practice ground before facing real life challenges. Chasing after a drifting leaf prepares the cheetah cub for a real hunt. Wrestling with siblings helps a young wolf understand what to do when confronted by a true rival in the future. Clearly, the same principle applies when a fighter pilot tests his/her skills in a flight simulator, before taking off for a real dogfight. This simulative function of games is especially evident when "game" is defined as "a system in which players engage in an artificial conflict, defined by rules, that results in a quantifiable outcome" [9]. Games also provide a medium for communication and conflict resolution, which is especially important for social animals like humans. In-game behavior usually reflects specific character traits such as competitiveness, honesty, courage etc., helping players know each other better, thus reducing the conflict potential in real life. When conflicts occur, once agreed upon a certain set of rules and regulations, games can bring real-life opponents together in a peaceful setting, and help them translate their hostilities into nonviolent competition. Therefore, although not enough to solve the actual problems between parties directly, games provide an opportunity to vent negative emotions that may pose an obstacle to reaching a reasonable agreement.

C. Evolution of Game

Because of such functional benefits, games of all kind have been an indispensable part of human life throughout history. Some authors even went as far as to suggest that civilization owes its very existence to the concept of game [10]. That aside, it is a known fact that games have evolved hand in hand with civilization. What started as simple races and primitive board games, grew in sophistication as different cultures came up with different sets of rules and developed a variety of new tools. New games emerged as others disappeared, and some games were combined to create advanced game designs.

This evolutionary process took a dramatic turn in the last quarter of the 20th century, as the advent of personal computers in the 1970s was soon followed by the rise of the internet in the 90s. The exponential growth rate of processing power paved the way for realistic graphics rendering, and rapid advances in artificial intelligence. This enabled the creation of sophisticated computer games in many different genres, which



can be played by one or more players using the same computer. Finally, in the 2000s, as dial-up internet steadily gave way to high-speed, broadband connections, a new era of gaming has begun with the creation of advanced VVs, which provide a “play-ground” for many kinds of MMOGs.

III. A PSYCHOLOGICAL ASSESSMENT OF VIRTUAL WORLDS

VVs are defined as *immersive 3D environments* in which many users are able to interact with each other via the internet [10]. Increasing number of users are engaged in VVs on a regular basis for different purposes from gaming to socializing. In all these worlds, users are able to project themselves into an online setting via an avatar, a 3D body whose appearance and behaviors can be controlled and tailored by the user.

In this virtual space, though the avatars, users can be anonymous or present themselves as a character in which they can play a role as they choose either close to or far away from their ‘real selves’ [11]. In other words, VVs create a new environment that enables the construction and reconstruction of the self [11]. Beyond that, the self can not only be modified but also be multiplied without any limits. Different cultures for different characters can coexist and interact with each other.

Virtual space engagement provides many opportunities to have ‘second chances’ for adults in which they can shape and reshape their lives, work through unsolved identity issues [11] and create a virtual life that they can succeed as they wished to. The users, especially with lower psychological well-being perceive their virtual characters as more favorable than their true personality [12]. In the end, it is a very powerful fantasy knowing that ‘I am not limited with my history and able to create and recreate myself and my life’.

Through character and environment building, control and mastery feelings are established much easier than the real life. Game players are engaged in economic activities, involved in hunting or combat, build friendships, form communities which in the end promise the sense of belongingness [13] and achievement. In that sense, virtual world and the real world are very similar by providing a space that people carry out their everyday activities and experience the feelings like sorrow, happiness, success, satisfaction, surprise, ambition, belongingness, and so on.

There are different ways of manifesting the self in virtual world. Players may reflect their lifestyles, values and attitudes into the virtual space at different levels. Studies show that every game player develops a distinctive lifestyle in virtual environment [14]. They usually act similar to or in parallel with their real value system. Most of the behavior patterns show common properties with the ones in real world.

The relationship between the behavior manifestations of virtual and the real worlds has been a great interest for many researchers, government institutions and radical groups like organized criminals. Among those behaviors, aggression stands out dramatically for many interest groups, especially for the ones that wish to explore the players that they can recruit for their own causes.

Expression of aggression like character attack or ‘illegitimate’ Player Killing and manifestations of gender identity in the online game world might be important clues of the real lifestyles of the players [15].

VVs also provide an environment in which people can communicate with each other by using their avatars. This system allows strangers to establish relationships and get to know each other better through the virtual reflections of themselves [16]. Millions of online players from very different parts of the world are able to communicate through their ‘ideal selves’ in their artificial ‘ideal world.’ This might create an emotional bond and attachment that could be very dangerous with the exploitation of the psychologically disordered people by terrorist groups.

An essential function of VVs is to create a sense of security for its users, which makes them feel free from the constraints imposed upon them by the society in real life. In that sense, a VV constitutes what is called a “magic circle,” a “shield of sorts, protecting the fantasy world from the outside world” [17]. However, that does not mean that VVs are chaotic environments. There are rules to follow, but these are not determined by the outside world. Instead, different MMOG designs come up with their own rules and limitations to be applied in the VVs. In other words, the same relation that exists between the real world and real life, could be said to exist also between VVs and MMOGs.

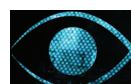
IV. MASSIVELY MULTIPLAYER ONLINE GAMES

Online gaming industry with its 400 million active users is a rapidly growing market. According to a report by Gartner, a US based global information technology research and advisory company, online gaming economy would reach approximately 30 billion dollars in 2015 [18]. Credit Cards and e-Wallets are preferred as payment methods by MMOG customers [19]. Market researches point out that, more than 60% of the MMOG players are older than 21 years, and approximately 80% of them are males younger than 35 years [20].

Although many genres, types or categorizations are available on the MMOG market, MMOGs can be examined under three basic categories in terms of their content: First Person Shooter Games (FPSGs), Fantasy Role Playing Games (FRPGs) and Real Life Simulations (RLSs).

FPSGs are played mostly in urban warfare settings and on several maps for different missions, such as neutralizing the enemy, capturing or protecting the base, liquidating individuals, and destroying or maintaining control of a designated area, vehicle, or machinery. Missions with asymmetric warfare themes are held by operators mostly in or around urban areas. FPSGs highly depend on tactical and operational level decision making under duress.

Secondly, FRPGs stay in touch with well-known tabletop games and fantasy literature. Urban spaces and aspects of modern city life become a less popular theme around FRP circles. Abilities are developed by FRP characters throughout their virtual careers. Unlike the reflexive, repetitive, and



normative nature of FPSGs, FRP environment is highly anarchic and depends on operational and strategic decision making.

Thirdly, games defined as RLSs, propose a different experience to their audiences. RLS experience covers most of the civic and civil aspects of human life, including pregnancy and even birth of so-called children. Unlike heavily militarized FPSGs or adventure oriented FRPGs, and their tactical, operational and strategic points of view, RLSs are almost as inclusive as real life as to their in-game dynamics.

V. METHODS OF USING MASSIVELY MULTIPLAYER ONLINE GAMES FOR NONGAMING PURPOSES

The aforementioned characteristics of MMOGs make them not only a valuable medium for research in many fields from sociology [21] to transportation engineering [22], but also a useful tool for gathering intelligence, recruitment, and training, no matter who uses them for such purposes, be it government agencies or criminal organizations. In various ways, it is indeed possible to break into the “magic circle,” and build bridges of information and interaction between the VWs and the outside world. The most benign and nonintrusive way is to take part in the MMOGs as a player. If, for instance, a certain avatar in an MMOG is known to be used by an identified real person, that person can be approached in the VWs by using another avatar. This method is identical to a classic HUMINT operation in the real world, but for one difference: avatars are used instead of real life masks.

More advanced methods can be examined under three categories with increasing levels of efficiency: intrusive use of existing MMOG infrastructures, setting up private MMOG servers, and creating specialized MMOGs.

A. Intrusive Use of Existing MMOG Infrastructures

The technical infrastructure of MMOGs comprises mainly two elements: servers, and players' computers. The gaming experience is the product of a continuous and massive information flow between the two elements. Theoretically, it is possible to illegally break into an MMOG infrastructure through either of those elements. Hacking into the computers of players or reaching MMOG server data by either technical or nontechnical means, enables the intruder to collect information on players' activities in the VW, which can then be used for intelligence purposes. The downsides of this method are that it carries the risk of facing criminal charges if caught, and that it requires advanced technical knowledge, skills, and tools.

B. Setting Up Private MMOG Servers

Controlling an MMOG server makes it possible to log all data flowing through that server. Therefore, setting up a private MMOG server enables its owner to record all dialogues and actions occurring in the game. This method does not require as much technical capability as the one above, yet it still carries the risk of being sued by MMOG companies for copyright infringement and other such offenses [23].

C. Creating Specialized MMOGs

The most effective method of using MMOGs is creating an MMOG that is specifically designed to serve one or more of the aforementioned purposes. As will be seen, different genres of MMOGs lend themselves to either of those purposes in different degrees. Therefore, being the designer of an MMOG and controlling its servers gives the game owner the best opportunities to use it for nongaming purposes. However, the costs of such an operation are so high that it is virtually unaffordable for all but the very wealthy actors.

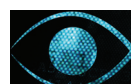
VI. INTELLIGENCE GATHERING, RECRUITMENT, AND TRAINING THROUGH MASSIVELY MULTIPLAYER ONLINE GAMES

A. MMOG as an Intelligence Gathering Environment

Despite their differences, all genres of MMOGs can be utilized for intelligence gathering purposes to certain extents. In one instance, a virtual epidemic spread among the avatars in one of the most popular FRPGs [24]. Soon, what was initially started by the game administrators as a challenge for powerful avatars, unexpectedly turned into a pandemic that began to kill scores of avatars indiscriminately. Unable to solve the crisis in any other way, the administrators had to reboot the VW to save the game. Named after the virtual disease that caused the crisis, the “Corrupted Blood incident” became a research topic for both epidemiologists [25]–[26], and counter-terrorism officials [27], who suggested that the spread of the disease, and the response pattern of avatars bore a close resemblance to real life epidemics.

FPSGs of an ideological leaning can also give valuable information about their owners and players. It is known that in recent years, Hezbollah designed two sequential FPSGs with anti-Israel themes. Neither of them can be regarded as an MMOG: the first one does not have a multi-player mode, and the second one lacks a “persistent world,” that is, a VW that continues to exist independent of the players. Nevertheless, in spite of their rather primitive nature, they do constitute valuable platforms for intelligence, both for Hezbollah and its enemies. The definition given for the second game by a Hezbollah member makes the point: “It is not only a game, it is an education and culture and it is part of the confrontation because the American and the Western companies created games featuring us as terrorists and it is widespread on the market. This achievement is an addition to the tools of resistance and confrontation” [28]. A sequential third game in the form of an MMOG would surely provide an even better tool for intelligence gathering.

However, arguably, RLSs with their comprehensive contents and non-fantastic settings are better suited to intelligence gathering purposes. Phyllis Johnson describes one such RLS: “[For] many members, [it] is not an escape from the real world, but an extension of it, particularly when it comes to responding to news reports of world conflict” [29]. The author informs that the RLS servers had to be temporarily shut down because of the influx of pro-Palestinian protesters after the real world violence in Gaza, in early 2009 [29]. The US presidential campaigns are known to be held in RLSs too,



including all the activism in the form of protests, rallies, and discussions [30]–[31]. Thus, in addition to the personal information about players that can be collected from RLSSs, it is also possible to gather intelligence about their political inclinations and actions.

B. MMOG as a Recruitment Medium

A 2012 report, prepared by the UN, explains how the internet can be used for recruitment purposes: “The Internet may be used not only as a means to publish extremist rhetoric and videos, but also a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda. Terrorist organizations increasingly use propaganda distributed via platforms such as password-protected websites and restricted access Internet chat groups as a means of clandestine recruitment” [32]. The rising popularity of MMOGs among young males, who are usually more prone to rebellious and aggressive behavior, makes MMOGs suitable mediums to find potential candidates for organized violence.

MMOGs are environments where players compete for self-realization through their avatars. This competition and the related gratification/frustration cycle may become dangerously addictive for those who are not content with themselves in the real world. Acting upon the same principle employed by Hasan Sabbah as he promised a false paradise to his desperate followers, such people in search for a more satisfactory and meaningful life can be easily lured into militancy.

Not only terrorist organizations but states, too, are using online video games for recruitment. The US government developed a game called America’s Army for contacting potential recruits, and released it for free on July 4, 2002. Although not exactly a MMOG, since it lacks a “permanent world,” this online FPSG was so successful that it “had made a more positive impression than all the Army’s other recruiting initiatives combined” [33].

C. MMOG as a Training Tool

Population researches reveal that 53% of the human population is living in urban areas [34]. It is expected that urban population will be increasing to 6.25 billion by 2050 and approximately 80% of that population will originate from the less developed regions of the world [35]. Experiences of Somalia, Fallujah, 9/11 and perpetual street clashes of the Middle East, display that all actors in the power play should be well prepared for an urban warfare environment.

Although some scholars suggest that the violence element of the MMOG experience would not cause a substantial increase in real world aggression [36], it does not mean that MMOGs are not valuable in terms of training for aggressive purposes. Real life disputes about religious, ethnical, or ideological matters are known to generate soft spots in societies. Thus, although aggression may not be a direct outcome of MMOGs, once the psychologically prone individuals are identified and approached in VWs, their aggressive tendencies may be put into action through political indoctrination and/or systematic radicalization. The value of the internet as a medium for propaganda has already been known for some time. As Nico Prucha mentions, a laptop is more than enough for that

purpose [37]. The MMOGs can be regarded as just a new and more effective tool for using the internet in that manner.

However, the use of MMOGs as training tools is not limited to ideological and psychological domains. There are several studies that show the positive effects of playing video games on motor skills such as increased eye-hand coordination, better reaction time, spatial visualization, mental rotation, visual attention etc., and the simulative aspects of gaming “can potentially lead to acquisition of complex real-life skills, such as driving, flying airplanes, and even playing golf” [38]. MMOGs with their interactive VWs that require players to develop their organizational skills in addition to their motor skills, adds a new dimension to the enumerated positive effects of video games.

The FPSG genre of the MMOGs is especially relevant for military purposes. Armed forces personnel, first responders, operators, case officers or insurgents are trained by state and non-state actors with different intentions. Preparing an asset on a specific mission requires scientific method which depends on preparing, testing, evaluation and feedback cycle. On the field, the protocol is simple; an operation is a zero-sum game. In that sense, real time battle simulations against real operators in a FPSG environment would bring invaluable experience to the table. Moreover, Weapons of Mass Destruction (WMD) and concerns about their use for terrorist purposes generate another field for MMOGs. There are studies about using MMOGs as a training tool against WMD’s, done by officers at Naval Postgraduate School (NPS) at 2004 [39] and 2012 [40].

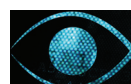
Going beyond the initial purpose of recruitment, more advanced versions of the aforementioned game, America’s Army, have been effectively used for training purposes, as well [41]–[42]–[43]. Yet another project taken by the US government is an advanced MMOG called Asymmetric Warfare Environment, which is specifically designed for training the military personnel, and is not released to the public [44]. It is reasonable to argue that this trend towards virtual training will continue exponentially, as new technological advances pave the way for more daring projects.

VII. CONCLUSION

As shown in this paper, in today’s fourth generation warfare environment, MMOGs provide a medium that can be effectively used by state and non-state actors for nongaming purposes such as intelligence gathering, recruitment, and training.

At this point, it is important to emphasize that the MMOG industry is a nascent phenomenon that emerged only around a decade ago. Therefore, today’s popular MMOGs are still very limited by the present-day technologies. For instance, there is still a big trade-off between realistic graphics and game play sophistication, because the current processing powers and connection speeds do not allow for a better option.

Another limitation of MMOGs that could be mentioned here is the non-random representation of the real life population in VWs. Considering that the average profile of MMOG players significantly differs from the real world population as to their ethnic background, gender, age, and annual income, MMOGs



USE OF MASSIVELY MULTIPLAYER ONLINE GAMES FOR INTELLIGENCE GATHERING...

do not lend themselves perfectly to the concerning nongaming purposes.

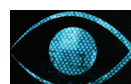
Finally, it is also worth noting that there are, and probably will always be, some essential differences between VWs and the real world. No matter how much investment is made in an avatar in terms of time, effort, and virtual currencies, the tragedy of losing an avatar in an MMOG will not be comparable to a loss of human life in the real world.

However, as new technologies emerge and the current ones are developed, the distinction between the real and virtual worlds is expected to blur further. Moreover, globalization dynamics in combination with cheaper technologies could lead to a better representation of real world populations in VWs. Therefore, the aforementioned limitations of MMOGs could be expected to decrease in importance as time goes by.

All in all, MMOGs appear to be a promising venue of investment for those who aspire to compete as powerful actors in tomorrow's world.

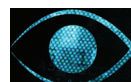
REFERENCES

- [1] H. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*. Kenneth Thompson (ed.), New York: McGraw Hill, 1985, p. 57.
- [2] W. S. Lind, K. Nightengale, J. F. Schmitt, J. W. Sutton, and G. I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989, pp. 22-26.
- [3] M. Castells, *The Information Age: Economy, Society, and Culture, Vol. I: The Rise of the Network Society*. 2nd Edition, United Kingdom: Wiley-Blackwell, 2010.
- [4] P. N. Howard, "The Arab Spring's Cascading Effects," *Pacific Standard* [Online], February 23, 2011. Available: <http://www.psmag.com/navigation/politics-and-law/the-cascading-effects-of-the-arab-spring-28575/>
- [5] H. Kendircioğlu, T. Kaymazlı, A. A. Eker, "Irregular Warfare with Cyber Means," *ISCTurkey 2013 Proceedings*, pp. 274-277, September 2013, p. 276.
- [6] R. Singel, "U.S. Spies Want to Find Terrorists in World of Warcraft," *Wired* [Online], February 22, 2008. Available: <http://www.wired.com/2008/02/nations-spies-w/>
- [7] B. H. Suits, *The Grasshopper: Games, Life and Utopia*. Toronto Buffalo: University of Toronto Press, 1978, p. 34.
- [8] J. McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*. New York: Penguin Press, 2011, p. 21.
- [9] K. Salen and E. Zimmerman, *Rules of Play: Game Design Fundamentals*. MIT Press, 2004, p.80.
- [10] J. Huizinga, *Homo Ludens*. London: Routledge & Kegan Paul, 1949.
- [11] N. Ducheneaut, M.-H. Wen, N. Yee, G. Wadley, "Body and mind: a study of avatar personalization in three virtual worlds," *CHI 2009*, pp. 1151-1160, April 4-9, 2009.
- [12] S. Turkle, "Constructions and reconstructions of self in virtual reality: Playing in the MUDs," *Mind, Culture and Activity*, 1(3), pp. 158-167.
- [13] K. Bessiere, A. Seay, and S. Kiesler, "The ideal elf: Identity exploration in World of Warcraft," *Cyber Psychology & Behavior*, 10(4), pp. 530-535.
- [14] S.-M. L. Whang and G. Chang, "Psychological analysis of online game users," *Proceedings of Human Computer Interaction*, 2, pp. 81-90, 2002.
- [15] S.-M. L. Whang and G. Chang, "Lifestyles of virtual world residents: Living in the online game 'Lineage'," *Cyber Psychology & Behavior*, 7(5), pp. 592-600, 2004.
- [16] K.-K. R. Choo and R. Smith, "Criminal exploitation of online systems by organised crime groups," *Asian Criminology*, 3, pp. 37-59, 2008.
- [17] E. Castronova, *Synthetic Worlds: The Business and Culture of Online Games*. Chicago and London: University of Chicago Press, 2005, p. 147.
- [18] Gartner News Release, "Gartner Says Spending on Gaming to Exceed \$74 Billion in 2011," July 5, 2011. Available: <http://www.gartner.com/newsroom/id/1737414>
- [19] Global Collect Research Report, "The Global MMO Games Market: Payments, Intelligence and Trends," July 2, 2013. Available: http://info.globalcollect.com/Portals/141744/docs/GlobalCollect_Global_MMO_Games_Market_report_03.pdf
- [20] Newzoo Market Research Report, "MMO Trend Report", November 25, 2011. Available: <http://www.newzoo.com/trend-reports/mmo-trend-report/>
- [21] V. C. Gaziz, "Video gaming: the sociology of a lifeworld," *published PhD thesis*, 2012.
- [22] R. B. Chen, H. S. Mahmassani, H. Yun, N. Contractor, D. Williams, "Travel and activity behaviors in virtual world environments," *TRB 89th Annual Meeting Compendium of Papers DVD*, 2010.
- [23] K. Graft, "Blizzard Wins \$88M Judgment Against WoW Private Server Owner," *Gamasutra* [Online], August 16, 2010. Available: http://www.gamasutra.com/view/news/29936/Blizzard_Wins_88M_Judgment_Against_WoW_Private_Server_Owner.php
- [24] "Online gamers rehearse real-world epidemics," *Sydney Morning Herald* [Online], August 21, 2007. Available: <http://www.smh.com.au/news/Technology/Online-gamers-rehearse-realworld-epidemics/2007/08/21/1187462217489.html>
- [25] R. D. Balicer, "Modeling infectious diseases dissemination through online role-playing games," *Epidemiology*, 18(2), pp. 260-261, March 2007.
- [26] E. T. Lofgren and N. H. Fefferman, "The untapped potential of virtual game worlds to shed light on real world epidemics," *The Lancet Infectious Diseases*, 7, pp. 625-629, 2007.
- [27] D. Thier, "World of Warcraft Shines Light on Terror Tactics," *Wired* [Online], March 20, 2008. Available: http://archive.wired.com/gaming/virtualworlds/news/2008/03/wow_terr_or
- [28] "Children play Israeli-killers in bloody new computer game," *Daily Mail* [Online], August 17, 2007. Available: <http://www.dailymail.co.uk/news/article-475966/Children-play-Israeli-killers-bloody-new-game.html>
- [29] P. Johnson, *Second Life, Media, and the Other Society*. New York: Peter Lang Publishing, 2010, p. 185.
- [30] A. J. Wharton. (2009, August). Shaping the 'public sphere' in Second Life: Architectures of the 2008 U.S. Presidential Election. *Journal of Virtual Worlds Research* [Online], 2(2). Available: <https://journals.tdl.org/jvwr/index.php/jvwr/article/view/411>
- [31] C. Kohler, "John Edwards' Second Life Vandalized," *Wired* [Online], March 01, 2007. Available: http://www.wired.com/2007/03/john_edwards_se/
- [32] *The Use of the Internet for Terrorist Purposes*, United Nations Office on Drugs and Crime, New York, 2012.
- [33] S. Zeller, "Training Games," *Government Executive* [Online], January 01, 2005. Available: <http://www.govexec.com/magazine/features/2005/01/training-games/18341/>
- [34] World Bank Data on Urban Development, 2013. Available: <http://data.worldbank.org/topic/urban-development>
- [35] United Nations Department of Economic and Social Affairs, "World Urbanization Prospects The 2011 Revision", 2012. Available: http://esa.un.org/unup/pdf/WUP2011_Highlights.pdf
- [36] D. Williams and M. Skoric, "Internet Fantasy Violence: A Test of Aggression in an Online Game," *Communication Monographs*, 2005, 217-233, p. 228.
- [37] N. Prucha, "Online Jihad versus Gaming Industry: A Comparative Look at Two Cultural Sub-Groups Online Ventures," *SIAC-Journal*, 2010, 70-80, p. 75.
- [38] J. C. Rosser, Jr, P. J. Lynch, L. Cuddihy, D. A. Gentile, J. Klonsky, R. Merrell, "The Impact of Video Games on Training Surgeons in the 21st Century," *Arch Surg.*, 142, 181-186, p. 182.
- [39] T. J. Richardson, "First Responder Weapons Of Mass Destruction Training Using Massively Multiplayer On-Line Gaming," Naval Postgraduate School, California, 2004. Available: <http://www.ntis.gov/search/product.aspx?abbr=ADA425028>
- [40] C. M. Gorman, "Getting Serious About Games-Using Video Game-Based Learning to Enhance Nuclear Terrorism Preparedness," Naval



Postgraduate School, California, 2012. Available:
<http://www.hsd1.org/?abstract&did=710287>

- [41] G. Jean, "Game Branches Out Into Real Combat Training," *NationalDefense* [Online], February 2006. Available:
http://www.nationaldefensemagazine.org/archive/2006/February/Pages/games_brance3042.aspx
- [42] N. Ungerleider, "Army Tweaks Recruitment Video Game to Train Soldiers for Real 'Hurt Locker' Situations," *Fast Company* [Online], August 03, 2011. Available:
<http://www.fastcompany.com/1771044/army-tweaks-recruitment-video-game-train-soldiers-real-hurt-locker-situations>
- [43] C. Boyd, "US army cuts teeth on video game," *BBC* [Online], November 25, 2005. Available:
<http://news.bbc.co.uk/2/hi/technology/4460082.stm>
- [44] "Spot On: The US Army's There-based simulation," *GameSpot* [Online], April 21, 2004. Available:
<http://www.gamespot.com/articles/spot-on-the-us-armys-there-based-simulation/1100-6093860/>



VoIP Güvenliği Kapsamında DoS Saldırılarının İncelenmesi, Örnek Senaryo Gerçekleştirme ve Güvenlik Politikası Geliştirme

K. Sencar, M. T. Sakallı, İ. M. Taş

Özet— VoIP (Voice over Internet Protocol), internet üzerinden veri paketlerinin iletilmesini sağlayan bir teknolojidir. VoIP'nin, SIP (Session Initiation Protocol) teknolojileri ile birlikte kullanılmaya başlanması ile VoIP teknolojisi, yeni nesil telekom dünyasında popüler hale gelmeye başlamıştır. Bu popülerliğin artması ve kullanım oranlarının yükselmesi ile VoIP/SIP teknolojilerinde güvenlik sorunları ile karşılaşmaya başlanmıştır. VoIP/SIP teknolojisi, IP ağı üzerinden hizmet veren bir servistir ve IP ağı üzerinden hizmet veren diğer servisler gibi Servis Reddi (Denial of Service, DoS) saldırılarından etkilenmektedir. Bu çalışmada VoIP güvenliğinin sağlanabilmesi için VoIP sistemlerde, gerçekleştirilmesi en kolay ancak engellenmesi en zor saldırı türleri, DoS saldırıları ve bu saldırılara karşı geliştirilen önlemler ve teknolojiler incelenmektedir. Buna ek olarak, bir VoIP güvenlik test laboratuvar ortamı kurularak bu ortamda VoIP sistemine çeşitli DoS saldırıları düzenlenmiş ve elde edilen bulgular yardımıyla VoIP sistemleri için DoS saldırılarına karşı güvenlik iyileştirmeleri elde edilerek bu iyileştirmeler, güvenlik tavsiyeleri olarak verilmiştir.

Anahtar Kelimeler— DoS saldırıları, güvenlik politikası geliştirme, VoIP, VoIP güvenliği

Abstract—VoIP (Voice over Internet Protocol) is a technology allowing data packets to be transmitted over the Internet. VoIP technology, together with the use of SIP (Session Initiation Protocol), has started to become more popular in the new generation telecom world. This increase in popularity and usage rates rise began to be faced with security problems in VoIP/SIP technology. VoIP/SIP technology is a service serving over an IP network. Therefore, it is affected by DoS (Denial of Service) attacks like the other services serving over an IP network. In this paper, DoS attacks, the easiest to be realized but the hardest to prevent in VoIP systems, are analyzed. The technologies and policies developed to prevent these types of attacks are discussed. Moreover, the security enhancements for VoIP system against DoS attacks are obtained by using the findings of applied DoS attacks on a VoIP system constructed in a VoIP security test laboratory. These security enhancements are presented as

Kübra SENCAR, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne, sencarkubra@gmail.com
Muharrem Tolga SAKALLI, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne, tolga@trakya.edu.tr
İsmail Melih TAŞ, Netaş, Siber Güvenlik Ar-Ge Departmanı, meliht@netas.com.tr

recommendations to strengthen the security of VoIP systems against DoS attacks.

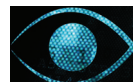
Index Terms— DoS attacks, developing the security policy, VoIP, VoIP security

I. GİRİŞ

VoIP (Voice over Internet Protocol), IP üzerinden ses iletim tekniğidir. Bu teknoloji sayesinde ses, veri paketleri halinde IP (Internet Protocol) üzerinden gönderilebilmektedir. IP üzerinden sesi iletmek, internete ulaşılabilen her yerde, birkaç cihaz ve hatta yalnız yazılımlar yardımı ile sesli görüşme yapabilmek anlamına gelmektedir. VoIP teknolojisinde iletim IP üzerinden yapıldığı için internette oluşan bütün sorunlar ve güvenlik tehditleri bu teknoloji için de geçerli olmaktadır. Sistemde tehdit hedefi olabilecek unsurlar; kullanılan protokoller, VoIP istemci ve sunucu bileşenleri, ağdaki diğer sistemler ile etkileşimini sağlayan çeşitli yazılımlar gibi farklı parametrelerden oluşabilmektedir. Bunların sonucunda VoIP trafiği kötü niyetli kişiler tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir. Bu sorunlar karşısında geliştirilen sistemler, VoIP görüşmelerini daha güvenilir hale getirmeyi hedeflemektedir [1].

VoIP güvenliğinin sağlanabilmesi ve VoIP görüşmelerinin daha güvenilir bir hale getirilebilmesi için VoIP sistemlerde, çok sık rastladığımız DoS (Denial of Service) saldırılarına karşı VoIP sistemlerinin zafiyetlerinin incelenmesi gerekmektedir. Böylece düşük maliyet, etkili bant kullanımı ve telefon servislerine yeni internet servislerinin (IPTV-Internet Protocol television-, video, konferans, ...) eklenme kolaylığı gibi özellikleri ile hem bireysel kullanıcılar hem de kurumsal kullanıcılar için popüler hale gelen VoIP teknolojisinin, DoS saldırılarından minimum düzeyde etkilenmesi amaçlanmıştır.

Bu çalışmada, VoIP teknolojilerine karşı gerçekleştirilen saldırılardan sık olarak rastlanan, DoS saldırıları incelenmektedir. VoIP güvenliği kapsamında, SIP tabanlı sistemlerin DoS saldırılarına karşı duyarlılıkları test edilmektedir. Testten elde edilen sonuçlar ile DoS saldırılarına karşı daha güvenli ürünlerin geliştirilmesi için fikir verilmekte, en iyi uygulama senaryolarını ve güvenlik politikalarını geliştirirken dikkat edilmesi gereken noktalara değinilmektedir.



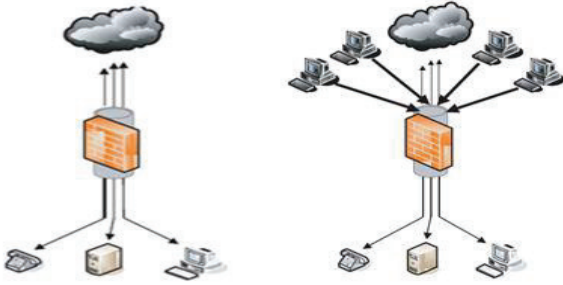
II. VoIP DoS SALDIRILARI

Bu bölümde VoIP mimarisinde karşılaşılan saldırılardan, gerçekleştirilmesi en kolay ancak engellenmesi en zor saldırı türlerinden olan, DoS saldırıları incelenmektedir.

VoIP teknolojisinde güvenli protokoller, destekleyici servisler ve cihazlar kullanılması durumunda bile VoIP mimarisinde servis engellemeye yönelik güvenlik açıkları oluşabilir. Bu durum VoIP mimarisinde tam bir koruma sağlanması önler.

DoS saldırısı, IP temelli ağları hedef alır. Bu saldırılar, sistemin çalışmasına küçük etkiler oluşturabileceği gibi, sistemi tamamen kullanılamaz hale de getirebilir. DoS saldırıları, farklı harici kaynaklardan çok sayıda veri paketi gönderilerek, sistemin tüm çağrıları karşılayamaması esasına dayanır. Bu saldırılarda, servisin etkisiz hale getirilmesi için bant genişliği ve CPU hedef alınır.

Şekil 1’de DoS saldırısına maruz kalan bir sistem gösterilmektedir. Şeklin ilk bölümünde normal bir trafik akışı, ikinci bölümünde ise saldırganlar tarafından oluşturulan trafiğin kullanıcıları nasıl etkilediği gösterilmektedir.



Şekil 1. DoS Saldırısı [1]

DoS saldırılarına karşı korunmak zordur. Çünkü VoIP, IP ağı üzerinden hizmet veren bir servistir ve IP üzerinden hizmet veren diğer servisler gibi DoS saldırılarından etkilenirler. Buna ek olarak DoS saldırıları özellikle VoIP gibi gerçek zamanlı veri akışının gerçekleştiği servislerde etkili olurlar. Çünkü bu servisler, ağın anlık durumuna karşı daha hassastır.

Günümüzde DoS saldırılarını gerçekleştirmek için kullanılan araçların kullanımlarında iyileştirmeler yapılarak, bu araçların kullanımları basitleştirilmiştir. Bu basitleştirme ile DoS saldırılarını gerçekleştirmek için kullanılan araçlar, popüler hale gelmeye başlamıştır. Araçlardaki popülerliğin artması ile Flood tabanlı DoS saldırıları daha sık görülmeye başlanmıştır.

DoS saldırılarının bir türü olan Flood tabanlı saldırılar, VoIP ağı içerisindeki çeşitli bileşenlerin etkisiz hale getirilmesini amaçlar. Bu saldırıda, çok sayıda paket gönderilerek kullanıcıların hizmet alması zorlaştırılır veya tamamen engellenebilir. Bu saldırılarda saldırgan,

kullanılabilir olan tüm ağı ya da sistem kaynaklarını (bant genişliği, CPU, vb.) tüketmeye çalışır. Flood tabanlı saldırılar hedeflerine bağlı olarak VoIP uygulamalarını farklı şekillerde etkileyebilmektedir. Aşağıda Flood tabanlı DoS saldırılarının türleri gösterilmektedir.

- UDP (User Datagram Protocol) Flood Saldırısı,
- TCP (Transport Control Protocol) SYN (Synchronize) Flood Saldırısı,
- ICMP (Internet Control Message Protocol) Flood/Smurf Saldırısı.

A. UDP Flooding Saldırısı:

UDP kaynak adresleri saldırganlar tarafından kolayca taklit edilebilmektedir. Bu nedenle Flood saldırıları içinde tercih edilen bir türdür. UDP Flooding saldırısı, uzaktaki bir bilgisayarın portlarına çok sayıda rastgele UDP paketi gönderilerek başlatılmaktadır. Böyle bir durumda saldırıya uğrayan makine;

- Portu dinleyen bir uygulama var mı diye kontrol eder,
- Hiçbir uygulamanın portu dinlemediğini görür,
- ICMP “Hedefe ulaşamıyor” paketi ile cevap verir.

Bu nedenle, çok sayıda UDP paketi gönderilmesi durumunda, kurban sistem de yanıt olarak çok sayıda ICMP paketi göndermeye zorlanır. Bu da kurban sistemin diğer istemciler tarafından erişilemez hale gelmesine yol açmaktadır. Saldırgan paketlerinde, sahte IP adresleri olabilir, bu durum geri dönen ICMP paketlerinin saldırganı ulaşmamasını sağlar ve saldırganın bağlantı konumunu anonimleştirir [8].

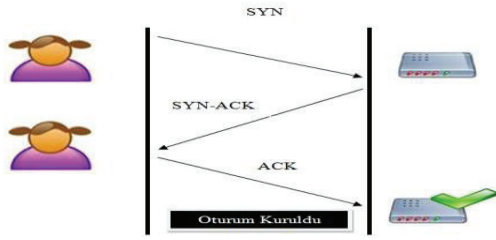
B. SYN Flood Saldırısı:

SYN Flood saldırısı DoS saldırılarından en bilineni, en sık karşılaşılanı ve en kolay gerçekleştirilenidir. Bu saldırıda, bir saldırgan sistemin yasal trafiğini isteklere cevap veremeyecek duruma getirmek için yeterli sunucu kaynaklarını tüketme girişiminde bulunarak, hedef alınan sisteme ardışık SYN istekleri göndermektedir.

Normalde bir istemci, sunucuya TCP bağlantısı başlatma isteğinde bulunduğu, sunucu ve istemci arasında bir dizi mesaj değiş-tokuşu yaşanmaktadır. Buna TCP üçlü el sıkışması denir ve standart bir TCP üçlü el sıkışmasının içeriği aşağıdaki gibidir.

- TCP istemcisi sunucuya bir SYN paketi gönderir.
- Sunucu, bu isteği bir SYN-ACK paketi ile cevaplar.
- İstemci, sunucuya bir ACK paketi gönderir.

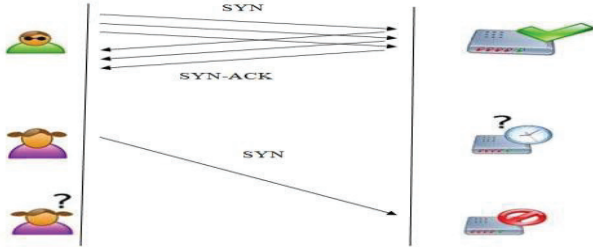
Şekil 2’ de istemci, normal bir TCP bağlantısı başlatma isteğinde bulunduğu gerçekleşen TCP üçlü el sıkışması gösterilmektedir.



Şekil 2. Normal bir TCP bağlantısı

SYN Flood saldırısında, saldırgan internet üzerinden kullanılmayan IP adreslerini kullanarak birçok SYN paketini hedef makineye yollar. Hedef makine, alınan her SYN paketi için kaynak ayırır ve bir onay paketini (SYN-ACK), SYN paketinin geldiği IP adresine yollar. Hedef makine, sahte kaynaktan ACK mesajı almak için bir süre bekler. Bu saldırının dönüm noktasıdır çünkü sahte IP adresinden hedef makineye hiçbir zaman ACK paketi gönderilmeyecektir. Hedef makine, kullanılmayan IP adresinden yanıt alamayacağı için SYN-ACK paketini defalarca tekrarlar. Saldırgan bu yöntemi üst üste tekrarladığında mevcut tüm kaynaklar tüketilir ve hedef makine yeni bir bağlantıyı daha kaldıramaz hale gelir. Bu nedenle diğer istemciler makineye bağlanamaz [5].

Şekil 3'te kendini gizlemek için sahte IP adresi kullanan bir saldırganın hedef sisteme, kapasitesinden fazla gönderdiği SYN paketleri ile gerçekleştirilen flood saldırısı gösterilmektedir.



Şekil 3. SYN Flood Saldırısı

Bu saldırı, bağlanan istemcilerin herhangi bir kimlik denetimi mekanizmasından geçmemesinden kaynaklanır. SYN paketlerini alan hedef makine, paketleri gönderen istemci taraf onaylanmadan kaynak ayırır. Bu da mevcut tüm kaynakların tükenmesine ve hedef makineye diğer istemcilerin bağlanamamasına neden olur [5].

C. ICMP Flood/Smurf Saldırıları:

Smurf saldırısında, saldırgan ağda kurban olarak seçtiği bilgisayarın IP adresini taklit ederek, ağdaki diğer bilgisayarlardan ping isteğinde bulunur. Bu ping paketi, kurban makinenin IP'sinden geliyormuş gibi görünecek şekilde hazırlanmıştır. Bu durumda ağ üzerindeki bütün makineler, kurban makineye ping atar. Hedef makine bu trafiği karşılayamaz ve bağlantı kesilir.

Saldırgan belirlediği çok sayıda makineye ping komutu göndermektedir. Ancak saldırgan, "IP Spoofing" yöntemi ile istek gönderen kaynak adreslerini, hedef makinenin IP adresi olarak değiştirir ve istek gönderilen tüm ağdaki makineler istediği hedef makineden geldiğini düşünerek bu makineye cevap dönerler. Bu durumda çok sayıda makine, hedef makineye aynı anda çok sayıda cevap gönderir ve hedef makine kilitlenerek normal hizmet vermemeye başlar.

III. FLOOD TABANLI DoS SALDIRILARI İLE İLGİLİ ÇALIŞMALAR

Bu bölümde, VoIP Pentest laboratuvar ortamı kuralarak, güvenlik zafiyet testlerinin uygulanması için DoS saldırıları düzenlenmiştir. Tüm çağrı, doğrulama ve güvenlik testleri Trixbox IP-PBX sistemi üzerinde ile gerçekleştirilmektedir. Sanallaştırma çözümü için Oracle Virtual Box ürünü kullanılmıştır. Güvenlik testleri sırasında Backtrack Linux dağıtımı içerisindeki VoIP güvenliği ile ilgili çeşitli yardımcı araçlar ve kütüphanelerden yararlanılmıştır. Ağ trafik ve protokol analizi için Wireshark ürünü kullanılmıştır. Hping aracı kullanılarak istenen TCP ve ICMP paketleri IP spoofing (yanıltma) özelliği kullanılarak DoS saldırılarının simüle edilmesi kullanılmıştır.

Flood tabanlı DoS saldırılarında, saldırgan kullanılabilir olan tüm ağı ya da kaynak sistemlerini tüketmeye çalışır. Sistemlerin Flood tabanlı DoS saldırılarından minimum düzeyde etkilenmesi için gereken güvenlik politikasının oluşturulabilmesi için bu saldırıların detaylı bir şekilde incelenmesi gerekmektedir. Bu çalışmada, TCP SYN Flood ve ICMP Flood/Smurf DoS saldırıları üzerinde durulmaktadır:

A. TCP SYN Flood Saldırıları:

SYN Flood saldırısının amacı, hedef sisteme kapasitesinden fazla SYN paketi göndererek, sistem kaynaklarını hizmet veremez hale getirmektir. Saldırgan sistemin trafiğini isteklere cevap veremeyecek duruma getirmek için sunucu kaynaklarını tüketme girişiminde bulunarak, hedef alınan sisteme ardışık SYN istekleri gönderir.

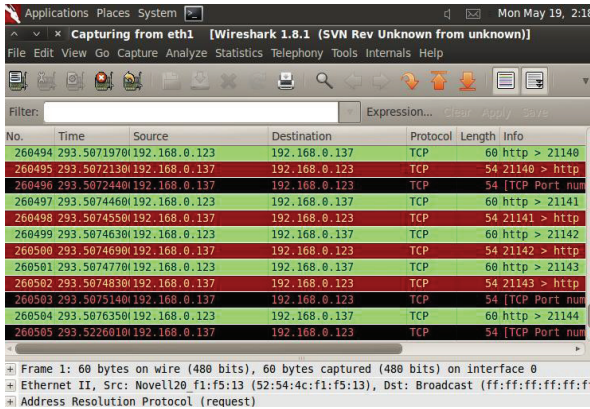
SYN Flood saldırısı TCP protokolünü kullanmaktadır. Hping3 aracıyla gerçek IP adresleri kullanarak SYN Flood saldırısı gerçekleştirmek için "**hping3 --flood -p 80 192.168.0.123 -S**" komut satırı kullanılmaktadır.

Şekil 4'te gerçek IP adresleri kullanılarak, hedef makinenin 80 numaralı portuna, "-S" parametresi ile SYN bayraklı TCP paketlerinin gönderilmesi gösterilmektedir.

```
File Edit View Terminal Help
root@bt:~# hping3 --flood -p 80 192.168.0.123 -S
PING 192.168.0.123 (eth1 192.168.0.123): S set, 40 headers + 0 data bytes
ping in flood mode, no replies will be shown
```

Şekil 4. Hping3 aracıyla gerçek IP adresleri ile SYN Flood saldırısı

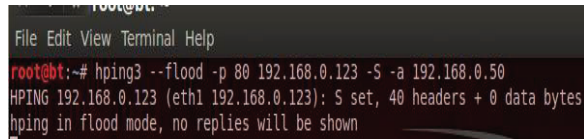
Şekil 5'te Hping3 aracında gerçek IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının Wireshark programı ile izlenmesi gösterilmektedir.



Şekil 5. Gerçek IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının izlenmesi

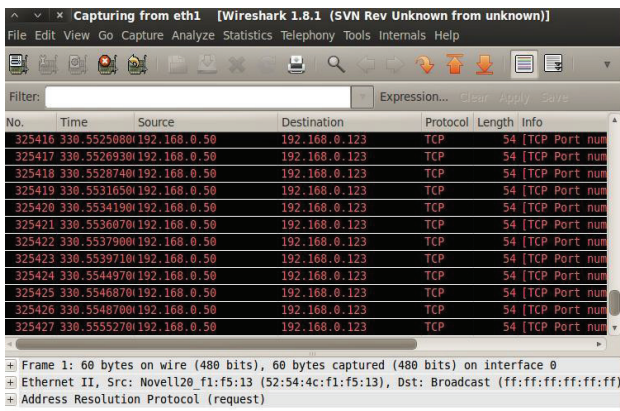
Hping3 aracında sahte IP adresleri kullanarak TCP SYN Flood saldırısı gerçekleştirmek için “**hping3 --flood -p 80 192.168.0.123 -S -a 192.168.0.50**” komut satırı kullanılmaktadır.

Şekil 6'da “-a” parametresi ile taklit edilen kaynak IP adresi ile gerçekleştirilen SYN Flood saldırısı gösterilmektedir. Bu şekildeki 192.168.0.50 IP adresi, sahte IP adresidir.



Şekil 6. Hping3 aracında sahte IP adresleri ile SYN Flood saldırısı

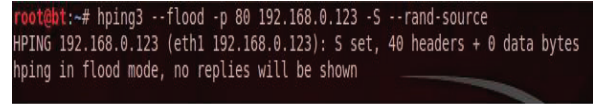
Şekil 7'de Hping3 aracında sahte IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının Wireshark programı ile izlenmesi gösterilmektedir.



Şekil 7. Sahte IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının izlenmesi

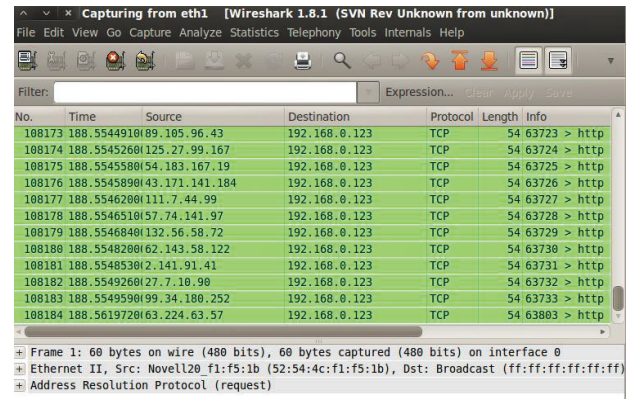
Hping3 aracında random sahte IP adresleri kullanarak TCP SYN Flood saldırısı gerçekleştirmek için “**hping3 --flood -p 80 192.168.0.123 -S --rand-source**” komut satırı kullanılmaktadır.

Şekil 8'de “--rand-source” parametresi ile her biri farklı sahte IP adresleri ile SYN Flood saldırısı gösterilmektedir. Bu şekildeki 192.168.0.50 IP adresi, sahte IP adresidir.



Şekil 8. Hping3 aracında random sahte IP adresleri ile SYN Flood saldırısı

Şekil 9'da Hping3 aracında rastgele sahte IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının Wireshark programı ile izlenmesi gösterilmektedir.



Şekil 9. Random sahte IP adresleri kullanılarak gerçekleştirilen SYN Flood saldırısının izlenmesi

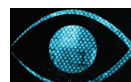
Tablo 1'de, SYN Flood saldırısı gerçekleştirilirken CPU kullanım oranındaki artış gösterilmektedir. Bu saldırının daha uzun süreli uygulanması sonucunda kaynak tüketimi kümülatif olarak artmıştır. Kullanıcıya yapılan çağrılar işleyebilmek için yeterli kaynak kalmayışa kadar uygulandığında sistem yeni taleplere cevap verememiş ve servis dışı kalmıştır.

TABLO 1
SYN Flood saldırısı esnasında CPU kullanım oranı

	CPU Kullanım Oranı
1-2 dakika	%2
3-4 dakika	%9
4-5 dakika	%13

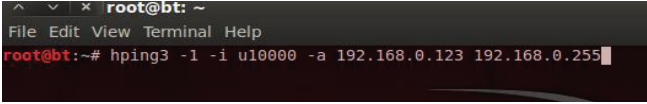
B. ICMP Flood/Smurf Saldırıları:

Smurf saldırısında saldırgan, “IP Spoofing” yöntemi ile istek gönderen kaynak adreslerini, hedef makinenin IP adresi olarak değiştirir. Böylece hedef bilgisayarın IP adresinden, ağır broadcast adresine ICMP isteği gönderilir ve ağ üzerindeki tüm bilgisayarlardan hedef bilgisayara yanıt gönderilmesi sağlanır.



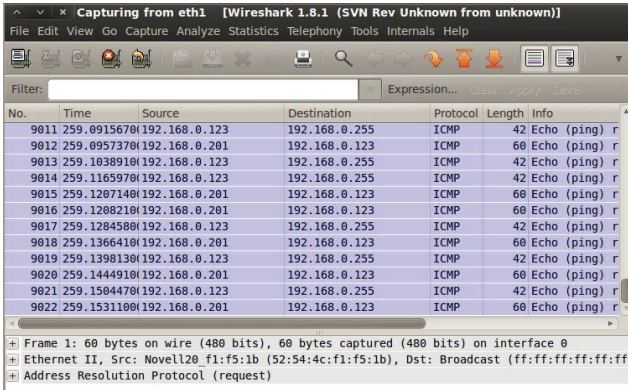
Backtrack’de Smurf saldırısı Hping3 aracıyla gerçekleştirilmektedir. Hping3 aracıyla Smurf saldırısını gerçekleştirmek için “**hping3 -1 -i u10000 -a 192.168.0.123 192.168.0.255**” komut satırı kullanılmaktadır.

Şekil 10’da “-a” parametresi ile taklit edilen IP adresinden “-1” parametresi ile oluşturulan ICMP paketleri gönderilerek gerçekleştirilen ICMP Flood saldırısı gösterilmektedir.



Şekil 10. Hping3 aracıyla Smurf saldırısı

Şekil 11’de Hping3 aracıyla gerçekleştirilen ICMP Flood saldırısının Wireshark programı ile izlenmesi gösterilmektedir.



Şekil 11. Wireshark ile random Smurf saldırısının izlenmesi

Tablo 2’de, ICMP Flood saldırısı gerçekleştirilirken CPU kullanım oranında artış görülmektedir. Bu saldırının daha uzun süreli uygulanması sonucunda kaynak tüketimi kümülatif olarak artmıştır. Kullanıcıya yapılan çağrılar işleyebilmek için yeterli kaynak kalmayacağı kadar uygulandığında sistem yeni taleplere cevap verememiş ve servis dışı kalmıştır.

TABLO II
ICMP Flood saldırısı esnasında CPU kullanım oranı

	CPU Kullanım Oranı
1-2 dakika	%2
3-4 dakika	%9
4-5 dakika	%13

IV. VOIP TEKNOLOJİLERİNİN FLOOD TABANLI DoS SALDIRILARINA KARŞI GÜÇLENDİRİLMESİ

Bölüm 3’te gösterildiği gibi VoIP sistemlerine karşı gerçekleştirilen SYN Flood saldırılarında ve ICMP Flood/Smurf saldırılarında, saldırgan bant genişliğini ya da CPU’yu tüketmeyi hedeflemektedir. Bu bölümde, yapılan çalışmalar sonucunda elde edilen bilgi birikimi ve tecrübeler

kullanılarak kaynak sistemlerinin tüketimini engellemek için alınabilecek önlemler verilmektedir.

A. TCP-SYN Flood Saldırıları İçin Önlemler:

Aşağıda TCP-SYN Flood saldırılarını engellemek ve kaynak sistemlerin tüketimini engellemek için alınabilecek önlemler gösterilmektedir.

- TCP servisleri önüne güvenlik duvarlarının konulması gerekmektedir.
- SYN Cookies (Çerez) özelliğinin kullanılması gerekmektedir. SYN Cookie özelliği aktif edilmiş bir sistemde, gelen SYN paketi için sistemden bir kaynak ayrılmamaktadır. SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanmaktadır. Bu hesaplama “**kaynak.ip + kaynak.port + hedef.ip + hedef.port + x değeri**” şeklinde hesaplanır ve hedefe gönderilir. Hedef son paket olan ACK paketini gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı tekrar kurulur. ISN numarası uygun değilse bağlantı kurulmaz. Böylece taklit edilmiş binlerce IP adresinden gelen SYN paketleri için sistemde bellek tüketilmemiş olur. Bu sayede sistemin SYN flood saldırılarına karşı daha dayanıklı hale gelmesi beklenmektedir.
- SYN Cache (Önbellek) özelliğinin kullanılması gerekmektedir. Dinleme modundaki port, gelen SYN paketlerine belirli boyutlarda bir alan ayırmaktadır. SYN Cache özelliği FreeBSD sistemlerde, gelen SYN paketleri için TCB değerinden daha az yer kaplayan başka bir veri yapısı kullanmayı önermektedir. Böylece sisteme gelen SYN paketlerinde daha az bellek alanı harcandığı gözlemlenmektedir. (Normalde 700 Byte civarı bellek alanı kullanılırken, SynCache ile 160 Byte civarı bellek kullanılır.). Ancak yoğun bir SYN Flood saldırısı gerçekleşirken SYN Cache özelliği de yeterli olmayacaktır. SYN Cache özelliği tek başına etkili bir koruma sağlamamaktadır. Bu nedenle SYN Cookie özelliği ile birlikte kullanılmaktadır. SYN Cookie ve SYN Cache özelliklerinin beraber kullanıldığı sistemlerde SYN Cache özelliği aktif edilmektedir. SynCache belirli bir değerin üstünde SYN paketleri almaya başladığında SYN Cookie devreye girdiği ve sistemin koruma moduna geçtiği gözlemlenmektedir.
- SYN Proxy (Vekil) özelliğinin kullanılması gerektiği gözlemlenmektedir. SYN Proxy, sadece oturum kurulmuş TCP bağlantılarını sunucuya geçirir. Güvenlik duvarlarında ve Syn Cookie özelliğinde sorun yaşandığı durumlarda rahatlıkla kullanılabilir. SYN Proxy, korumaya aldığı sistemlere gelecek tüm SYN paketlerini karşılamaktadır ve üçlü el sıkışma tamamlandıktan sonra paketleri koruduğu sistemlere yönlendirmektedir.

- Rate Limiting yönteminin kullanılması gerekmektedir. Bir IP adresinden 500'den fazla SYN isteği geldiğinde, isteğin geldi IP adresi engellenecekler listesine eklenmektedir ve o IP adresine ait oturum tabloları boşaltılmalıdır.
- Ülkelerin IP bloklarına göre erişim izninin verilmesi gerekmektedir. Saldırı esnasında TCP portunun, tüm dünyaya kapatılıp sadece bulunulan ülkenin IP bloklarına açılması gerekmektedir. Böylece saldırı sırasında yalnızca random IP adresleri üretiliyorsa, bu yöntemin saldırıyı %75-%90 etkisiz hale getirdiği gözlemlenmektedir.

B. ICMP Flood/Smurf Saldırıları İçin Önlemler:

ICMP Flood/Smurf saldırılarını ve kaynak sistemlerin tüketimini engellemek için yönlendirici ve işletim sistemlerinin, broadcast adreslerine gelen ICMP paketlerine cevap vermesi engellenmelidir.

V. SONUÇLAR

VoIP teknolojisi günümüzde popüler bir teknolojidir. Düşük maliyet, etkili bant kullanımı ve telefon servislerine yeni internet servislerinin (IPTV, video konferans vb.) eklenmesi kolaylığı gibi özellikleri ile hem bireysel kullanıcılar hem de kurumsal kullanıcılar için önemli bir teknolojidir. VoIP teknolojisinde birçok güvenlik sorunu bulunmaktadır ve bu güvenlik sorunlarına karşı birçok güvenlik önlemi yer almaktadır.

Laboratuvar ortamında yaptığımız çalışmalar sonucunda, VoIP sistemlerinin DoS saldırılarına maruz kaldığında, sistemin yüksek seviyede bir ağ trafiği oluşmasından dolayı ya da sistem kaynaklarının aşırı tüketiminden dolayı yorulmaya başladığı ve sistemin erişilemez hale geldiği gözlemlenmiştir.

VoIP sistemlerinin DoS saldırılarına maruz kaldığında kolaylıkla servis dışı kalmasını engellemek için alınan önlemler ile sistemin DoS saldırılarından minimum düzeyde etkilenmesi sağlanabilmektedir. Çalışmamız sonucu elde ettiğimiz sonuçlar doğrultusunda;

- SYN Flood saldırılarına karşı SYN Cookies, SYN Cache, SYN Proxy özelliklerinin birlikte aktif edildiği ve Rate Limiting yönteminin kullanıldığı bir güvenlik politikası oluşturularak sistemin %70-%90 korunabildiği,

- ICMP Flood/Smurf saldırısı ile yönlendirici ve işletim sistemlerinin broadcast adreslerine gelen ICMP paketlerine cevap vermesinin engellendiği bir güvenlik politikası oluşturularak sistemin %90-%95 oranında korunabildiği gözlemlenmektedir.

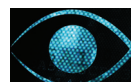
Günümüzde popüler bir teknoloji olan VoIP/SIP teknolojisinin bireysel ve özellikle de kurumsal kullanıcılar için daha vazgeçilmez olabilmesi için VoIP sistemleri henüz konuşlandırma aşamasında iken DoS saldırılarına yönelik güvenlik önlemlerinin alınması tavsiye edilmektedir.

VI. BİLGİLENDİRME

Bu çalışma Netaş tarafından yürütülen TEYDEB 1501 - 3130514 numaralı VGA (VoIP Güvenlik Aracı) projesi tarafından desteklenmiştir.

KAYNAKLAR

- [1] C. Çakır, (2009), "VoIP Teknolojilerinde Güvenlik", Yüksek Lisans Tezi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2009, 238817.
- [2] İ. M. Taş, E. Akça, "SIP Saldırı Teknikleri ve Savunma Yöntemleri", 5. Uluslararası Kriptoloji ve Bilgi Güvenliği Konferansı, ODTU, Ankara, Mayıs 2012.
- [3] P. Thermos, A. Takanen, "Securing VoIP Networks", Pearson Education, Inc., Massachusetts, USA, 2008.
- [4] D. Endler, M. Collier, "Hacking Exposed VoIP: Voice Over IP Secrets & Solutions", McGraw-Hill/Osborne, 2007.
- [5] İ. M. Taş, E. Akça, "Tümleşik Haberleşme Güvenlik Riskleri ve Savunma Stratejileri", NopCon Uluslararası Hacker Konferansı, Bilgi Üniversitesi, İstanbul, Mayıs 2012.
- [6] İ. M. Taş, H. Taş, "VoIP Ağ Güvenliği Perspektifinden Firewall, VoIP IPS ve SBC Karşılaştırması", Bilişim 2012, Ankara, Kasım 2012.
- [7] D. Sisalem, J. Floroiu, J. Kuthan Jiri, U. Abend, H. Schulzrinne, "SIP Security", 2009.
- [8] H. Önal, "DNS Hizmetine Yönelik DoS/DDoS Saldırıları", Ocak 2012 [Online]. Available: http://www.bga.com.tr/calismalar/dns_ddos.pdf
- [9] O. Özbirecikli, "VoIP, SIP Sinyalleşmeye Yönelik Saldırı Uygulamaları, Zafiyet Analizleri ve Güvenlik Önlemleri", Lisans Tezi, Kocaeli Üniversitesi, Mühendislik Fakültesi, Kocaeli, 2013
- [10] B. Şişko, "Oturum Başlatma Protokolü – SIP, İnternet Protokolü Üzerinden Ses – VoIP ve Uygulamaları", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Kasım 2006.
- [11] F. Huici, S. Niccolini, N. d'Heureuse, "Protecting SIP Against Very Large Flooding DoS Attacks", 2010.
- [12] M. Voznak, J. Safarik, "DoS Attacks Targeting SIP Server and Improvements of Robustness", 2012.
- [13] M. Z. Rafique, M. A. Akbar, M. Farooq, "Evaluating DoS Attacks Against SIP-Based VoIP Systems".
- [14] D. Sisalem, J. Kuthan, "Denial of Service Attacks and SIP Infrastructure", Technical University of Berlin, 2007.
- [15] G. Ormazabal, S. Nagpal, E. Yardeni, H. Schulzrinne, "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems", Columbia University, Department of Computer Science, 2010.
- [16] S. Keskin, S. Özgünel, "İnternet Protokolü Üzerinden Ses İletiminde Güvenlik", Yıldız Teknik Üniversitesi, İstanbul, 2007.



Enhancing Totp Protocol By Embedding Current Gps Location

U. A. Abdurrahman, M. Kaiiali and J. Muhammad

Abstract—Static password authentication is no longer considered secure in the internet and banking services. This is because, easy-to-guess passwords such as first-six-digit numbers, names and date of birth are easily uncovered by automated password stealing devices or programs. Multi-factor authentication has been proposed to meet the demand of organizations by providing stronger authentication options to their users. Time-based One-Time Password (TOTP) protocol is one of the widely accepted mechanisms that incorporate multi-factor authentication. TOTP is adopted in Google Authenticator and Windows Authenticator software. However, this protocol has certain limitations; it uses a static shared key and stores it in a clear form into SQLite database (DB) on the mobile device; the timestamp used as a seed to generate the OTP is easy-to-guess; and its mobile app is not PIN protected. Due to these limitations, there is a need to provide a countermeasure to these issues. This paper proposes an enhancement to TOTP by introducing GTOTP. GTOTP generates the OTP based on pre-shared key, timestamp and user's current GPS location. The use of GPS location increases the strength of the generated token by embedding dynamic information (GPS) into the seed used to generate the OTP. The paper discusses different attack scenario to prove that the proposed GTOTP is secure. GTOTP has been implemented and tested. Difficulties of incorporating GPS values into the seed have been addressed.

Index Terms—Multi-Factor Authentication, TOTP, Web Security, Hashing, GPS Applications

I. INTRODUCTION

Today, computing becomes universal, people now are relying on computers to do their business. The internet has become a medium for uncountable e-services on which people perform their business transactions. However, there is a need to provide an utmost protection to the system, the information being sent and the network used to process the information.

Information security refers to the provisions and policies adopted to prevent and monitor unauthorized access, misuse,

modification or denial of a computer network and network-accessible resources [1, 2]. It also involves the authorization of access to data in a network. Users are assigned an ID associated with a chosen password or other authenticating information that allows them to access information and programs within their authority [1].

Traditionally, users tend to use static passwords in securing their systems. However, these passwords suffer potential attacked risks: passwords can be guessed, forgotten, stolen, eavesdropped or deliberately being told to other people. The solution to these problems is by the use of a more secure way of authentication called multi-factor authentication [3]. A multi-factor authentication technology is used to provide higher security guarantee than static passwords.

A multi-factor authentication is an approach for authentication, which requires the use of two or more of the universally recognized authentication factors [4] (as illustrated in Fig. 1):

- 1) A *knowledge* factor: something you know (e.g. password, PIN)
- 2) A *possession* factor: something you have (e.g. smart cards, tokens)
- 3) An *inherence* factor: what you are (e.g. biometrics)
- 4) An optional fourth factor *relatives*: who you know (e.g. brother, wife).



Fig. 1. Multi-factor authentication [5].

So many methods of multi-factor authentication have been presented in the literature in which so many researchers made use of a combination of two or more of the above mentioned factors. One of the multi-factor authentication approaches that is widely in use is SMS-based authentication, where a randomly generated One Time Password (OTP) is sent by

Manuscript received July 30, 2014.

Abdurrahman U. A. is an Assistant Lecturer at the Department of Computer Science, Northwest University, Kano, Nigeria (e-mail: usmanalhaji79@gmail.com).

Mustafa Kaiiali is an Assistant Professor at the Department of Computer Engineering, Mevlana University, Konya, Turkey (e-mail: mkaiiali@mevlana.edu.tr).

Muhammad J. is a Research Assistant at the Department of Computer Engineering, Mevlana University, Konya, Turkey (e-mail: mohdjawadi@yahoo.com).

service providers to the user's mobile phone through an SMS message [6]. This requires additional cost for sending SMSs to all customers who are willing to login. Unlike SMS-based multi-factor authentication, the proposed GTOTP authentication does not require any additional cost.

Nystrom proposed a method of multi-factor authentication using a SecurID which is based on a security device [7]. In this method, each device has a unique seed used to generate a pseudo-random number (OTP) to authenticate the user along with his other credentials. The device is timely synchronized and its seed is stored in the server in order to validate the sent OTP. RSA SecurID [8] is an example of this method (Fig. 2). This approach has an advantage over the SMS-based one as it does not require additional cost for sending SMSs and it is accessible worldwide, unlike SMS-based approach which is limited within the geographic boundaries of a particular country unless the international roaming service is activated. However, for large companies specifically those who offer free services such as Yahoo and Google, it is costly and infeasible to deliver the security device to each customer. Moreover, the device itself may get stolen.

Compared to SecurID, the proposed GTOTP is considered to be more secure as SecurID is based on a fixed seed while the proposed GTOTP will be based on a modifiable pre-shared seed and dynamic GPS location. Moreover, GTOTP is cheaper and easier to deploy, as it does not require a specific security device like SecurID. Nowadays, due to the revolution in smartphone technology, our phones have sufficient applications, gadgets and sensors that can be utilized for secure authentications rather than using specific devices (i. e. SecurID). This reduces the cost and increases the usability.



Fig. 2. RSA SecureID Authentication [9].

Liou, Jing, and Sujith proposed a method similar to SecurID called SofToken that generates a pseudo-random number as an OTP based on a seed shared between the authentication server and a software application installed on the user's computer/mobile [10]. The seed is renewed for every successful login. This approach eliminates the cost of the hardware token; however, it increases the security risk as the new shared seed is sent over non-secure channel so it can be intercepted by an intruder.

Another software based OTP generator has been proposed in [11, 12]. It uses IMEI and IMSI numbers as the seed to generate the OTP. However, IMEI number is not very secure as it is known to the mobile service provider; also IMSI is a cellular network identifier which makes the method not valid worldwide (in case if the user travels worldwide and changes his SIM card accordingly).

Sabzevar, Alireza and Angelos stated a method of using a graphical image to represent a password; the password is entered by pointing on appropriate points of the image, which the user has obtained through his mobile device from the service providers [13]. It has the same drawback of the previous approach as it also depends on particular service provider.

In another paper by Soleymani and Maheswaran who-you-know-based authentication factor was used as the second factor of authentication [14]. This factor is used as a voucher, where a user asks a friend to vouch for him. The user contacts his friend asking for a vouching code which he then uses to log-in to the web page. They make use of user's cellphones to automate this process. Each time a user calls a friend, a token will be generated (vouching) for this contact. A sufficient number of these tokens can be used to authenticate a user. However, this method complicates the authentication process.

Another popular method of authentication currently in use is HOTP/TOTP-based authentication [15]. In this method, an internet user can install an Authenticator App on his mobile phone. This app computes the verification code using a HMAC-based OTP (HOTP) or Time-based OTP (TOTP) as shown in Fig. 3.



Fig. 3. HOTP/TOTP-Based Authentication by Google [16].

With HOTP, the server and client share a secret value and a counter, which are used to compute an OTP independently on both sides. Whenever a password is generated and used, the counter is incremented on both sides, allowing the server and client to remain in sync. This algorithm works based on an increasing counter value (C) and a fixed symmetric key (K) shared between the token generator and the validation system as shown in (1). The Authenticator App uses HMAC-SHA-1 algorithm for the generation of HOTP value [17].

$$\text{HOTP}(K, C) = \text{Truncate}(\text{HMAC-SHA-1}(K, C)) \quad (1)$$

Where the Truncate function extracts 4-byte dynamic binary code out of a 160-bit HMAC-SHA-1 result and then reduces it to modulo 10^{digit} .

On the other hand, TOTP uses the same algorithm as HOTP with one major difference. The counter used in TOTP is replaced by the current time as shown in (2). The client and server remain in sync as long as the system times remain the same. This is done by use of Network Time Protocol. The shared secret key is generated by the server and delivered to the client using a form of QR Code [18].

$$\text{TOTP} = \text{HOTP}(K, T) \quad (2)$$

K is the shared key, T is an integer representing the number of time-steps between the initial counter time T_0 and the Current UNIX Time. T is computed as shown in (3) where X is the time-step in seconds (30 sec by default).

$$T = (\text{Current UNIX Time} - T_0) / X \quad (3)$$

The advantage of this algorithm is that user does not have to be connected with any kind of service provider (Internet, GSM, etc.) to get the verification codes. However, despite being one of the most popular and widely accepted authentication mechanisms, TOTP implementations, such as Google Authenticator and Windows Authenticator, have the following weaknesses:

- 1) It uses a static pre-shared key and stores it in a clear form into an SQLite DB in the mobile device.
- 2) The dynamic part of the seed used to generate the OTP is only the timestamp, which is easy-to-guess.
- 3) The mobile app used to generate the OTP is not PIN protected. So it can be broken if somebody steals the mobile device.

This paper proposes an enhancement to the TOTP protocol (named as GTOTP) by embedding current GPS location in the seed used to generate the OTP. Embedding GPS location in the seed makes it more dynamic and so the OTP will be more secure and harder-to-guess. Table I compares the proposed GTOTP with the previous discussed multi-factor authentication mechanisms.

TABLE I
COMPARING THE DISCUSSED MULTI-FACTOR AUTHENTICATION METHODS

	SMS- Based	SecurID	TOTP	GTOTP
Cost	Not Free	Not Free	Free	Free
Service Access	Restricted	Worldwide	Worldwide	Worldwide
Secure Seed	Fixed	Fixed	Dynamic / Easy to Guess	Dynamic / Hard to Guess
Service Provider	Cellular Network	Not Required	Not Required	Internet
Stolen Device	Not Protected	Not Protected	Not Protected	Protected

The remaining sections of this paper are organized as follows: Section II presents the proposed GTOTP authentication mechanism. Section III discusses the GTOTP implementation issues. Section IV provides a security analysis of the proposed protocol. Section V concludes the paper.

II. GTOTP AUTHENTICATION MECHANISM

GTOTP has five main components: user's initial registration component, a client-side application that runs on smartphones, a database for storing user's standard credentials, a server-side authentication service and a GPS server to track user's GPS location. All of these components are synchronized using NTP Protocol. The GTOTP scheme adopts a user's GPS location in addition to pre-shared key and timestamp to strengthen the security of the generated token. Unlike the static pre-shared key and the easy-to-guess timestamp, GPS location is dynamic, hard-to-guess information that will increase the security of the generated hash.

A. Initial Registration (To be done once)

One of the critical parts that need to be addressed properly in the aforementioned protocol is how to negotiate the shared keys between the user's phone (client) and the server. GTOTP adopts the TOTP way of sharing the key. However, GTOTP requires two shared keys, one to be used as a seed for OTP generation (as in TOTP) and the other to be used for establishing secure channel with the GPS server discussed later. To securely negotiate a shared key, here are the steps:

- 1) The user should enable the multi-factor authentication service from his/her account settings page.
- 2) The server generates the shared key, stores it associated with current user id and presents it on the user's screen in barcode form (Fig. 4 shows the barcode that corresponds to the key: **MA4Q-EUH5-BA7U-XYZC**).
- 3) The user clicks on "scan barcode" button in his/her client app. The phone's default barcode scanner will be launched. The user positions the phone's camera at the barcode appears on his/her computer screen in order to scan it. By doing so, the GTOTP client app learns and stores the shared key.



Fig. 4. Secret Shared Key embedded in a bar code.

B. GTOTP Authentication

After negotiating the secure channel parameters between the authentication server and the user's mobile device. The user can go ahead to access his account any time he/she wants according to the following three steps illustrated in Fig. 5.

1) Initial Authentication:

In this step, the user requests his/her personal web page URL through any internet-enabled device D_1 as shown in Fig. 5. The Web Portal Server S_1 has to respond back to D_1 with the authentication page asking the user to provide his/her traditional credentials (username/password). The user provides his/her credentials to D_1 , which sends them to S_1 for verification. If the user is verified, the system proceeds to the next step.

2) GTOTP Security Token Generation

The GTOTP client app, installed on the user's mobile device D_2 , is used to generate the GTOTP security token based on the following parameters:

- **The Pre-Shared Key:** It is a secret key which has previously been shared between the client and the server during the initial registration process. This parameter is inherited from TOTP.
- **Timestamp:** This is the current time in D_2 . It helps to randomize the seed used to generate the GTOTP One Time Password. It also reduces the risks of replay attacks. This parameter is also inherited from TOTP.
- **GPS Location:** User's current GPS location is another important factor used to strengthen the security token. This factor is unique to the user and very dynamic. While TOTP seed is based on static key and easy to guess timestamp, GPS location increases the seed dynamism and makes it harder to guess. Current GPS location is synchronized with the GPS server through a pre-established secure channel (whose key was negotiated during the initial registration). Therefore, the GPS server keeps track of user's location every time the security token is generated.

All the above-mentioned factors are concatenated to form GTOTP seed. GTOTP keeps using HMAC-SHA-1 algorithm to generate its OTP. HMAC-SHA-1 acts upon the seed and produces a 160-bit message digest. This message digest is further truncated to 6-digits for easy entering by the user. This process results in a security token T_1 (4) that is unique and last for 30 seconds period.

$$T_1 = \text{Truncate}(\text{Hash}(\text{Pre-Shared Key} \parallel \text{GPS} \parallel \text{TS})) \quad (4)$$

At the same time D_2 updates the GPS server (S_2) with the user's GPS location and timestamp (TS) through a secured channel.

3) Token Verification

S_1 receives the security token T_1 and gets the GPS updates of the corresponding user from S_2 . Following that, it generates a security token T_2 . Then it compares T_2 with the one it has received from the user (T_1) as shown in Fig. 6, if they match, the user is authenticated and his/her personal web page is sent back to D_1 .

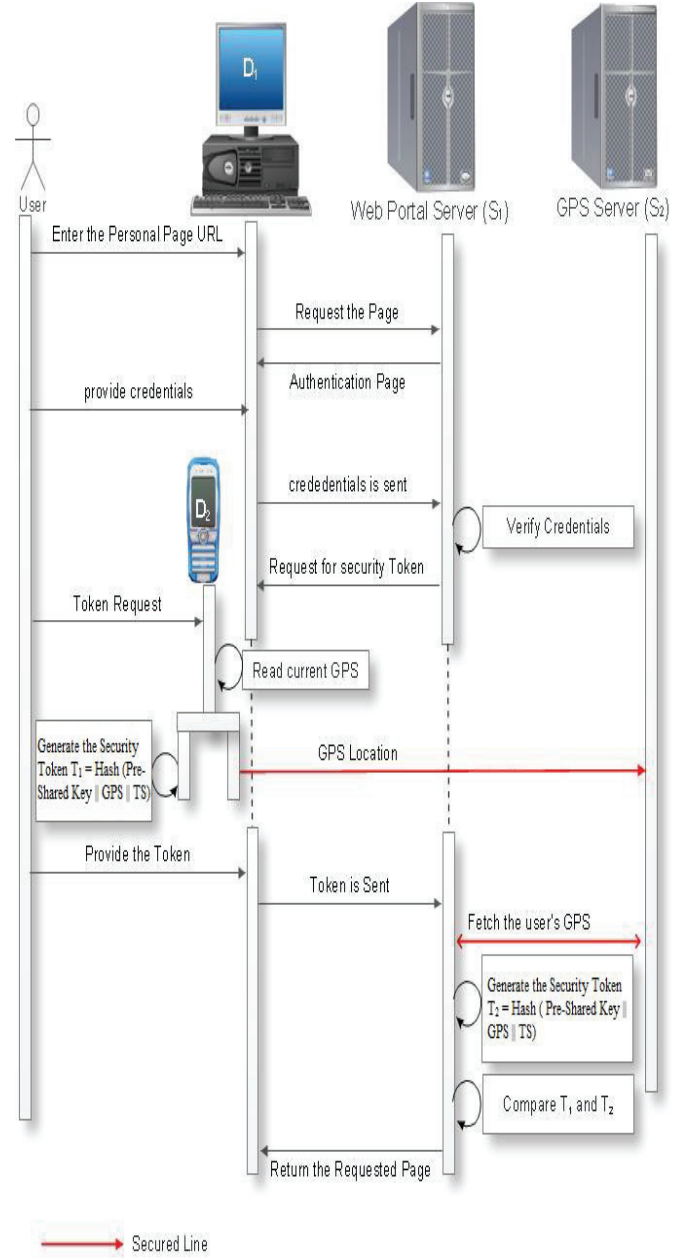


Fig. 5. GTOTP Authentication [3].

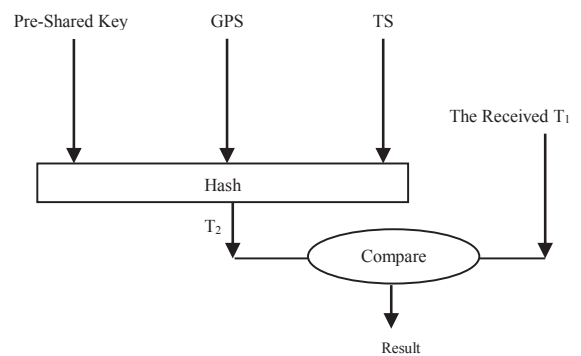


Fig. 6. Token Verification [3].

III. GTOTP IMPLEMENTATION ISSUES

A. Device Theft Countermeasure:

Many TOTP implementations such as: Google Authenticator are not protected against device theft. For that, we have developed the GTOTP client app to be PIN protected in order to mitigate the threat of shared key disclosure by mobile device theft.

B. Shared Key Protection:

TOTP implementations such as: Google Authenticator stores the Pre-Shared Key in a clear form in an SQLite database. This increases the chance of key disclosure using malicious software accessing the database. For that, GTOTP client app stores the shared key encrypted using the user's app PIN as well. Once the app is launched, the user is prompted to provide the PIN, and then the app fetches the encrypted key from the SQLite database and decrypts it using the provided PIN.

C. DYNAMISM:

A shared key = ZO5UJAY5RMH2E72U, a timestamp = 12569537309, and 10 different GPS locations (of approximately 1 km difference each) have been considered and the security token has been computed and depicted in Table II. The experiment shows that for a very small standard deviation (STD) of the GPS values, we get a large STD for the generated security tokens. This shows that for a little change in user's GPS location, there will be a drastic change in the security token. This proves the dynamic effect of the GPS coordinates on the generated token.

TABLE II
STANDARD DEVIATION OF 10 GPS LOCATIONS AND THEIR CORRESPONDENT SECURITY TOKENS FOR A FIXED TIMESTAMP AND SHARED KEY

	Latitude	Longitude	Security Token
Location 1	23.001	32.01	527273
Location 2	23.002	32.02	238761
Location 3	23.003	32.03	579027
Location 4	23.004	32.04	246264
Location 5	23.005	32.05	577068
Location 6	23.006	32.06	624019
Location 7	23.007	32.07	361999
Location 8	23.008	32.08	299430
Location 9	23.009	32.09	639977
Location 10	23.01	32.1	014026
Standard Deviation	0.002872	0.028723	199092.9

D. ACCURACY:

The user's GPS coordinates changes significantly only when he/she changes his/her position to an approximately 10 meters [21]. The dynamism of GPS appears significantly if the user changes his location for more than 10 meters.

E. LATENCY:

The higher the number of satellites a GPS receiver can view the better the accuracy [19]. However, due to so many factors,

like atmospheric effect, multipath effect, etc. a GPS signal reception can be delayed or blocked. Moreover, GPS units typically do not function underwater, indoors, or underground [20]. These factors certainly affect the accuracy of the GPS signals and consequently increase the GPS latency.

For these reasons, our GTOTP implementation is designed to use the previous GPS location of the user to generate the security token in case it finds it difficult to receive a new GPS signals within 30 seconds.

F. PRIVACY:

Using GPS location as a parameter in generating the security token raises the issue of revealing user's location without his/her consent. To overcome this issue, our GTOTP implementation is designed in such a way that, the use of GPS parameter in generating the security token is made optional. GTOTP app gives the user the option to exclude GPS location from the OTP seed; in this case, the app works exactly as the earlier discussed TOTP code generator. The only difference here is that our app is PIN protected and the shared key is stored encrypted.

G. Lost Mobile Device:

If the user has lost his/her mobile device, he/she can no longer access his/her personal web page. To encounter this issue, GTOTP provides an option to pre-register an alternative mobile device (let's say user's wife mobile device) that can be used alternatively in this case. Probably the server has to ask the user extra security questions before it allows him/her to use the pre-registered alternative mobile device.

IV. GTOTP SECURITY ANALYSIS

This section shows how the proposed scheme can resist various threats:

A. Resistance against D1 device hack:

If an intruder gains access to the user system (D₁) and obtain information about his standard credentials (username and password). The intruder still won't be able to log in to the server as he does not have the information required to generate the GTOTP token.

B. Resistance against replay attack:

An intruder obtained information about user's credentials (username and password) and he was also able to intercept the communication between the mobile device and the authentication server to capture the sent token. With the token being made to get expired by time (i.e. 30 seconds) and by first use (valid to be used for one time only), the intruder won't be able to use the captured token even within its lifetime as it has already been used by the user.

C. Using one-way hash function:

Assuming the intruder has the user's fixed credentials (username and password) and he/she was also able to know the user's current GPS location (being his/her colleague). Still he/she cannot generate a valid token as he does not have the

Pre-Shared Key. The Pre-Shared Key has never been transmitted over any channel during authentication. Since the used hash function is a one-way and pre-image resistance function, there is no way for the intruder to get the Pre-Shared Key out of a sniffed token.

D. Using PIN protected app:

If an intruder has stolen the user's mobile phone and has already obtained the user's fixed credentials (username and password), for this scenario, we made the GTOTP client app a PIN protected app, unlike Google Authenticator. Therefore, the intruder would not be able to use the app as far as he does not know its PIN.

V. CONCLUSION AND FUTURE WORK

This paper highlights the TOTP limitations and addresses them by introducing an enhanced protocol called GTOTP. It incorporates the GPS parameter in the seed, which makes it more dynamic and increases the strength of the generated token as well. So many multi-factor authentication approaches have been discussed in the literature. However, each of them has certain security issues in one way or another: either it is easy to compromise; or difficult to implement; or requires an additional cost of obtaining a special device. Our GTOTP makes use of mobile phone (that is common to all users) to generate security tokens (OTPs). This method has been effectively implemented on Android, tested and proved to be robust and secure. An overview of the various parts of the system has been provided in the paper. Additionally, a security assessment was also carried out.

As for further work, the GTOTP algorithm can be extended to include user's biometric parameter to increase the security of the system. Also GTOTP has to be implemented on Blackberry, Apple and Windows mobile phones to provide a wider range of support.

REFERENCES

- [1] "Network Security", http://en.wikipedia.org/wiki/Network_security
- [2] User, Assurance, and Audit Planning. "An Introduction to Computer Security: The NIST Handbook." (1995).
- [3] Abdurrahman, U. A., Kaiiali, M., & Muhammad, J. (2013, November). A new mobile-based multi-factor authentication scheme using pre-shared number, GPS location and time stamp. In *Electronics, Computer and Computation (ICECCO), 2013 International Conference on* (pp. 293-296). IEEE.
- [4] Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. "Multi-Factor Authentication." U.S. Patent No. 20,130,055,368. 28 Feb. 2013.
- [5] "Secure Your Future Now", <http://info.softexinc.com/bid/54466/Data-Breach-should-you-be-concerned>
- [6] Alzomai, Mohammed, Bander AlFayyadh, and A. Josang. "Display security for online transactions: SMS-based authentication scheme." *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*. IEEE, 2010.
- [7] Nystrom, M. "The SecurID (r) SASL Mechanism." (2000).
- [8] "SecurID", <http://en.wikipedia.org/wiki/SecurID>
- [9] "RSA's Recent Compromise", <http://www.thewestbrooks.com/bruce/techblog/2011/03/21/409>
- [10] Liou, Jing-Chiou, and Sujith Bhashyam. "A feasible and cost effective two-factor authentication for online transactions." *Software Engineering and Data Mining (SEDM), 2010 2nd International Conference on*. IEEE, 2010.
- [11] Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE, 2009.
- [12] Eldefrawy, Mohamed Hamdy, Khaled Alghathbar, and Muhammad Khurram Khan. "OTP-Based Two-Factor Authentication Using Mobile Phones." *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*. IEEE, 2011.
- [13] Sabzevar, Alireza Pirayesh, and Angelos Stavrou. "Universal multi-factor authentication using graphical passwords." *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on*. IEEE, 2008.
- [14] Soleymani, Bijan, and Muthucumaru Maheswaran. "Social authentication protocol for mobile phones." *Computational Science and Engineering, 2009. CSE'09. International Conference on*. Vol. 4. IEEE, 2009.
- [15] "TOTP", <https://tools.ietf.org/html/rfc6238>.
- [16] Borchert, Bernd, and Max Günther. "Indirect NFC-Login."
- [17] "HOTP", <https://tools.ietf.org/html/rfc4226>
- [18] "Google Authenticator", <http://code.google.com/p/google-authenticator/wiki/KeyUriFormat>
- [19] Zhang, Pei, et al. "Hardware design experiences in ZebraNet." *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004.
- [20] Tan, Hwee-Pink, et al. "A survey of techniques and challenges in underwater localization." *Ocean Engineering* 38.14 (2011): 1663-1676.
- [21] LaMarca, Anthony, et al. "Place lab: Device positioning using radio beacons in the wild." *Pervasive computing*. Springer Berlin Heidelberg, 2005. 116-133.



End-to-end Encrypted Communication Between Multi-device Users

Halil Kemal Taşkın, Murat Demircioğlu and Salim Sarımurat

Abstract—The rapid growth of the mobile device industry has led people to start to use more than one device (smart phones, tablets, laptops etc.) and this results in a multi-device environment. People often tend to use more than one device in their daily lives by switching between them or using them simultaneously. From the security point of view, end-to-end encryption is a problem in multi-device environment. Known applications are lack of multi-device end-to-end encryption schemes and have some known issues [4].

In this paper, we present a new protocol that allows end-to-end encrypted communication, multi-device user synchronization with offline key exchange capability. Our protocol can be deployed on cloud services without compromising the security requirements.

Index Terms—Multi-device Users, Mobile Devices, Private Communication, End-to-end Encryption, Cloud Computing.

I. INTRODUCTION

INTERNET became the state of art communication tool between people. In its early stages, instant messaging (ICQ, IRC, MSN etc.) was the first major communicator and after that e-mail became more popular. But, with the growth of mobile devices, instant messaging, again, became the major communication way for people.

Instant messaging using mobile devices was a game changer since it allowed people to communicate in realtime at anywhere and anytime. Also, mobile technologies brought the cloud technologies more popular so every data could be reached from anywhere. On the other hand, from security point of view, instant messaging over cloud networks had privacy issues since your data could be easily sniffed or intercepted over the cloud network. There are several cryptographic solutions for end-to-end encrypted communication. OTR based protocols [1], [2] and ZRTP [3] are some of the popular protocols used for this purpose. Using end-to-end encryption, relaying servers or other third parties that have access to network between the communicating parties can not intercept or sniff the messages sent through the network.

However, people start to use more than one device (smart phones, tablets etc.) and this resulted in a multi-device environment. In a multi-device environment, users expect that any

message sent to any device of a user should be synchronized instantly to all devices of the user. People use their devices in their daily lives by switching between them or using them simultaneously. So synchronization between these devices by preserving end-to-end encryption capabilities is an important problem. Cloud based services are easiest and cheapest solutions for network infrastructures. Thus, preserving these security properties using a cloud based service is also an important problem.

Conventional end-to-end encryption protocols don't support synchronization of messages when one party on the communication is a multi-device user. Instant messaging applications such as Whatsapp, Viber and Facebook Messenger are widely used but their protocols are not known clearly and they are mostly lacking end-to-end encryption schemes. Applications like TextSecure, Threema and Telegram claims that they use end-to-end encryption. But, they all are lack of multi-device environment capabilities. Apple's iMessage service is the only one which handled both multi-device user environment and end-to-end encryption capabilities. But recent studies [4] showed that the protocol is vulnerable to a man-in-the-middle attack that could be executed by the relaying servers which totally destructs the end-to-end encryption flavor.

In this work, we present a new end-to-end encryption protocol which allows multi-device user synchronization with offline key exchange capability and is resistant against man-in-the-middle attacks. End-to-end encryption is achieved in such a way the protocol could easily be deployed on a cloud based service without compromising the security requirements.

We give the abstract protocol details. Some parameter and format selection is up to implementation. In Section II, we state the security requirements for the concerns mentioned above. Our protocol details are given in Section III. Finally, Section IV concludes our work.

II. SECURITY REQUIREMENTS

In our protocol we have some assumptions that enables security features. Below, these security requirements and concerns are discussed. Also, details of how we use them in our protocol is given.

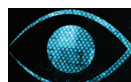
- **End-to-end Encryption Flavor:** End-to-end encryption is the major aim of our work. All data leaving a client must be encrypted in such a way that the cloud service operators have no knowledge of the message content. Thus, our protocol makes use of Public Key Cryptography (PKC) for exchanging keys before the communication starts.

H.K. Taşkın and M. Demircioğlu are with the Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University.

H.K. Taşkın, M. Demircioğlu and S. Sarımurat are with Oran Information Technologies.

S. Sarımurat is with the Department of Computer Science and Engineering, Sabancı University.

This research is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under the project number TEYDEB-1130063 titled "Mobil Terminaller Üzerinde Kriptografik Yöntemler Kullanılarak Uçtan Uca Güvenli Bir İletişim Sisteminin Tasarlanması ve Geliştirilmesi".



- **Private Key Distribution:** In a multi-device environment with PKC, it is essential to have the long term private key on all devices. The easiest way to distribute data including private keys is to store them on the cloud in an encrypted way that server should not be able to decrypt data.
- **Server-side Security:** The data stored on the server should be resistant against brute force and dictionary attacks. In our implementation we use double scrypt [10] key derivation function with salting to store user password. Server is also responsible for the message delivery. For every user there should be a storage quota on the server, higher quotas mean more messages and key parts users can store.
- **Offline Key Exchange:** To establish a key exchange in a conventional end-to-end encryption scheme, both parties have to be online. But in a mobile environment this could not be always possible because of its asynchronous nature. Thus, we introduce a proper way of key exchange while two parties don't require to be online at the same time. We store signed Diffie-Hellman key parts on the cloud and make use of them when needed. Size of the short term key list is optional. It can be changed due to the increasing load of messages. In our implementation it is fixed to 1024.
- **Re-keying:** To achieve forward secrecy, session keys should be updated in a regular interval. In our protocol re-keying is handled in a similar way as it is done in [1]. Also, when the long term private key compromised, it should not be possible to recover previous session keys. To achieve this, we use long term keys only for signing key exchange process.
- **New Device Addition:** In a multi-device environment new devices should be easily added and removed from the user's account. But authentication is also an important issue. We require two-factor authentication when a device is registered. There is no maximum limit for devices but it can be limited up to implementation.
- **Certificate Pinning:** For client-server communication we use certificate pinning for TLS. This approach provides two major advantages. First, there is no need for a trusted third party such as CAs. Secondly, even legitimate authorities (with a valid certificate) can not intercept the network traffic between client and server. For client-client verification we use offline verification settings. Offline verification could be done in several ways such as using QR codes, mnemonics and text-based verification. Details of offline verification techniques are out of scope of this paper.
- **Two-factor Authentication:** The server only requests username and password. All user data in the cloud is stored by encrypting with user password. Thus, even we use state-of-art scrypt key derivation function, security depends on the user password meaning a strong password is required for better protection against the issues in Section II. Also, two-factor authentication is required for clients to register. If a user registers first time, an SMS OTP is used for authentication. If a user is adding a new

client to its account, OTP data is sent to its previous clients over the application itself.

- **Local Disk Encryption:** Any data that is stored on the client should be encrypted. This includes private keys. Methods used for this purpose is out of scope of this paper. But we assume all clients use local disk encryption.

III. THE PROTOCOL

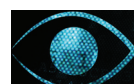
In this chapter, we give the details of our protocol. In our assumption, two parties which want to communicate with each other have multiple devices and they are all connected to a centralized server infrastructure. All communication between devices are relayed over this infrastructure.

From the cryptographic point of view, restrictions of the mobile devices are important due to cryptographic operations are the major performance bottlenecks of the systems. Therefore, protocols and algorithms that have small footprint and fast implementations are needed for mobile environments. Specifically, asymmetric operations require most cpu power. Thus, we acted carefully while selecting the algorithms. Our cipher suite is as follows:

- Signing algorithm: Ed25519 [5]
- Key exchange algorithm: Curve25519 [6]
- Symmetric encryption algorithm: ChaCha20 [7]
- Message authentication code: Poly1305 [8]
- Hash function: Keccak [9]
- Key derivation function: scrypt [10]
- Operating system's Cryptographically Secure Random Number Generator (CSRNG) is used for random number generation.

We use the following notations throughout the paper.

- A and B are the public pseudonyms (usernames) for the parties (users).
- A client is the mobile device (and application in it) that the user is interacting with.
- A has m devices: $A_0, A_1, \dots, A_{m-1}$
- B has n devices: $B_0, B_1, \dots, B_{n-1}$
- S is the centralized server.
- $||$ is concatenation.
- MSB n -bit of m is the most significant n -bit of m .
- LSB n -bit of m is the least significant n -bit of m .
- e_X and d_X are Ed25519 public and private keys used for signing/verification operations of part X , respectively.
- $[m]_{d_X}$ is the signature of message m signed by part X .
- $\{s_m\}_{e_X}$ is the verification operation of signature s for message m with part X 's public key.
- $H(m)$ is the KECCAK-256 hash function of message m .
- $KDF(pwd, salt)$ is the scrypt 512-bit key derivation function with user password pwd and 128-bit nonce $salt$.
- $EncMac_{K,IV}(m)$ and $DecMac_{K,IV}(m)$ are ChaCha20-Poly1305 authenticated encryption and decrypt-and-verify algorithms with message m , 256-bit key K and 64-bit initialization vector IV , respectively. The generated authentication tag is 128-bit and appended to the ciphertext.



A. Server Details

We assume that the centralized server can be deployed using cloud based services. As message communication backend we use XMPP [11]. XMPP handles most of the server-side deployment difficulties including distributed server infrastructure. We handle client registration, authentication and messaging. Our messaging format is converted to XMPP payloads and messages are delivered through XMPP. Communication between servers and clients are all TLS [12] secured with certificate pinning. Using certificate pinning avoids the need for a trusted third party such as CAs and ensures that nobody (even legitimate authorities) is doing a man-in-the-middle attack against the communication channel. A database stores informations about users. On the server side, we are storing the following information for every user:

- **Username** (username): A valid mobile phone number is used for identification of the user.
- **One-time Password State** (otp-state): Used for two-factor authentication.
- **Device List** (device-list): List of user's devices. Elements of the list contain three values: *device-id*, *device-data* and *session-data*.
- **Database Salt** (db-salt): Contains the salt value used in password-data
- **Hashed and Salted User Password** (password-data): Contains salted and hashed (with KDF) value of the local password data.
- **Encrypted Encryption Key** (eek-data): Contains the encrypted encryption key and IV used to encrypt long term and short term private keys.
- **Encrypted Long Term Private Key** (L_{priv}): Contains the encrypted Ed25519 long term private key. The data is encrypted with a key derived from user password.
- **Self-signed Long Term Public Key** (L_{pub}): Contains the self-signed Ed25519 public key used for signature verification. This data is public to requests.
- **Encrypted Short Term Private Keys** (S_{priv}): Contains an encrypted list of Curve25519 short term DH key exchange private keys. Elements of the list contain three values: *curve25519-private-key*, *key-uid* and *timestamp*. The list is encrypted with a key derived from user password.
- **Signed Short Term Public Keys** (S_{pub}): Contains a list of Curve25519 short term DH key exchange public keys. Elements of the list contain 4 values: *curve25519-public-key*, *key-signature*, *key-uid*, *timestamp*. This data is public to requests. Public and private key pairs are matched with the *key-uid* identifier which is the hash of *curve25519-public-key*.

Usage details about the information stored on the server will be given in the following subsections.

B. Client Registration

1) **New Client Registration:** When a new user A wants to register first time with the system, the protocol is as follows:

- 1) Using client, user A types its username and a password (pwd). The password itself is never sent to server.

Instead, the fingerprint of the password is sent to server. To compute the fingerprint *local-pwd-data*, the client generates nonce *local-salt* and computes the password data and sends registration request to the server.

$local-salt = \text{LSB } 128\text{-bit of}$

$$H("314159265359" || username)$$

$$K = KDF(pwd, local-salt)$$

$local-pwd-data = \text{MSB } 256\text{-bit of } K$

$$A \xrightarrow{"Register", username, local-pwd-data} S$$

- 2) Server checks if the user exists or not. If it exists than the request is rejected. If not, the server creates a new user in the database, generates a random salt value and fills *username*, *db-salt* and *password-data*.

$$password-data = KDF(local-pwd-data, db-salt)$$

Then, server randomly generates an *otp-state* and sends it to the user's username using an SMS gateway. Server also sends acknowledgment to the client and requests the verification code which is sent by the server.

- 3) When client gets the verification SMS, user writes the code into client application and sends the verification request to the server as follows:

$$A \xrightarrow{"VerifyOTP", username, otp-data} S$$

- 4) Server checks if the *otp-data* matches with the *otp-state* in the database for the corresponding *username*. If it is, server generates *session-data* and *device-id* and sends an acknowledgment to the client, requests device information and long term and short term private and public key data.

$$A \xleftarrow{"Welcome", username, device-id, session-data} S$$

- 5) Client saves the device-id and session-data in an encrypted format. They are used to authenticate the client later.
- 6) Client randomly generates random encryption keys and IVs K_1, K_2, IV_1, IV_2 for both long term and short term private keys. K_1, IV_1 is used to encrypt long term private key data and K_2, IV_2 is for short term private key data. Client randomly generates IV_E and encrypts the encryption keys using a form the key K which was derived from user password in step 1 as follows:

$$K_E = \text{LSB } 256\text{-bit of } K$$

$$eek-data = EncMac_{K_E, IV_E}(K_1 || IV_1 || K_2 || IV_2) || IV_E$$

Now, client generates long term Ed25519 public private key pair (e_A, d_A), encrypts the private one and signs the public one. Client also generates 1024 short term Curve25519 public private key pairs ($st-pub_n, st-priv_n$), encrypts the private ones and signs the public ones. All data is formed in a proper way to be stored on a

database. The storage format is up to implementation but using base64 and JSON would be a good choice.

$$L_{priv} = EncMac_{K_1, IV_1}(d_A) || IV_1$$

$$L_{pub} = e_A || timestamp || [H(e_A || timestamp)]_{d_A}$$

$$S_{priv} = \{EncMac_{K_1, (IV_1+n)}(st-priv_n) \mid 0 \leq n < 1024\}$$

$$S_{pub} = \{st-pub_n || timestamp || [H(st-pub_n || timestamp)]_{d_A} \mid 0 \leq n < 1024\}$$

- 7) Client generates *device-data* which is a unique identifier for this particular client. Then, sends *device-data* and encrypted datas to the server.

$$A \xrightarrow["eek-data, L_{priv}, L_{pub}, S_{priv}, S_{pub}"]{"RegisterData", username, device-data, session-data} S$$

- 8) Server registers data into the database and a new user is created. Server returns final welcome acknowledgment.

2) *Existing Client Registration*: When an existing user wants to add a new client to its account, the protocol is as follows:

- 1) Assume user A has i clients, namely $A_0, A_1, \dots, A_{i-1}$ and wants to add a new client A_i .
- 2) Using the new client, user writes its username and password (*pwd*). *username* and *password-data* (shown in Section III-B1) is sent to server with tag "AddClient".
- 3) Server checks if *username* is valid and corresponding *password-data* matches. If it is, a new *otp-state* is randomly generated and sent to user's previous clients $A_0, A_1, \dots, A_{i-1}$.
- 4) When user gets OTP data from one of its previous clients, writes the code into new client's application. Client sends the verification data to the server.
- 5) Server checks if the *otp-data* matches with the *otp-state* in the database for the corresponding *username*. If it is, server generates a new device with *session-data* and *device-id* and sends an acknowledgment to the client.
- 6) Once new client gets the acknowledgment and session details, it requests the data set *eek-data, L_{priv}, L_{pub}, S_{priv}, S_{pub}* with session authentication.
- 7) Server sends the data set to the client and client generates the decryption keys from user password as mentioned in Section III-B1.
- 8) After verifying the data integrity, client stores the public and private key data, generates *device-data* and sends to the server.
- 9) Server stores the new client details and returns final welcome acknowledgment.

3) *Client Authentication (Login/Logout)*: When a user logs out on a client, that client application sends a de-registration request to the server for that particular *device-data*. Or when user deletes the client application from the client and reinstalls it, session authentication fails and in both cases server deletes the corresponding device from the database. If user wants to

add that client again to its account, the protocol is same as existing client registration mentioned in Section III-B2.

4) *Client-to-client Communication*: Assume that users A and B are registered with the server and A has m devices: $A_0, A_1, \dots, A_{m-1}$, B has n devices: $B_0, B_1, \dots, B_{n-1}$. A wants to start a secure chat session with B from its client A_i . All communication between clients are relayed over the server. When a message is sent to any of the user's client, it is relayed by the server to all clients that are associated with that user. We assume that A and B are friends and shared each other's long term public keys over the server and done the offline verification step as mentioned in Section II. Communication is established as follows:

- 1) A sends a chat request to server.

$$A \xrightarrow["from: A, session-data"]{"InitChatWith", B} S$$

- 2) Server returns the next short term public key of B with its id.

$$A \xleftarrow{st-pub_B, [st-pub_B]_{d_B}, key-uid_B} S$$

Queuing of the DH key parts are handled by the server. When all key parts are used, server randomly returns key parts.

- 3) A verifies the signature of B 's short term public key, randomly generates an IV_{AB} and selects its next short term private/public key pair $st-priv_A$ and $st-pub_A$. Then, computes the shared secret K_{AB} and sends the key exchange details to the server.

$$K_{AB} = KDF(Curve25519(st-priv_A, st-pub_B), IV_{AB})$$

$$SKID = H(st-pub_A, st-pub_B, IV_{AB})$$

$SKID$ is used as session key ID and included within every message encrypted with K_{AB} .

$$A \xrightarrow["KeyExchange", from: A, to: B, session-data]{key-uid_A, key-uid_B, IV_{AB}, EncMac_{K_{AB}, IV_{AB}+1}(SKID)} S$$

From now on, A can send message m to B using the shared secret key K_{AB} as follows:

$$A \xrightarrow["Message", from: A, to: B, session-data, timestamp, SKID]{EncMac_{K_{AB}, IV_{Rnd}}(m || timestamp || SKID), IV_{Rnd}} S$$

The authentication tag generated by the *EncMac* operation is also used for the message id (*MID*) to track messages by server. It does not matter if user B is online or not. All messages (including key exchange messages) sent by user A can be stored on the cloud and delivered when B becomes online.

- 4) Server gets the key exchange details and sends a push notification to the user B .
- 5) When B gets online, server first sends the key exchange details sent by the user A . Using these data (shown in step 3), B requests A 's corresponding short term public key from the server, verifies the signature of the public key, generates session key, verifies the $SKID$ and sends acknowledgment to the server, then starts to accept

messages. If verification fails, key exchange request is rejected.

$$K_{AB} = KDF(\text{Curve25519}(st\text{-}priv_B, st\text{-}pub_A), IV_{AB})$$

6) B first decrypts than verifies the message m .

$$m = DecMac_{K_{AB}, IV_{Rnd}}(m || timestamp || SKID)$$

B does the same procedure to send a message to party A .

IV. CONCLUSION

We presented an end-to-end encryption scheme which allows multi-device synchronization and offline key exchange. Multi-device synchronization is achieved by backing up all private data on the cloud in a secure way therefore any new client for a user can easily fetch all private keys from the cloud. The private keys' security on the cloud is based on the user password and the password is never known by the server. Offline key exchange is achieved by storing pre-computed key exchange parts on the cloud, thus, even if the user is not online, its key exchange data can be requested from the cloud. User authentication is done using two-factor authentication where user should write its password and OTP data. Our design has two protection methods against man-in-the-middle attacks. First one is public key pinning which secures the communication between the client and server. Secondly, client to client communication is secured by one-time offline verification. Also, using timestamp based message id prevents possible reply attacks.

Our protocol allows two-parties with multiple devices to communicate in a secure way but is lack of group chat. Thus, adopting group chat functionality without compromising security requirements into our design is the major future work for our research.

ACKNOWLEDGMENT

The authors would like to thank Ali Aydın Selçuk and Mutlu Çiçek for their support and assistance with this project.

REFERENCES

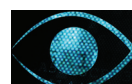
- [1] H.K. Taşkın, M. Demircioğlu, *Off-the-Record Communication with Location Hiding*, Information Security and Cryptology, Ankara, Turkey, Sep 2013.
- [2] N. Borisov, I. Goldberg, E. A. Brewer, *Off-the-record communication, or, why not to use PGP*, WPES 2004: 77-84.
- [3] P. Zimmermann, A. Johnston, Ed., J. Callas, *ZRTP: Media Path Key Agreement for Unicast Secure RTP*, Apr 2011, <http://tools.ietf.org/html/rfc6189>.
- [4] Quarkslab, *iMessage Privacy*, HITBSecConf2013, <http://blog.quarkslab.com/imessage-privacy.html>.
- [5] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, B. Yang, *High-speed high-security signatures*, Journal of Cryptographic Engineering 2 (2012), 77-89.
- [6] D. J. Bernstein, *Curve25519: new Diffie-Hellman speed records*, Proceedings of PKC 2006.
- [7] D. J. Bernstein, *ChaCha, a variant of Salsa20*, Workshop Record of SASC 2008: The State of the Art of Stream Ciphers.
- [8] D. J. Bernstein, *The Poly1305-AES message-authentication code*, Proceedings of Fast Software Encryption, 2005.
- [9] G. Bertoni, J. Daemen, M. Peeters, G. V. Assche, *The Keccak sponge function family*, <http://keccak.noekeon.org/>.

- [10] C. Percival, *Stronger Key Derivation via Sequential Memory-Hard Functions*, BSDCan'09, May 2009, <https://www.tarsnap.com/scrypt.html>.
- [11] *The Extensible Messaging and Presence Protocol*, <http://xmpp.org/>.
- [12] T. Dierks, E. Rescorla *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008, <http://tools.ietf.org/html/rfc5246>.

Halil Kemal Taşkın Halil Kemal Taşkın (S'14) graduated from Department of Mathematics Teaching at Gazi University, Turkey in 2009. He then received his M.Sc. degree in Cryptography from Institute of Applied Mathematics at Middle East Technical University in 2011 and he has been continuing his Ph.D. studies at the same department since 2011. During his studies, he has worked on Block Cipher Cryptanalysis and involved in a project about Differential Cryptanalysis funded by TÜBİTAK. Since 2013, he has been working as Cyber Security Specialist in Oran Teknoloji, Turkey.

Murat Demircioğlu Murat Demircioğlu (S'14) was born in Istanbul, Turkey, in 1986. He graduated from Department of Mathematics at Middle East Technical University, Turkey, in 2009. He then received his M.Sc. degree in Cryptography from Institute of Applied Mathematics at Middle East Technical University, Turkey in 2011 and he has been continuing his Ph.D. studies at the same department since 2011. During his studies, he has worked on Quantum cryptography and also involved in a project about Differential Cryptanalysis funded by TÜBİTAK. He worked as a Research Assistant in Institute of Applied Mathematics of Middle East Technical University, Turkey, from 2012 to 2013. Since 2013, he has been working as Cyber Security Specialist in Oran Teknoloji, Turkey.

Salim Sarımurat Salim Sarımurat graduated from Computer Engineering Department of Bilkent University, Turkey, in 2011. He then received his M.S. degree from Computer Science and Engineering Department of Sabancı University, Turkey, 2013. During his M.S. studies, he was working on a project, funded by Scientific and Technological Research Council of Turkey (TÜBİTAK), to develop secure key predistribution methods for mobile and multiphase Wireless Sensor Networks that improves resiliency performance against node capture attacks. Salim currently works as an Information Security Consultant.



Some Examples of New Nonlinearity Preserving Bijective Mappings

İ. Sertkaya, A. Doğanaksoy

Abstract—It is well known that the affine equivalency mappings preserve nonlinearity. Aside from the affine equivalency mappings, it is proved that there exist non-affine bijective mappings that act Boolean functions and keep nonlinearity invariant for all Boolean functions. For a fixed Boolean function, the explicitly constructed nonlinearity preserving bijective mappings create the same orbit structure with the affine equivalency mappings. On the other hand, the authors proved the existence of new nonlinearity preserving mappings that do not coincide with affine equivalency mappings based on the nonlinearity distributions. In the pursue of the explicit construction of this new nonlinearity preserving bijective mappings, here we give some examples for 3, 4 and 6 variable Boolean functions. We believe that if a generic construction method will be derived, these mappings would be used as a practical tool for constructing new Boolean function families.

Index Terms—Boolean functions, affine equivalency mappings, nonlinearity preserving mappings.

I. INTRODUCTION

MEIER and Staffelbach proved that nonlinearity is invariant under the action of general affine group AGL_n of degree n over $\mathbb{F}_2$ [1]. Later, by extending the result of [2, p. 417], Preneel proved that affine equivalency mappings $AGL_n \ltimes \mathcal{A}_n$ also preserve nonlinearity [3].

Searching Boolean functions that possess high cryptographic design criteria values is an ongoing research subject [4], [5]. The aim is to find new families of Boolean functions not equivalent to the existing ones which would lead to obtain better primitives for cryptographic design.

The orbits of the action of $AGL_n \ltimes \mathcal{A}_n$ on the set of n variable Boolean functions $\mathcal{F}_n$ partitions the set into equivalence classes. These classes are comprised of the functions having the same degree, nonlinearity and frequency distribution of absolute Walsh spectrum values, see [1], [3], for the other properties that also preserved please refer to [6, Section 5.1, p. 81]. Therefore they constitute a practical tool for classifying the Boolean functions into families. When a Boolean function having highly desirable design properties is achieved with either heuristic search or direct construction methods, affine equivalency mappings are used to verify that these new functions does not belong to an existing family.

Since the cardinality of $\mathcal{F}_n$ is 2^{2^n} , the maximal group of bijective mappings that can act on $\mathcal{F}_n$ is the symmetric

group $\text{Sym}(\mathcal{F}_n)$ and isomorphically $S_{2^{2^n}}$. $AGL_n \ltimes \mathcal{A}_n$ is a proper subgroup of AGL_{2^n} which also a proper subgroup of $S_{2^{2^n}}$. Commonly, $AGL_n \ltimes \mathcal{A}_n$ are considered as the only mappings that keep nonlinearity invariant for all Boolean functions. However, the authors explicitly constructed nonlinearity preserving bijective mappings in $AGL_{2^n} - (AGL_n \ltimes \mathcal{A}_n)$ and furthermore in $S_{2^{2^n}} - AGL_{2^n}$, see [7] and [8]. However given a Boolean function, the orbits of these mappings coincides with $AGL_n \ltimes \mathcal{A}_n$ [9]. On the other hand, in the same study the authors give the exact number of nonlinearity preserving bijective mappings for $n \leq 6$ and moreover without constructing explicitly, they proved that the existence of new bijective mappings that do not coincide with $AGL_n \ltimes \mathcal{A}_n$.

Exact classification or enumeration of nonlinearity preserving mappings is still an open problem. The current state of the classification of nonlinearity preserving bijective mappings is illustrated in Figure 1 and for values $n \leq 6$, where nonlinearity distributions is computable, the enumeration of nonlinearity preserving bijective mappings is given in [9].

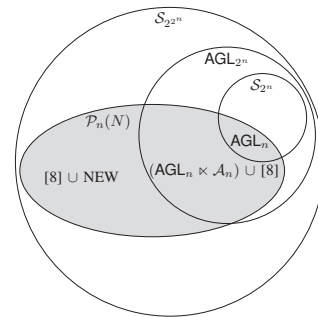
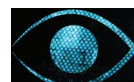


Fig. 1. Current state of nonlinearity preserving bijective transformations. (Here, NEW represents new maps for which the examples given in this work.)

Classification and enumeration of nonlinearity preserving mappings, has both theoretical and practical influences in cryptographic research. Indeed without loosing the satisfied security margins, choosing efficiently implementable Boolean function or if possible maximizing other security margins by using these mappings is a research goal. In this study, in order the clarify these concepts we are constructing some examples for 3, 4 and 6 variable Boolean functions. These examples may not be generic but they emphasize the notions given above. The paper is organized as follows: in Section II we give notations and definitions and in Section III we recall necessary propositions, next we give the examples of new nonlinearity preserving bijective mappings in Section IV and finally Section V concludes the study.

İ. Sertkaya is with the Institute of Applied Mathematics, METU, Ankara, and the Mathematical and Computational Sciences Labs, TÜBİTAK BİLGEM UEKAE, Gebze, Kocaeli, TURKEY e-mail: isa.sertkaya@tubitak.gov.tr

A. Doğanaksoy is with the Institute of Applied Mathematics and the Department of Mathematics, METU, Ankara, TURKEY email: aldoks@metu.edu.tr
Manuscript received July 30; revised September 1, 2014.



II. PRELIMINARIES

Unless otherwise stated explicitly, the following definitions and notions are given regarding [10], [11].

Let $\mathbb{F}_2^n$ be the n -dimensional $\mathbb{F}_2$ -vector space admitting the usual *lexicographical* ordering as follows: for any $\alpha, \beta \in \mathbb{F}_2^n$, $\alpha < \beta$ if and only if there exists $i \in \{1, 2, \dots, n\}$, such that $a_1 = b_1, \dots, a_{i-1} = b_{i-1}$ and $a_i < b_i$. According to this ordering we label each element of $\mathbb{F}_2^n$ as

$$\alpha_0 = (0, 0, \dots, 0) < \alpha_1 < \alpha_2 < \dots < \alpha_{2^n-1} = (1, 1, \dots, 1),$$

and we denote $n \times 1$ vectors by $[\alpha] = (a_1, a_2, \dots, a_n)^t$.

Any function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is called a *Boolean function* and can be represented uniquely by

- the corresponding *truth table* given by

$$T_f = (f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^n-1})),$$

where T_f is lexicographically ordered, or equivalently,

- the corresponding *algebraic normal form* that is the multivariate polynomial over $\mathbb{F}_2$ given by

$$\begin{aligned} f(x_n, x_{n-1}, \dots, x_1) &= c_0 \oplus c_1 x_1 \oplus \dots \oplus c_n x_n \\ &\quad \oplus c_{12} x_1 x_2 \oplus \dots \\ &\quad \oplus c_{123} x_1 x_2 x_3 \oplus \dots \\ &\quad \vdots \\ &\quad \oplus c_{12\dots n} x_1 x_2 \dots x_n. \end{aligned} \quad (1)$$

The set of all Boolean functions defined on $\mathbb{F}_2^n$ is denoted by $\mathcal{F}_n$. The *degree* $\deg(f)$ of f is the degree of its algebraic normal form, i.e. the number of variables in the highest order term with nonzero coefficient. If $\deg(f) \leq 1$ then f is called *affine*, i.e., it is of the form $f(x_n, x_{n-1}, \dots, x_1) = \langle c, x \rangle \oplus c_0$, where $c_0 \in \mathbb{F}_2$ and $\langle c, x \rangle = c_1 x_1 \oplus \dots \oplus c_n x_n$ is the *standard inner product* with $x, c \in \mathbb{F}_2^n$. The set of all affine Boolean functions on $\mathbb{F}_2^n$ is denoted by $\mathcal{A}_n$, where each function in $\mathcal{A}_n$ will be given by

$$\ell_{(\alpha_i, a)} : x \mapsto \langle x, \alpha_i \rangle \oplus a.$$

For a given function f , the *Hamming weight* $w(f)$ is given as usual as the number of ones in T_f . The set $\text{Sup}(f) := \{\alpha \in \mathbb{F}_2^n \mid f(\alpha) = 1\}$ is called the *support* of the function f . For given functions f and g , the *Hamming distance* $d(f, g)$ is the Hamming weight of $f \oplus g$.

The matrices defined over $\mathbb{R}$ and constructed iteratively with the Kronecker product $\otimes$ satisfying

$$H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1} = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}.$$

are called *Sylvester Hadamard matrices* [12], [13].

The *Walsh transform* $W_f: \mathbb{F}_2^n \rightarrow \mathbb{R}$ of a function f is given by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, \omega \rangle}, \text{ for all } \omega \in \mathbb{F}_2^n.$$

The truth table of the Walsh transform

$$W_f := (W_f(\alpha_0), W_f(\alpha_1), \dots, W_f(\alpha_{2^n-1}))$$

is called the *Walsh Spectrum* of f , and it can be expressed as $W_f = \zeta_f H_n$ (see [14]) where

$$\zeta_f = ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \dots, (-1)^{f(\alpha_{2^n-1})})$$

is the truth table of the *signed function* $(-1)^{f(x)}$ of f .

Definition 1: [15], [1] The *nonlinearity* N_f of a function f is its distance to the nearest affine function. N_f can be expressed with the Walsh transform of f as follows:

$$N_f = \min_{\ell_{(\beta, a)} \in \mathcal{A}_n} d(f, \ell_{(\beta, a)}) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|.$$

A function f is called a *bent function* if $W_f(w) = \pm 2^{n/2}$ for any $w \in \mathbb{F}_2^n$. Bent functions only exist if n is even [16], [17], and form a special set $\mathcal{B}_n$ of Boolean functions attaining maximal nonlinearity for a fixed positive even integer n [1].

III. NONLINEARITY PRESERVING BIJECTIVE MAPPINGS

A. Affine equivalency

We start with constructing the group which comprised of affine equivalency mappings.

Definition 2: [18] Let GL_n be the group of all nonsingular matrices of order n over $\mathbb{F}_2$. Let further AGL_n be the group

$$\text{GL}_n \ltimes \mathbb{F}_2^n := \{(A, \alpha) \mid A \in \text{GL}_n, \alpha \in \mathbb{F}_2^n\},$$

with respect to the operation $\bullet$. The group law and its inverse are given by

$$\begin{aligned} (A, \alpha) \bullet (A', \alpha') &:= (A'A, \alpha'A + \alpha), \\ (A, \alpha)^{-1} &:= (A^{-1}, \alpha A^{-1}) \end{aligned}$$

for all $(A, \alpha), (A', \alpha') \in \text{AGL}_n$.

Similarly, we define the group

$$\text{AGL}_n \ltimes \mathcal{A}_n := \{(\tau, \ell_{(\beta, a)}) \mid \tau \in \text{AGL}_n, \ell_{(\beta, a)} \in \mathcal{A}_n\},$$

which can be given more explicitly as follows:

$$\text{AGL}_n \ltimes \mathcal{A}_n := \{(A, \alpha, \beta, a) \mid A \in \text{GL}_n, \alpha, \beta \in \mathbb{F}_2^n, a \in \mathbb{F}_2\},$$

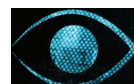
where τ and $\ell_{(\beta, a)}$ are given by the mappings $\tau: x \mapsto xA \oplus \alpha$ and $\ell_{(\beta, a)}: x \mapsto \langle x, \beta \rangle \oplus a$.

We have an immediate action of the group $\text{AGL}_n \ltimes \mathcal{A}_n$ on $\mathcal{F}_n$ as follows

$$(A, \alpha, \beta, a)f := f(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$

Two Boolean functions f and g are said to be *affine equivalent* if and only if for $(A, \alpha, \beta, a) \in \text{AGL}_n \ltimes \mathcal{A}_n$ the following holds

$$f(x) = (A, \alpha, \beta, a)g = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$



B. Non-affine Nonlinearity Bijective Preserving Mappings

The truth table of an n -variable Boolean function is an ordered 2^n tuple over $\mathbb{F}_2$. Hence, any bijective mapping acting on such functions can be regarded as a permutation of 2^{2^n} elements. In particular, we can view every bijective mapping as an element of $\mathcal{S}_{2^{2^n}}$.

Let $\psi \in \mathcal{S}_{2^{2^n}}$. We say that ψ preserves nonlinearity if $N_f = N_{\psi f}$ for all $f \in \mathcal{F}_n$. Hence, it follows that ψ preserves nonlinearity if and only if the absolute maximum of the Walsh spectra of f remains invariant, that is

$$\max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| = \max_{\omega \in \mathbb{F}_2^n} |W_{\psi f}(\omega)| \text{ for all } f \in \mathcal{F}_n.$$

We denote the set of all nonlinearity preserving bijective maps acting on the n -variables Boolean functions by

$$\mathcal{P}_n(N) = \{\psi \in \mathcal{S}_{2^{2^n}} \mid N_f = N_{\psi f} \text{ for all } f \in \mathcal{F}_n\}.$$

In general any mapping $\psi : \mathbb{F}_2^{2^n} \rightarrow \mathbb{F}_2^{2^n}$ can be written as

$$\begin{aligned} \psi : (x_1, x_2, x_3, \dots, x_{2^n}) \mapsto & (\psi_1(x_1, x_2, \dots, x_{2^n}), \\ & (\psi_2(x_1, x_2, \dots, x_{2^n}), \\ & \vdots \\ & \psi_{2^n}(x_1, x_2, \dots, x_{2^n})), \end{aligned}$$

or,

$$\psi : [x] \mapsto \begin{bmatrix} \psi_1(x_1, x_2, \dots, x_{2^n}) \\ \psi_2(x_1, x_2, \dots, x_{2^n}) \\ \vdots \\ \psi_{2^n}(x_1, x_2, \dots, x_{2^n}) \end{bmatrix}, \quad (2)$$

where each $\psi_i : \mathbb{F}_2^{2^n} \rightarrow \mathbb{F}_2$ is a 2^n variable Boolean function called *coordinate function* of ψ . Each ψ_i 's can be represented by their algebraic normal form uniquely;

$$\begin{aligned} \psi_i(x_1, x_2, \dots, x_{2^n}) = & c_0^{(i)} \oplus c_1^{(i)} x_1 \oplus \dots \\ & \oplus c_{12 \dots 2^n}^{(i)} x_1 x_2 \dots x_{2^n}. \end{aligned} \quad (3)$$

Then, by porting (3) into (2) and re-labeling, we get

$$\begin{aligned} \psi : [x] \mapsto & \underbrace{\begin{bmatrix} c_0^{(1)} \\ c_0^{(2)} \\ \vdots \\ c_0^{(2^n)} \end{bmatrix}}_{[\lambda_0]} \oplus \underbrace{\begin{bmatrix} c_1^{(1)} \\ c_1^{(2)} \\ \vdots \\ c_1^{(2^n)} \end{bmatrix}}_{[\lambda_1]} x_1 \oplus \dots \oplus \\ & \underbrace{\begin{bmatrix} c_{12}^{(1)} \\ c_{12}^{(2)} \\ \vdots \\ c_{12}^{(2^n)} \end{bmatrix}}_{[\lambda_{12}]} x_1 x_2 \oplus \dots \oplus \underbrace{\begin{bmatrix} c_{12 \dots 2^n}^{(1)} \\ c_{12 \dots 2^n}^{(2)} \\ \vdots \\ c_{12 \dots 2^n}^{(2^n)} \end{bmatrix}}_{[\lambda_{12 \dots 2^n}]} x_1 x_2 \dots x_{2^n}, \end{aligned}$$

and now equivalently we have

$$\begin{aligned} \psi : [x] \mapsto & [\lambda_0] \oplus M[x] \oplus [\lambda_{12}] x_1 x_2 \oplus \dots \\ & \oplus [\lambda_{123}] x_1 x_2 x_3 \oplus \dots \\ & \vdots \\ & \oplus [\lambda_{12 \dots 2^n}] x_1 x_2 \dots x_{2^n} \end{aligned} \quad (4)$$

where

- $x = (x_1, x_2, \dots, x_{2^n}) \in \mathbb{F}_2^{2^n}$ hence each $x_i \in \mathbb{F}_2$,
- $\lambda_j \in \mathbb{F}_2^{2^n}$ with each $c_j^i \in \mathbb{F}_2$,
- M is the $2^n \times 2^n$ matrix whose column form is $M = [[\lambda_1] \ [\lambda_2] \ \dots \ [\lambda_{2^n}]]$.

The above representation gives the following classifications.

- $\psi \in \text{AGL}_n \ltimes \mathcal{A}_n$ if
 - $\lambda_0 \in \mathcal{A}_n$ and $M \in \mathcal{S}_{2^n}$ correspond to the permutation matrix representation of an element in AGL_n and
 - $\lambda_j = (0 \ 0 \ \dots \ 0)$ for all $j \neq 0, 1, 2, 3, 4, \dots, 2^n$.
- $\psi \in \text{AGL}_{2^n}$ if
 - $\lambda_0 \in \mathbb{F}_2^{2^n}$ and $M \in \text{GL}_{2^n}$ and
 - $\lambda_j = (0 \ 0 \ \dots \ 0)$ for all $j \neq 0, 1, 2, 3, 4, \dots, 2^n$.
- $\psi \in \mathcal{S}_{2^{2^n}}$ is called *non-affine* if it has at least one non-zero λ_j , for $j \in \{12, 13, \dots, 12 \dots 2^n\}$.

In truth more detailed but not complete lattice of subgroups of $\mathcal{S}_{2^{2^n}}$ is shown in Fig. 2.

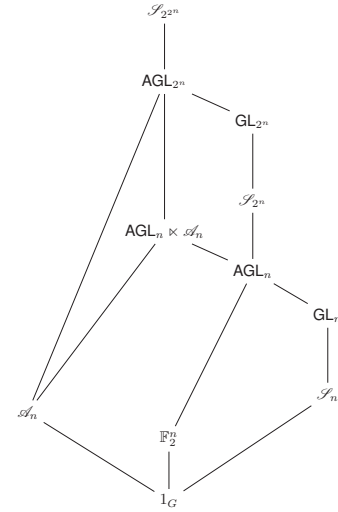


Fig. 2. Lattice of subgroups of $\mathcal{S}_{2^{2^n}}$ (not a complete list)

It is not difficult to see that $\text{AGL}_n \ltimes \mathcal{A}_n \subseteq \text{AGL}_{2^n}$. Furthermore, AGL_{2^n} is as a proper subgroup of $\mathcal{S}_{2^{2^n}}$.

These observations led not only to generalize the action under the larger group AGL_{2^n} (instead of considering the equivalency under $\text{AGL}_n \ltimes \mathcal{A}_n$), but also to prove the existence of new classes of nonlinearity preserving mappings lying in $\text{AGL}_{2^n} \setminus \text{AGL}_n \ltimes \mathcal{A}_n$ [7].

In [8, Proposition 3.8], the existence of nonlinearity preserving non-affine bijective mappings is proved by explicit construction and in [9] it is further proved that even if they are non-affine mappings these mappings actually produce the

same orbit structure as $\text{AGL}_n \ltimes \mathcal{A}_n$ for any fixed function, that is;

Proposition 3: [9] Let the notations be as above. Let further $\psi \in \mathcal{S}_{2^{2n}}$ be a non-affine mapping satisfying

- 1) $\lambda_0 \in \mathcal{A}_n$,
- 2) The matrix $M = (P' \oplus B)$ with $P' \in \mathcal{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1 \ \varepsilon_2 \ \dots \ \varepsilon_{2^n}]$ with $\varepsilon_i \in \mathcal{A}_n$, $1 \leq i \leq 2^n$,
- 3) $\lambda_j \in \mathcal{A}_n$ for all $j \in \{12, 13, \dots, 12 \dots 2^n\}$ where at least one of $\lambda_j \neq (0 \dots 0)$.

Then ψ is an element of $\text{AGL}_n \ltimes \mathcal{A}_n$ for a fixed function $f \in \mathcal{F}_n$.

Furthermore it is proved that

Theorem 4: [9] For $n \geq 3$ there exist nonlinearity preserving non-affine mappings not lying in the class of Proposition 3.

IV. EXAMPLES OF NEW MAPPINGS

The proof of Theorem 4 rely on the cardinalities gathered from nonlinearity distributions and beside the existence, it does not state any families. Here we will give some examples to illustrate these mappings. The examples may seem to be basic and in a way they are. However, we believe examining such example would give clues about structure of these new nonlinearity preserving mappings.

Due to the space constraints the algebraic normal form of the nonlinearity preserving transformations are not given explicitly for $n \geq 4$. However, since any transformation is an element of $\mathcal{S}_{2^{2n}}$, it is possible to represent the permutations as a product of disjoint cycles. Within these cycles, the functions will be given by their truth table in hexadecimal value without the "0x" prefix.

Example 5: Let $\psi \in \mathcal{S}_{2^{23}}$ be the mapping, whose explicit permutation representation is given in Appendix, satisfying,

$$[T_f] \mapsto [\lambda_0] \oplus M[T_f] \oplus$$

$$[\lambda_{123458}]f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_7) \oplus$$

$$[\lambda_{123457}]f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_6) \oplus$$

$$[\lambda_{1234568}]f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5)f(\alpha_7) \oplus$$

$$[\lambda_{1234567}]f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5)f(\alpha_6)$$

where $\lambda_0 = (0, 0, 0, 0, 1, 1, 1, 1)$, $\lambda_{123458} = \lambda_{123457} = \lambda_{1234568} = \lambda_{1234567} = (0, 0, 0, 0, 0, 1, 0, 1)$ and M is the matrix;

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Trivially, ψ is not an affine mapping, indeed it does not satisfies the conditions given in Proposition 3, since $(0, 0, 0, 0, 0, 1, 0, 1)$ is not truth table of an affine function. Moreover, it can be easily checked that this map is invertible and preserves nonlinearity for all functions.

Example 6: Assume $\psi \in \mathcal{S}_{2^{24}}$ be a permutation of $\mathbb{F}_2^{24}$ with cycle representation,

$$\pi_\psi = (0002, 3ec3, fffe, 33ce, 7fff, 2ff0)(001b, 33aa, e48d, f681, 6a77, 97f7, 050a, 027c, 665a, 1370, fff0)(059c, a63f, e1ee, 36af, 72be, fca9)$$

It can be easily verified that ψ keeps nonlinearity values invariant for all $f \in \mathcal{F}_n$, that is $\psi \in \mathcal{P}_4(N)$. When the algebraic normal form of ψ is written explicitly, it will be seen that some non-affine terms are not the truth table of an affine function. Thus ψ is not of the form given in Proposition 3.

Example 7: Let $\psi \in \mathcal{S}_{2^{26}}$ be the permutation such that its disjoint cycle representation is

$$\pi_\psi = (9556566a3ffcfcc0, 0ddfcbb3a4456dd9)$$

Trivially, ψ maps all functions to itself except the ones in the disjoint cycles, i.e. it keeps nonlinearity invariant for those functions. The cycle has bent functions whose nonlinearity values are 28. Thus, $\psi \in \mathcal{P}_6(N)$. However, the bent function 9556566a3ffcfcc0 has algebraic degree 2 while its image under ψ , 0ddfcbb3a4456dd9, has algebraic degree 3. ψ can not be of the form as given in Proposition 3 since in that case it should have also kept the algebraic degree invariant.

Indeed, in a generic way, one can easily construct new nonlinearity preserving mappings in the following way. Consider two different affine equivalency classes of the same nonlinearity values, for instance regard the classes given in [19], [18], [20], [6]. Taking into account of the bijectivity property of the transformation, map the one of affine equivalency class members to the other class. Basically, while mapping the rest to themselves, select at least two functions belonging to the different affine equivalency classes and then map each to the other to produce a bijective nonlinearity preserving mapping. By Proposition 3, it is certain that the transformations created as above won't belong to the explicitly known non-affine bijective nonlinearity preserving mapping. Moreover these transformations will not produce the same orbit structure as affine equivalency mappings.

When an expressive construction or classification given for these explicitly unknown mappings, such mappings may probably be used as a practical tool especially to construct new functions that are not belonging to the same equivalency classes may be performed.

V. CONCLUSION

Studying the elements $\mathcal{S}_{2^{2n}}$ and classifying them with respect to nonlinearity preserving property is still an open problem. Due to the huge cardinality of the mappings, pursuing this research may seem to be highly involved. Despite this fact, it may lead to a deeper insight to the nonlinear functions or nonlinearity classes and additionally it may become a practical tool for constructions of new Boolean functions. In this work, some examples of new transformations keeping nonlinearity invariant are given. For future studies, it would be interesting to further investigate nonlinearity preserving mappings in order to construct these mappings with explicit

methods. Such constructions may be used as a practical tool for finding new Boolean function families.

APPENDIX

EXPLICIT PERMUTATION REPRESENTATION OF EXAMPLE 5

The bijective mapping presented in Example 5, is given below regarding the disjoint cycle representation.

$$\pi_{\psi} = (00, 0f, 55, 3c, 5a, 66, 33)(01, 0e, 54, 3d, 5b, 67, 32)(02, 0b, 45, 3e, 5e, 76, 31, 04, 1f, 57, 38, 4a, 64, 37, 10, 0d, 51, 2c, 58, 62, 23)(03, 0a, 44, 3f, 5f, 77, 30, 05, 1e, 56, 39, 4b, 65, 36, 11, 0c, 50, 2d, 59, 63, 22)(06, 1b, 47, 3a, 4e, 74, 35, 14, 1d, 53, 28, 48, 60, 27, 12, 09, 41, 2e, 5c, 72, 21)(07, 1a, 46, 3b, 4f, 75, 34, 15, 1c, 52, 29, 49, 61, 26, 13, 08, 40, 2f, 5d, 73, 20)(16, 19, 43, 2a, 4c, 70, 25)(17, 18, 42, 2b, 4d, 71, 24)(6a, 6c, 78)(6b, 6d, 79)(6e, 7c, 7a)(6f, 7d, 7b)(82, 84, 90)(83, 85, 91)(86, 94, 92)(87, 95, 93)(88, cf, fa, e4, b8, c5, b1, 8b, ca, eb, e2, ac, d7, b7, 9f, d8, ed, f6, be, d1, a3, 8d, de, f9, e1, a9, c6, b4, 9a, c9, ee, f3, af, d2, a6, 9c, dd, fc, f5, bb, c0, a0)(89, ce, fb, e0, a8, c7, b5, 9b, c8, ef, f2, ae, d3, a7, 9d, dc, fd, f4, ba, c1, a1)(8a, cb, ea, e3, ad, d6, b6, 9e, d9, ec, f7, bf, d0, a2, 8c, df, f8, e5, b9, c4, b0)(8e, db, e8, e7, bd, d4, b2)(8f, da, e9, e6, bc, d5, b3)(98, cd, fe, f1, ab, c2, a4)(99, cc, ff, f0, aa, c3, a5)$$

ACKNOWLEDGMENT

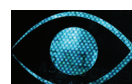
The authors would like to thank the anonymous reviewers for their valuable comments on the preliminary version of this work.

REFERENCES

- [1] W. Meier and O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions," in *Advances in Cryptology — EUROCRYPT '89*, ser. Lecture Notes in Computer Science, J. Quisquater and J. Vandewalle, Eds. Springer Berlin Heidelberg, 1990, vol. 434, pp. 549–562.
- [2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. Amsterdam: North-holland Publishing Company, 1978.
- [3] B. Preneel, "Analysis and Design of Cryptographic Hash Functions," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, Jan. 1993.
- [4] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Information and Computation*, vol. 208, no. 4, pp. 341 – 350, 2010.
- [5] S. Maitra, "Boolean functions on odd number of variables having nonlinearity greater than the bent concatenation bound," in *NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (NATO ASI Zvenigorod, 2007)*, ser. NATO Science for Peace and Security Series, B. Preneel and O. A. Logachev, Eds. IOS Press books, 2008, pp. 173–182.
- [6] A. Braeken, "Cryptographic Properties of Boolean Functions and S-Boxes," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, 2006.
- [7] İ. Sertkaya and A. Doğanaksoy, "On Nonlinearity Preserving Bijective Transformations," in *Proceedings of the National Cryptology Symposium II*, Ankara, Turkey, 2006, pp. 27–36.
- [8] —, "Some Results on Nonlinearity Preserving Bijective Transformations," in *Proceedings of BFCA'07 Conference*, Paris, France, 2007, pp. 27–42.
- [9] İ. Sertkaya, A. Doğanaksoy, O. Uzunkol, and M. S. Kiraz, "Affine Equivalency and Nonlinearity Preserving Bijective Mappings over $\mathbb{F}_2$," submitted to the International Workshop on the Arithmetic of Finite Fields (WAIFI 2014).
- [10] C. Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2010, ch. Boolean Functions for Cryptography and Error Correcting Codes, pp. 257–397.
- [11] İ. Sertkaya, "Nonlinearity Preserving Post-Transformations," Master's thesis, Middle East Technical University, Ankara, Turkey, June 2004.
- [12] J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers," *Philosophical Magazine*, vol. 34, pp. 461–475, 1867.
- [13] J. Hadamard, "Résolution d'une question relative aux déterminants," *Bull. Sciences Math.*, vol. 2, no. 17, pp. 240–246, 1893.
- [14] J. Seberry and X.-M. Zhang, "Highly nonlinear 0–1 balanced Boolean functions satisfying strict avalanche criterion (extended abstract)," in *Advances in Cryptology — AUSCRYPT '92*, ser. Lecture Notes in Computer Science, J. Seberry and Y. Zheng, Eds. Springer Berlin Heidelberg, 1993, vol. 718, pp. 143–155.
- [15] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *Computers and Digital Techniques, IEE Proceedings E*, vol. 135, no. 6, pp. 325–335, 1988.
- [16] O. S. Rothaus, "On "bent" functions," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300 – 305, 1976.
- [17] J. F. Dillon, "A Survey of Bent Functions," *The NSA Technical Journal*, vol. Special Issue, pp. 191–215, 1972.
- [18] J. A. Maiorana, "A Classification of the Cosets of the Reed-Muller Code $R(1, 6)$," *Mathematics of Computation*, vol. 57, no. 195, pp. 403–414, 1991.
- [19] E. Berlekamp and L. Welch, "Weight Distributions of the Cosets of the $(32, 6)$ Reed-Muller Code," *Information Theory, IEEE Transactions on*, vol. 18, no. 1, pp. 203–207, Jan 1972.
- [20] J. E. Fuller, "Analysis of affine equivalent Boolean functions for cryptography," Ph.D. dissertation, Queensland University of Technology, Queensland, Australia, 2003.

İsa Sertkaya received M.Sc. and Ph.D. Degrees in cryptography from the Middle East Technical University, Ankara, in 2004 and 2014 respectively. His area of research interest includes Boolean functions.

Ali Doğanaksoy received M.Sc. and Ph.D. Degrees in mathematics from the Middle East Technical University, Ankara, in 1983 and 1987 respectively. After a period of research in differential geometry, he directed to cryptography. His area of interest includes Boolean functions, randomness tests.



A High Capacity Html Steganography Method

E. Satir, A. Sargin, T. Kanat, and C. Okuducu

Abstract—With the widespread use of the Internet and the booming growth of the computer industry, people nowadays can easily retrieve multimedia contents with their own computers or mobile phones over the Internet or mobile channels. In this case, data hiding is one of the useful schemes for delivering secret messages. Steganography refers to the science of invisible communication. In this study, we proposed a high capacity HTML steganography method that employs URL addresses. Here, URL addresses are used as steganographic cover and the HTML side of the concerning web page is used as a platform for camouflage. Accordingly, it is enough to send only the obtained URL to the recipient. Experiments were performed by investigating steganographic capacity and imperceptibility. The capacity value is increased to 8.85% for the secret message containing 600 characters. Besides, steganographic security is provided via RSA encryption and elaborating the computation by LZW.

Index Terms— HTML steganography, LZW compression, steganography

I. INTRODUCTION

WITH the widespread use of the Internet and the booming growth of the computer industry, people nowadays can easily retrieve multimedia contents with their own computers or mobile phones over the Internet or mobile channels. In this case, data hiding is one of the useful schemes for delivering secret messages. Steganography refers to the science of “invisible” communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. As broadband technologies improve bandwidth at the last-mile, multimedia content, such as still images, audio and video, have gained increasing popularity on the Internet.

E. Satir is with Duzce University, Faculty of Engineering, Computer Engineering Department, Duzce, 81620 TURKEY (corresponding author to provide phone: 0380-542-1100; e-mail: esrasatir@duzce.edu.tr).

A. Sargin is with Ministry of National Education, Karakopru Middle School, Sanliurfa, TURKEY (phone: 0506-675-9838; e-mail: abdurrahimsargin42@gmail.com).

T. Kanat is with Ministry of National Education, Konya, TURKEY (phone: 0535-513-3566; e-mail: tayfunkanat91@gmail.com).

C. Okuducu is with Ministry of National Education, Goger Middle School, Diyarbakir, TURKEY (phone: 0506-980-5692; e-mail: cengizoku@hotmail.com).

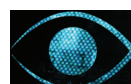
Given the high degree of redundancy present in a digital representation of multimedia content (despite compression), there has been an increased interest in using multimedia content for the purpose of steganography. Indeed many such techniques have been devised in the past few years [1]. Contemporary approaches are often categorized based on the steganographic cover type such as text, image, audio, or graph [2].

Textual steganography can be classified as textual format manipulation (TFM) and textual fabrication (TF) [2]. TFM modifies an original text by employing spaces, misspellings, fonts, font size, font style, colors, and non-color (as invisible ink) to embed an encoded message. However, comparing the original text with the modified text will trigger suspicion and enable adversary to pin down where the message is hidden in the text [2]. In addition, TFM can be distorted, discerned by human eye, or detected by a computer [2].

On the other hand, textual fabrication techniques generate an entire text-cover for hiding a message rather than manipulating an existing text. Examples of these approaches are null cipher [3], mimic functions [4], [5] NICETEXT and SCRAMBLE [6], and translation-based [7]-[9]. However, the text cover that is generated by these approaches often has numerous linguistic flaws that can raise suspicion. In addition, revealing the hidden message may be feasible [2].

In 2009, Desoky proposed a method called Listega which takes advantage of using textual list to camouflage data by exploiting itemized data to conceal messages. Simply, it encodes a message then assigns it to legitimate items in order to generate a cover text in a form of list. Listega establishes a covert channel among communicating parties by employing justifiably reasons based on the common practice of using textual list of items in order to achieve unsuspecting transmission of generated covers [10].

In 2010 Desoky proposed a steganographic approach that employs NLG (Natural Language Generation) and template techniques along with Random Series values (RS), e.g. binary, decimal, hexadecimal, octal, alphabetic, alphanumeric, etc., of Domain-Specific Subject (DSS) to generate a noiseless text-cover. DSS (like financial, medical, mathematical and etc.) has plenty of room to conceal data and allows communicating parties to establish a covert channel such as a relationship based on the profession of the communication parties to transmit a text-cover. Desoky’s method, called Matlist (Mature Linguistic Steganography), embeds data in a form of RS values, function of RS, related semantics of RS, a combination of these, etc. He mentioned that Matlist did not preserve the meaning of text-cover every time it is used, instead it retains different legitimate meaning for each



A HIGH CAPACITY HTML STEGANOGRAPHY METHOD

message while remaining semantically coherent and rhetorically sound [11].

Ryabko and Ryabko (2011) proposed steganographic systems for the case when cover texts are generated by a finite-memory source with possibly unknown statistics. The probability distributions of cover texts with and without hidden information are the same; this means that the proposed stego systems are perfectly secure, i.e. an observer can not determine whether hidden information is being transmitted. The main idea behind the proposed stego systems is the following: Suppose that for a cover text x generated by a source, a set S of cover texts can be founded such that each cover text in S has the same probability of being generated as x . Moreover, assume that each element of S defines S , uniquely. Then, instead of transmitting the cover text x that was actually generated, the cover text can be transmitted in the set S whose number in S corresponds to the secret text which is wanted to be passed. This does not change the probabilistic characteristics of the source, provided the secret text consists of independent and identically distributed (i.i.d.) equiprobable bits. Therefore, an observer can not tell whether secret information is being passed. There are two disadvantages of the outlined stego system: first, the rate of transmission of secret text is not optimal, and second, it applies only to i.i.d. cover texts [12].

To make a steganographic communication even more secure the message can be compressed and encrypted before being hidden in the carrier. Cryptography and steganography can be used together. If compressed, the message will take up far less space in the carrier and will minimise the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography [13].

Finally in 2012, Satir and Isik proposed a LZW (Lempel-Ziv-Welch) compression based [14] and an enhanced version; Huffman compression based [15] text steganography methods where capacity and security issues were considered. In the proposed methods, LZW and Huffman coding algorithms were used to increase the capacity and to contribute the security. Moreover, the proposed methods construct stego keys and employs Combinatorics-based coding in order to increase the security and to provide the desired randomness. For imperceptibility and to render the carrier medium innocent, they constructed forward mail platform as stego cover in order to conceal secret information. They obtained 7.042 % and 7.962 % capacity values for the secret message containing 300 characters (or 300·8 bits) via LZW and Huffman coding algorithms, respectively. They stated that the hidden information cannot be extracted, easily without the used stego keys. Besides, the extraction procedure was rendered more complex by means of the employed compression techniques.

In this study, a steganographic method that employs web page as the carriers, has been proposed. The purpose of this study is to obtain a significant increment ratio in the amount of secret data that is aimed to be hidden while complicating the extraction procedure and ensuring the imperceptibility. For capacity issue, secret data has been compressed via LZW coding since it is widely used in the literature and most importantly, it does not necessitates to send any additional

information to the recipient for decompression. Certainly, this situation has an additional contribution to capacity. For imperceptibility issue, secret data has been camouflaged in HTML (Hyper Text Markup Language) side of the web page without making any modification. After detecting the coordinates of the secret data on the web page, RSA (Rivest-Shamir-Adleman) encryption algorithm has been applied for the purpose of security. Then, these encrypted content has been compressed again and embedded to the URL (Uniform Resource Locator) of the concerning web page. Thus, we obtain the URL that has a legitimate length. Evaluation procedure of the proposed method has been carried out by measuring steganographic capacity in terms of percent. Besides, imperceptibility has been considered as the main issue. The rest of the paper has been organized as follows:

A detailed explanation of the proposed scheme has been provided in the 2nd section. The performed experiments and the obtained results have been mentioned in the 3rd section. Finally a general outcome has been expressed in the 4th section.

II. THE PROPOSED METHOD

Embedding and extracting phases of the proposed scheme will be explained in this section by mentioning the necessary calculations. It will be useful to provide a quick scenario, before a detailed explanation.

As noticed from the above sections, we proposed a steganographic scheme by employing HTML side of web pages. In the sender side, the secret message is firstly compressed. Then this obtained shorter content is hidden in source code (HTML side) of each web page in the collection, respectively. Namely we perform the same hiding operation for every web page in the collection. Here, the purpose is to find the best web page that provides the maximum capacity rate. After defining the best one, the compression operation is again applied to the achieved content as the result of hiding. Thus, capacity is increased again while the computation is being elaborated. Finally, the current content is encrypted and embedded in the URL of the concerning web page. So, it is sufficient to only send the obtained URL to the recipient since the secret message can be extracted by reaching the corresponding web page via this URL. Namely, once the recipient gets the URL, he/she can extract the secret message by applying inverse of the embedding phase.

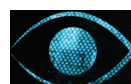
A. Embedding phase

Block diagram of the embedding phase has been provided in Figure 1.

Let's explain the operations and variables in each block.

1. *Compression*: Secret message is compressed via LZW coding in this step. Let M be an array containing characters of secret message and M' be the content after compression. As the result, we can claim that:

$$S(M') \leq S(M)$$



A HIGH CAPACITY HTML STEGANOGRAPHY METHOD

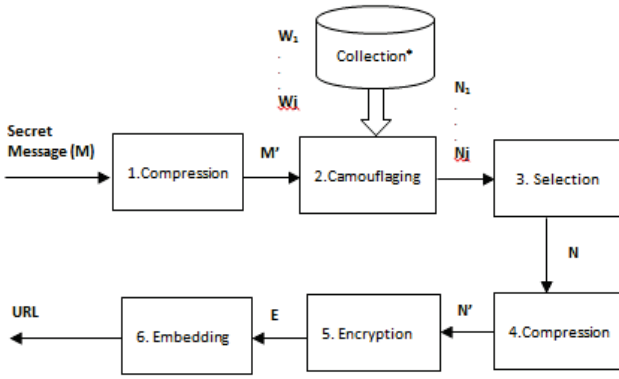


Fig. 1. Block diagram of the embedding phase

2. Camouflaging: In this step, we employ collection of web pages to enhance the capacity. Let W be a web page in the collection. We consider the source code, namely HTML side, of the web page for camouflaging. Thus, we can represent W as an array containing the symbols in the HTML side.

$$M' = (m'_1, m'_2, \dots, m'_i)$$

$$W = (w_1, w_2, \dots, w_j)$$

Since HTML side consists of the symbols including letters, numbers, marks and etc. we can perform the following operations to achieve the new content N :

$$\begin{aligned} m'_1 = w_1 &\rightarrow n_1 = 1 \\ m'_1 = w_2 &\rightarrow n_1 = 2 \\ &\vdots \\ m'_1 = w_j &\rightarrow n_1 = j \end{aligned} \quad (1)$$

Let's assume that $n_1=1$. This means that the first elements of W (the first symbol in HTML code) and M (the first character in secret message) are the same. After estimating the first element of N like that, the rest is estimated by considering the relative distances via Equation 2:

$$\begin{aligned} m'_2 = w_2 &\rightarrow n_2 = 2 - 1 \\ m'_2 = w_3 &\rightarrow n_2 = 3 - 1 \\ &\vdots \\ m'_2 = w_j &\rightarrow n_2 = j - 1 \end{aligned} \quad (2)$$

This operation is performed iteratively till all elements of M' is mapped. As the result we obtain a numerical array; N whose element number equals to the element number of M' .

$$S(N) = S(M') = j \quad (3)$$

The essential point in this step is that we perform the camouflaging for every W in the collection by using the same M' . Thus, we will be able to define the best W in the next step.

3. Selection: In this step, we consider the steganographic capacity rate to choose the best W in the collection. Steganographic capacity is calculated via Equation 4 [10]:

$$C = \frac{\text{BitsofSecretMessage}}{\text{BitsofStegoCover}} \quad (4)$$

Accordingly, we can adapt this formula to our scheme as follows:

$$C = \frac{\text{Bitsof}M'}{\text{BitsofURL}} \quad (5)$$

Notice that this calculation is performed for each W in the collection. As the result, W that gives the maximum C is chosen as the carrier to camouflage. Besides, rest of the operations are performed on N which corresponds to the chosen W .

4. Compression: The obtained N is compressed via LZW coding again. The purpose of this operation is to enhance steganographic capacity and elaborating the computation for steganographic security. At the end of this step, we have a new numerical array N' . Certainly we can claim that:

$$S(N') \leq S(N)$$

5. Encryption: In this step, N' is encrypted via RSA encryption algorithm. Let's call this content E . The purpose of this operation is to ensure steganographic security in case of any observations and to render the proposed scheme resilient against attacks.

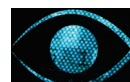
6. Embedding: In this step, the encrypted array; E is embedded into the URL of the chosen W (in step 3). Here, the most important point is not to have any error message when the modified URL is typed on the browser. Therefore, collection consists of the web pages which can be adapted to our scheme. Thus, for the sender, it is enough to send this URL to the recipient. There is no other content that has to be sent since the URL correctly directs the recipient to the chosen web page (W).

B. Extracting phase

Block diagram of the extracting phase has been provided in Figure 2.

Again, let's explain the operations in each block.

- 1. Separation:** In this step, the embedded part is separated from the URL, to apply the operations of the embedding phase in the reverse order. Thereby, we obtain array E .
- 2. Decryption:** E is decrypted via RSA. Thus, we obtain N' ; namely the compressed array that corresponds to the selected W .
- 3. Decompression:** In this step, we decompress N' to reach array N which is obtained after camouflaging (step 2) in embedding phase.



A HIGH CAPACITY HTML STEGANOGRAPHY METHOD

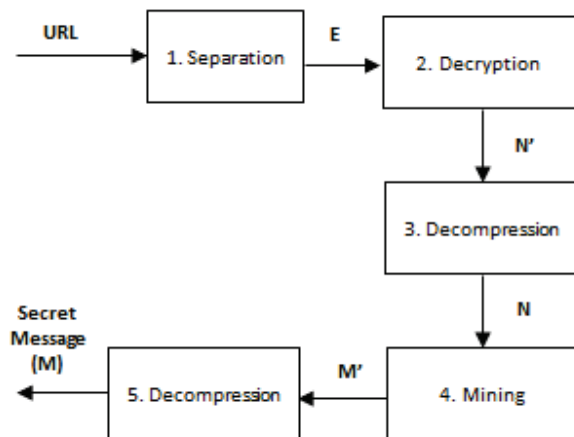


Fig. 2. Block diagram of the extracting phase

4. Mining: We have an URL that comes from the sender and we have N from the previous step. Thus, we can achieve M'; the compressed form of the secret message. Notice that the URL correctly directs us to the web page (W) used for camouflaging. We can obtain M' by performing the following mappings on the HTML side of the concerning W.

$$\begin{aligned}
 m'_1 &= w(n_1) \\
 m'_2 &= w(n_1 + n_2) \\
 &\vdots \\
 m'_j &= w(n_{j-1} + n_j)
 \end{aligned} \tag{6}$$

That is to say, m'_1 equals to the element of W indexed as n_1 , m'_2 equals to the element of W indexed as n_1+n_2 and so on.

5. Decompression: In this step, we decompress M'. Thus, we obtain M, the secret message by only employing the sent URL. Unlike the embedding phase, we neither used the collection, nor performed a selection since the URL provides us the carrier; namely the chosen web page.

III. EXPERIMENTAL RESULTS

In this section, the experimental procedure and the obtained results have been explained. The experiments have been carried out via a software written in C# language. For an unbiased evaluation, secret messages (M) have been produced by employing Lorem Ipsum texts (<http://www.tr.lipsum.com/feed/html>)[16]. Besides, for a wide-range observation, investigation phase has been carried out by considering different lengths of secret messages. Length of each secret message has been incremented 50 by 50 beginning from 50 to 600.

For evaluation, steganographic capacity has been considered in terms of percent. Capacity rate has been calculated for each secret message by using Equation 5. Results of the performed experiments and comparison results

TABLE I
CAPACITY VALUES TILL 600 CHARACTERS

n	Secret Message	C(%)
50	Lorem ipsum dolor sit amet, consectetur cras amet.	6.257
100	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam tristique nunc lectus, eu cras amet.	6.464
150	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer consequat eleifend orci sed mollis. Vestibulum lobortis malesuada purus nec volutpat.	7.038
200	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas erat massa, elementum at orci sed, feugiat dignissim urna. Nunc fringilla fermentum tempus. Donec feugiat neque lacus, sit amet metus.	7.532
250	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam gravida et erat ac ornare. Sed lectus dolor, iaculis nec nulla non, feugiat vehicula orci. Vivamus gravida dapibus enim sed elementum. Cum sociis natoque penatibus et magnis dis nullam.	7.727
300	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi tellus turpis, vulputate at bibendum sed, volutpat vitae leo. Phasellus vel nulla at leo accumsan volutpat sed vitae arcu. Ut id aliquam velit, et tristique metus. Sed laoreet ex vitae odio pulvinar ultricies. Ut sit amet augue volutpat.	7.947
350	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec est turpis, dapibus in felis in, euismod molestie ex. Mauris quis sapien in est tincidunt pulvinar quis nec arcu. Aliquam sit amet mattis lorem. Praesent volutpat, sem ac aliquam scelerisque, purus ligula tristique mi, at hendrerit nunc orci sed est. Vestibulum ante ipsum primis in sed.	8.241
400	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam sed vehicula est. Vestibulum dignissim a neque a blandit. Aenean auctor odio sit amet nibh faucibus facilisis. Quisque a tortor hendrerit diam sagittis mattis. Etiam ullamcorper ipsum finibus, pretium justo id, ullamcorper odio. Aliquam dapibus est in tincidunt facilisis. Nulla luctus scelerisque diam, et vulputate elit ultricies amet.	8.398
450	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent quis fringilla leo. Nam ut rhoncus ante. Sed venenatis ut nunc vitae bibendum. Phasellus vel urna ultricies, maximus lectus ut, porttitor metus. Curabitur luctus, mi sed iaculis accumsan, urna mi vestibulum lacus, nec luctus arcu tellus aliquam nisi. In ac finibus quam. Nulla facilisi. Cras hendrerit ante a est rhoncus malesuada. Vivamus eget ultrices augue. Proin at faucibus amet.	8.422
500	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut non tortor tempor, pharetra sapien non, fringilla erat. Sed at eleifend ex, at finibus massa. Etiam quis scelerisque metus. Duis est tellus, imperdiet et lorem sit amet, placerat elementum magna. Proin egestas, libero a varius gravida, est leo porttitor lorem, sit amet imperdiet sapien augue quis eros. Nam sit amet est malesuada, tempor purus eget, euismod ex. Vestibulum eget turpis id ex tempus maximus consectetur eget ante massa nunc.	8.557
550	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi rhoncus eu lacus non convallis. Nunc consectetur congue viverra. Phasellus vitae ligula eu justo sodales venenatis in ac nulla. Ut ornare consequat facilisis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aliquam in lacinia nunc, vel vehicula lorem. Suspendisse convallis tempor ipsum. Nullam vitae condimentum ex. Etiam magna ipsum, viverra eget velit nec, maximus condimentum lectus. Suspendisse aliquam egestas ligula, nec blandit metus.	8.712
600	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris ac urna eu lorem lobortis malesuada fermentum non enim. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Praesent id lobortis neque. Curabitur a commodo ipsum. Ut porttitor felis felis, eget imperdiet velit efficitur in. Nulla suscipit elit lacus, ac tincidunt turpis pulvinar sed. Nunc ultrices faucibus pulvinar. Pellentesque mattis dui id lorem sodales dapibus. Praesent semper, metus ut suscipit congue, neque orci tempus urna, vitae placerat purus nisl quis augue. Curabitur non volutpat.	8.850



A HIGH CAPACITY HTML STEGANOGRAPHY METHOD

in the literature have been indicated in Table 1, Table 2, respectively.

In Table 1, details about the performed experiments have been presented. Character length (n) of each secret message, the employed secret message produced via Lorem Ipsum and the obtained capacity rate have been provided. Graphical result of the performed experiments has been demonstrated in Figure 3.

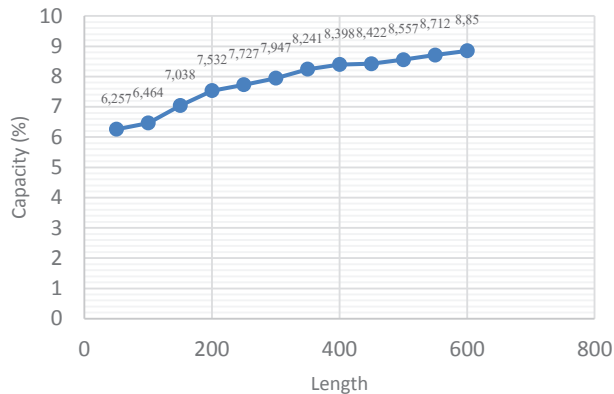


Fig. 3. Graphical result

In the given graph, we can see that there were small swings, but they are negligible. Namely, by basing on Figure 3, we observe that steganographic capacity continued to increase. The obtained maximum capacity value is 8.85% and the corresponding length is 600 characters. By basing on the given graph in Figure 3, we can claim that generally capacity increased as the length increased.

Comparison of the proposed method with the other contemporary methods in the literature has been presented in Table 2, in terms of capacity. Capacity of mimic function method that produces grammatically correct but meaningless texts has been calculated by employing Lorem Ipsum patterns via the given link. Capacities of Nicetext and Listega methods have been provided by basing on the samples in the cited articles. Capacities of translation based, Satir and Isik's schemes have been provided by considering the cited articles and thesis. Finally, capacity of Matlist method has been calculated statistically (averagely) by considering the given values in the cited article since this method is highly subject dependent. As seen in Table 2, the proposed method increased the capacity value to 8.85%. It has been calculated by employing the Lorem Ipsum Patterns via Eq. (5). This is a significant rate when the secret message containing 600 characters is considered.

For instance, the obtained URL for the secret message that has 10 characters, has been given below:

$$M = (L, o, r, e, m, i, p, s, u)$$

URL:

<http://www.selcuk.edu.tr/index.php?id=&NzYyLzExMDYyM>

TABLE II
COMPARISON RESULTS

Method	Capacity (%)	Explanation
Mimic functions[4],[5]	1.143	Calculated by employing Lorem Ipsum Patterns (http://www.spammimic.com/)
NICETEXT [6],[17],[18]	0.29	Provided by basing on the samples in the referred articles
Translation based [9]	0.33	Noted in by the authors the referred article
Listega [10]	3.87	Provided by basing on the example in the referred article
Satir and Isik [14]	6.92	Reported in the cited article
Satir and Isik [15]	7.017	Reported in the cited article
Satir and Isik in 2013 [19]	8.15	Reported in the cited thesis
Matlist [11]	8.74	Calculated averagely via the reported values in the referred article since it is subject dependent.
The proposed method	8.85	Calculated by employing Lorem Ipsum Patterns

jEvMzYvMzYvMzYvMjEvMzYvMzYvMTc2OS8yMS8zNi8zOC8zNi8yMS8zNi8zOC8xNDUvMjEvMzYvMzgvNjk2LzIxLzM2LzM2Lz2NC8yMS8zNi8zNi82OTYvMjEvMzYvMzYvNzYyLzIxLzM2LzM4LzE0NS8yMS8=

This URL is the steganographic cover that is sent to the recipient. When the recipient gets this URL, he/she types this on the browser and then he/she can extract the secret message by applying inverse of the embedding procedure. However, we observed that length of the obtained URL increased, too. This situation can conflict with the imperceptibility issue, since a very long URL address can raises suspicion.

IV. CONCLUSION

In this study, we proposed an HTML steganography method that employs URL addresses. Here, URL addresses have been used as steganographic cover and the HTML side of the corresponding URL has been used as a platform for camouflaging. Accordingly, it is enough to send only the obtained URL to the recipient.

Experiments have been performed by investigating steganographic capacity and imperceptibility. The capacity value is increased to 8.85% for the secret message containing 600 characters. Besides, it is observed that capacity increased as the character length increased. But it is observed that the length of the obtained URL increased, too. Since very long URL addresses can raise suspicion while communication, the balance between capacity and imperceptibility should be protected. Accordingly, hiding very long secret messages can endanger imperceptibility. For this situation we employed LZW coding. Besides, in case of making the algorithm public, we employed RSA encryption to provide security. Using LZW compression also supports steganographic security since it complicates the extraction procedure. For future studies, we aim to investigate the effects of other encryption-compression combinations to hide longer secret messages and thus, we will be able to render the proposed scheme more functional.



A HIGH CAPACITY HTML STEGANOGRAPHY METHOD

REFERENCES

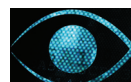
- [1] R. Radhakrishnan, M. Kharrazi, and N. Memon, "Data Masking: A new approach for steganography?," *Journal of VLSI Signal Processing* vol. 41, no.3, pp. 293-303, 2005.
- [2] A. Desoky, M. Younis, "Chestega: chess steganography methodology," *Security and Communication Networks*, vol. 2, no. 2, pp. 555-566, 2009.
- [3] D. Kahn, *The Codebreakers: The Story of Secret Writing*, Revised ed., Scribner, New York, 1996.
- [4] P. Wayner, "Mimic Functions," *Cryptologia*, vol. 16, no. 3, pp. 193-214, 1992.
- [5] P. Wayner, *Disappearing Cryptography (2nd edn)*. San Francisco, California, USA: Morgan Kaufmann, 2002, pp. 81-128.
- [6] M. Chapman, G. Davida, "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text," in *Proc. International Conference on Information and Communications Security, Lecture Notes in Computer Science*, vol. 1334, Springer, Beijing, P.R. China, 1997, pp. 335-345.
- [7] C. Grothoff, K. Grothoff, L. Alkhutova, R. Stutsman, and M. Atallah, "Translation-based steganography," *CERIAS Tech Report 2005-39*, West Lafayette, IN: Purdue University, 2005.
- [8] C. Grothoff, K. Grothoff, L. Alkhutova, R. Stutsman, and M. Atallah, "Translation-based steganography," In *Proc. Information Hiding Workshop (IH 2005)*, Barcelona, Spain: Springer-Verlag, June 2005, pp. 213-233.
- [9] R. Stutsman, C. Grothoff, M. Atallah, and K. Grothoff, "Lost in Just the Translation," In *Proc. The 21st Annual ACM Symposium on Applied Computing (SAC'06)*, Dijon, France, April 2006, pp. 338-345.
- [10] A. Desoky, "Listega: list-based steganography methodology," *International Journal of Information Security*, vol. 8, no. 4, pp. 247-261, 2009.
- [11] A. Desoky, "Matlist: Mature linguistic steganography methodology," *Security and Communication Networks*, vol. 4, no. 6, pp. 697-718, 2010.
- [12] B. Ryabko, D. Ryabko, "Constructing perfect steganographic systems," *Information and Computation*, vol. 209, no. 9, pp. 1223-1230, 2011.
- [13] K. Bailey, K. Curran, "An evaluation of image based steganography methods using visual inspection and automated detection techniques," *Multimedia Tools and Applications*, vol. 31, no. 3, p. 327, 2006.
- [14] E. Satir, H. Isik, "A compression-based text steganography method," *The Journal of Systems and Software*, vol. 85, no. 10, pp. 2385-2394, 2012.
- [15] E. Satir, H. Isik, "A Huffman compression based text steganography method," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 2085-2110, 2014.
- [16] (2014, Jul. 29) [Online].
<http://www.tr.lipsum.com/feed/html>
- [17] M. Chapman, G. I. Davida, and M. Rennhard, "A practical and effective approach to largescale automated linguistic steganography," in *Proc. Information Security Conference (ISC'01), Lecture Notes in Computer Science*, vol. 2200, Springer, Malaga, 2001, pp. 156-165.
- [18] M. Chapman, G. I. Davida, "Plausible deniability using automated linguistic steganography," in *Proc. International Conference on Infrastructure Security (InfraSec'02), Lecture Notes in Computer Science*, vol. 2437, Springer-Verlag, Berlin, 2002, pp. 276-287.
- [19] E. Satir, "Bilgi Güvenliği İçin Metin Steganografisinde Yeni Bir Yaklaşım," Ph.D. dissertation, Dept. Computer Eng., Selcuk Univ., Konya, Turkey, 2013.

E. Satir was born in Konya/Turkey 1983. She completed her undergraduate degree in Gazi University, Technical Education Faculty, Computer and Electronic Education Department, in 2005. She completed her graduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2009. her doctorate degree in Selcuk University, Faculty of Engineering, Computer Engineering Department in 2013. Currently, she is working as an assistant professor in Duzce University, Faculty of Engineering, Computer Engineering Department.

A. Sargin was born in Konya/Turkey 1990. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Karakopru Middle School in Sanliurfa.

T. Kanat was born in Nigde/Turkey 1991. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Konya.

C. Okuducu was born in Karaman/Turkey 1991. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Goger Middle School in Diyarbakir.



Security Analysis of the Encrypted Mobile Communication Applications

Murat Demircioğlu, Halil Kemal Taşkın and Salim Sarımurat

Abstract—Communication over the Internet have moved from desktop computers to handheld devices over the course of the last decade. People have started using cell phones, tablets etc. in daily lives and communication methods have switched to using these devices. Although there are many different options available for instant messaging between modern time internet users, not many of them provide trusted methods for securing the communicated message and considering users' privacy.

In this paper, we have analyzed the security and privacy concerns of three well-known and widely-used mobile communication applications called Telegram, TextSecure and Threema. We have defined the general security requirements expected from such applications and then compared their approaches individually.

Index Terms—Mobile Messaging, End-to-end Security, Telegram, TextSecure, Threema,

I. INTRODUCTION

INSTANT messaging is a kind of online chat offering a real-time text transmission over the Internet. As the mobile technology evolves, a new kind of instant messaging takes place and it is called Mobile Instant Messaging. In this technology, instant messaging services can be accessible from a portable device, ranging from smart phones to tablet computers which use the operating systems such as Android [1], iOS [2], Blackberry OS [3], Windows Phone [4], etc. There are so many mobile chat applications to use in the mobile devices.

Beside this, as the ordinary users become conscious about the information security, they demand secure mobile messaging applications. For this purpose, so many applications are provided.

In this paper we compare three of the most popular secure mobile communication applications in the manner of security. These are Telegram[5], TextSecure[6] and Threema[7].

In Section II, we specified 10 security requirements for a secure mobile messaging application. Then the selected three applications are compared under these requirements in Section IV. At the end, the overall security of them are stated in Section V.

M. Demircioğlu and H.K. Taşkın are with the Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University.

M. Demircioğlu, H.K. Taşkın and S. Sarımurat are with Oran Information Technologies.

S. Sarımurat is with the Department of Computer Science and Engineering, Sabancı University.

This paper is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under the project number TEYDEB-1130063 titled "Mobil Terminaller Üzerinde Kriptografik Yöntemler Kullanılarak Uçtan Uca Güvenli Bir İletişim Sisteminin Tasarlanması ve Geliştirilmesi".

II. SECURITY REQUIREMENTS

A secure mobile chat application should provide the following properties.

1) *Cryptographic Primitives*: Cryptographic primitives are low-level cryptographic algorithms which are well-established and generally used to create cryptographic protocols. Some of the commonly used primitives are:

- Authentication,
- Symmetric key cryptography,
- Public key cryptography,
- Digital signatures,
- One-way hash functions,
- Pseudo random number generator.

2) *Forward Secrecy*: Forward secrecy is a kind of key-agreement protocol. It ensures that if the attacker compromises one of the long-term keys in the future, then s/he can not compromise a session key produced from a set of long-term keys. The key used to encrypt the data must not be used to produce any other keys, and if the key used to encrypt data is produced from some other keying material, then this material must not be used again to produce any other keys. By this way, compromise of a single key allows access only to data encrypted by that single key.

3) *Disk Encryption*: In order to protect digital data, disk encryption techniques convert data into unreadable code which can not be deciphered easily by unauthorized people. Disk encryption software or hardware is used to encrypt every bit of data on a disk or disk volume. By this way, unauthorized access to data storage is prevented.

4) *Secure Group Chat*: In addition to establishing secure connection between two parties, users may want to add more participants to their conversation without leaving the secure environment provided by the application.

5) *Multiple Device Support*: The protocol should include support for users having multiple devices. In this scenario, any user can have multiple devices with the secure chat application. If a secure message is wanted to sent via the application, it should be reachable through all devices of the recipient and previous chat logs should also be reachable from all devices of both the sender and the recipient.

6) *Fingerprint Verification*: In order to prevent man-in-the-middle attack (MITM) attacks, users should verify each others' identities by using offline methods. For this purpose, parties can read their fingerprints to each other on an offline channel or they can use QR code to verify each other.

7) *Contact List Synchronization*: Contact list of the users should not be stored on the servers in a clear text. Instead

of this, hash value of the contact list can be stored on the servers and periodically it can be checked if new users from the contact list have started to use the application.

8) *Open Source*: Open source software is a software development methodology whose source code is publicly available to anyone for modification, security control or enhancement. Any software, which are not open source, may have some security flaws or backdoors.

9) *Self-Destruction*: Setting a time for self-destruction provides automatically deletion of messages. After the self-destruction time runs out, the messages are wiped out automatically from all devices.

10) *Emergency Passphrase*: There will be two pass phrases set for the application. One of them is to secure the application data and the second one for the emergency case. If someone forces user to give the passphrase, s/he will give the second passphrase and it will erase all data.

III. DESCRIPTION OF MOBILE APPS: TELEGRAM, TEXTSECURE, AND THREEMA

In this section, we give the general descriptions of the applications which we have compared. These applications are Telegram, TextSecure and Threema, respectively.

A. Telegram

Telegram is an open source encrypted instant messaging application for iOS, Android and Windows Phones. It has also unofficial desktop applications for OS X, Windows and Ubuntu. Browser extension is also an alternative for mobile communication, but the user needs to register his/her phone on a mobile Telegram application. Telegram provides encrypted and self-destructing messages, photos, videos and documents.

The application offers two types of chats. Standard chat uses client-server encryption and it can be accessed from multiple devices. Secret Chat uses end-to-end encryption and two participating devices can only access to it. Telegram claims that third parties, including them, can not get access to the messages. Self-destruction time can be set for messages and media in a Secret Chat. After the self-destruction time runs out, the messages are wiped out automatically from both devices.

All kind of chats are encrypted with the new protocol MTProto [9] which is created by Nicolai Durov. The protocol is based on RSA 2048 encryption [10], 256-bit symmetric AES [11] encryption and Diffie-Hellman key exchange protocols [12].

Chat history of Telegram is stored on Telegram cloud servers and accessible from any number of devices. On the other hand, secure chat logs are only accessible from two participating devices, and users' other devices can not reach to the encrypted chat logs.

Telegram provides a standard group-chat option up to 200 members. However, it does not support secure group-chat. Most people use group-chat feature of messaging applications frequently, so this is a very important drawback for Telegram.

Message read status is enabled in Telegram; one check for sent messages and two checks for read messages. In this way the sender can ensure whether the message is sent or read.

Clients of Telegram are open source, so verifying the end-to-end encryption mechanism is possible. However, server-side software of Telegram is closed source, so it is not possible to verify the claimed encryption standards are properly used and well implemented.

B. TextSecure

TextSecure is an open source encrypted messaging application for Android devices. TextSecure uses an end-to-end encryption protocol which provides secrecy for instant messages, MMS and SMS. Open WhisperSystems is the developer of TextSecure and it is released under the GPLv3 license. Whisper Systems is co-founded by roboticist Stuart Anderson and security researcher Moxie Marlinspike in 2010. Moreover, Whisper Systems produced the application RedPhone which provides encrypted voice calls. The Guardian Project [8] also supports and recommends TextSecure.

By using TextSecure, users are able to send text messages, group messages, photos, videos, documents and contact information over 3G, LTE or Wi-Fi to other TextSecure users.

TextSecure uses standard SMS/MMS to communicate with non-TextSecure users. Blue and green text bubbles are used to distinguish messages that have been sent via the user's data connection and messages that have been sent via SMS/MMS. Blue bubble indicates communication over a data connection and green bubble indicates SMS-based communication.

TextSecure will use the user's data connection as default if possible to send the message. In other words, if the user sends a message to another registered TextSecure user, it will be treated as an additional data transfer and there will be no SMS charge associated with the message. If there is not any available data connection, then the application will use standard SMS/MMS to send the message.

The application will automatically encrypt all conversations held with other registered TextSecure users. In the user interface, encrypted messages are denoted by a lock icon. Media and other attachments are encrypted in the same way as other messages.

TextSecure also encrypts users' text locally on their smartphones. Anything stored by the app is encrypted on their Android device. The application will encrypt all conversations ongoing with other registered TextSecure users and the encrypted messages are indicated by a lock icon. In addition, media and other attachments are encrypted in the same way. Therefore, if the attacker is able to gain physical access to users' phone, s/he will not be able to obtain plain data of this encrypted data.

TextSecure provides group chat. Users can create a group, name it, set an avatar, and invite unlimited number of recipients, who are all able to leave at will.

TextSecure uses Off-the-Record (OTR) [15] protocol and made some improvements to the deniability and forward secrecy aspects, and added a mechanism to allow the ephemeral key negotiation to work asynchronously. TextSecure uses Curve25519 [13], AES-256, and HMAC-SHA256.

Verification of the users communicating with is done via comparing their fingerprints. Thus, MITM attacks are prevented. The keys which are used to encrypt the user's messages

are stored on the device alone, and they are protected by an additional layer of encryption if the user enabled a passphrase.

In order to ensure that new AES keys are used for every single message, TextSecure uses the cryptographic ratchet [6]. It also provides both forward secrecy and future secrecy properties. The protocol also features enhanced deniability properties.

TextSecure-Server is the software that handles message routing for the data channel. Client-server communication is protected by TLS/SSL. REST API and push messaging are used to handle communication.

The servers do not store any contact information. Hashed contact numbers (with no other accompanying information) are periodically uploaded to the servers in order to determine which contacts are also TextSecure users, but this data is never stored.

C. Threema

Threema is a commercial encrypted messaging application for iOS and Android devices. It provides asymmetrically end-to-end encrypted instant messages, group conversations, multimedia files and voice messages. Users can also share their GPS locations securely via Threema.

After the application installed for the first time, a key pair is generated and the public key is sent to the server while the private key is kept on the user's device. Then all messages and media files that are sent to other Threema users are encrypted with their respective public key.

The Swiss company Threema Kasper Systems GmbH develops Threema. The application is especially popular in German speaking countries.

Threema is not an open source application. Therefore, it can not be reviewed without the agreement of its authors. Validation Logging feature of the application can be used to log the incoming and outgoing messages. This feature logs the bodies of the message, but not all the data that is exchanged with the server. So, there is no way to prove that the message that is being logged correlates to data that is being sent by the application. So, it is hard to trust completely to this application.

Threema is using the NaCl Cryptography Library [16] and it works properly on both iOS and Android.

In order to show the verification level of contacts Threema shows three dots next to every contact. One red dot means no verification, two yellow dots mean that a user's identity has been verified by the server, and three green dots mean that user's key and ID have been personally scanned and verified. This is a good way to direct users to use strong security and prevent MITM attacks.

The protocol does not provide a Perfect Forward Secrecy, but they claim to have implemented it at the transport layer. Forward secrecy is provided on the network connection (not on the end-to-end layer). Client and server negotiate ephemeral random keys. They are stored in RAM and replaced every time the app restarts (or at least once every seven days).

Asymmetric cryptography is used to protect the communication between two users and the communication between the

application and the servers. ECDH on Curve25519 is used with a hash function and a random nonce to generate a unique 256 bit symmetric key for each message, and then XSalsa20[14] stream cipher is used to encrypt the message. A 128 bit MAC is added to each message to detect changes. Servers' public keys are hard-coded into the application.

Threema has two layers of encryption; one is the end-to-end layer between two users, and the other is an additional layer between the app and the servers to protect against eavesdropping. All local files are also stored encrypted on the device. Encryption and decryption of the messages are made on the device. Therefore, they claim third parties can not decrypt the messages.

IV. COMPARISON

In this section the security requirements are compared for Telegram, TextSecure and Threema. Each topic mentioned in Section II are explained separately and the differences between these applications are shown briefly in the Table I.

- 1) **Cryptographic Primitives:** State of art cryptographic algorithms should be used in the protocol.

Telegram uses its own protocol called MTPROTO Mobile Protocol. It consists of AES-256 encryption with infinite garble extension (IGE), and hash function SHA-1. Using SHA-1 is not a good option, because studies [17] showed that SHA1 has some major vulnerabilities.

TextSecure uses ECDH on Curve25519, AES-256 for symmetric key encryption, and HMAC-SHA256 in its protocol. These algorithms have been used in hundreds of applications and tested for many years. So, TextSecure has chosen to use state of art algorithms.

Threema uses ECDH on Curve25519 and stream cipher XSalsa20 to encrypt the message. 128 bit MAC is also added to the end of each message.

In conclusion, TextSecure and Threema prefer to use state of art cryptographic algorithms. But Telegram uses SHA-1 which has some security problems, and their AES-IGE mode selection is questionable.

- 2) **Forward Secrecy:** In forward secrecy, if one of the long term keys is compromised, a session key produced from a set of long-term keys can not be recovered.

Telegram supports forward secrecy in an impractical way. In order to provide forward secrecy, user should delete message logs and start a new secure conversation. So, forward secrecy is achieved manually.

TextSecure supports forward secrecy and it uses its own OTR protocol.

Threema provides forward secrecy between client and server. There is no end to end forward secrecy between clients.

Therefore, TextSecure is the only application providing forward secrecy among these three applications.

- 3) **Disk Encryption:** All data of the application should be stored encrypted in the disk of the mobile device. Otherwise, physical access to the mobile device will lead to a security vulnerability.

Telegram does not provide disk encryption.

In *TextSecure*, when the application started, it asks the passphrase which was set on the first installation. All data used by *TextSecure* are encrypted by this passphrase. Unless the application is completely terminated, it continues to operate on background and does not ask for the passphrase again.

Threema uses different methods of disk encryption for iOS and Android. In iOS, *NSFileProtectionComplete* Library is used to encrypt the data, and the device PIN is used for the encryption key. While the screen is unlocked, the application can be used without a key, but a four digit PIN can be set in the application settings for an extra security.

Therefore, *TextSecure* and *Threema* both provide disk encryption, but *Telegram* does not.

- 4) **Secure Group Chat:** A group chat is a standard part of the mobile chat applications. But in a secure chat application, it is expected that the group chat is also secured.

Telegram provides a group chat up to 200 participants, but it is not a secure chat. The application provides secure chat for only one to one conversations.

TextSecure provides a secure group chat option with unlimited participants.

Threema supports a secure group chat up to 20 users, but none of the participants of the group can be removed. For any change in the group participants, the conversation is restarted again with new encryption keys.

Therefore, only *TextSecure* and *Telegram* support secure group chat, but *TextSecure* looks like a little bit better.

- 5) **Multiple Device Support:** This option is not available in both *TextSecure* and *Threema*. But in *Threema* it is planned to add multiple device support in the future. In *Telegram*, users can log-in multiple devices with the same phone number. While adding a new device, a verification code is sent to other previously registered devices. After verification completed, the name of the new added device and its IP address is also sent to other devices. But when a secure chat starts, the messages are received by only one device.

So, none of the above applications support multiple devices.

- 6) **Fingerprint Verification:** Verification of users by using offline methods will prevent MITM attacks.

In *Telegram*, the symmetric key used for the session is showed as a QR code like picture on the device screen, and then users can compare them.

TextSecure users can verify their identities by showing their fingerprints in text format to each other, or by scanning QR code of their finger prints.

In *Threema*, if users verify each other via QR code, it will be stated as the highest security level verification and these users are labeled with three dots.

So, all applications have an offline verification methods.

- 7) **Contact List Synchronization:** Both *Telegram* and *TextSecure* send the contact list of the user to the servers in a clear text format to find the other users using the

same application. On the other hand, *Threema* sends the hash values of phone numbers and e-mail addresses in the contact list of the user to the server.

Since the space for all phone numbers is $10^{10} \approx 2^{33}$, it is easy to build a rainbow table for phone numbers and compare the hash values. So, taking hash of the phone numbers is not an enough security measure.

- 8) **Open Source:** *Threema* is not an open source application, so it is not possible to verify what they say about their security. On the other hand *Telegram* and *TextSecure* are open source. Therefore, one can check the code easily to verify its security.
- 9) **Self-Destruction:** This option is only available for *Telegram* users. In a session, the self-destruction time can be set at anytime. After the time expires, the message is deleted automatically.
- 10) **Emergency Passphrase:** This option is not available in these applications. But in security forums, this feature is wanted in the case of emergency.

V. CONCLUSION

In this paper, 10 security criteria are defined to compare *Telegram*, *TextSecure* and *Threema*. These criteria are explained in Section II and the applications are compared in Section IV. Both three applications doesn't support multiple devices and emergency passphrase.

Although *Telegram* becomes very popular in a short time, adding some more features (e.g. disk encryption and secure chat) to it will be good for its security.

Threema comes the second in this comparison. Not having an efficient secure group chat and not being an open source are the main disadvantages of this application.

Among these three applications *TextSecure* provides better features for a secure chat. The lack of iOS support is the main shortage.

ACKNOWLEDGMENT

The authors would like to thank Ali Aydın Selçuk and Mutlu Çiçek for their support and assistance with this project.

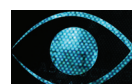


TABLE I
COMPARISON OF TELEGRAM, TEXTSECURE AND THREEMA

	Telegram	TextSecure	Threema
Cryptographic Primitives	Own protocol which consists of AES-256 in IGE mode and SHA-1	ECDH on Curve25519, AES-256, HMAC-SHA256	ECDH on Curve25519, XSalsa20
Forward Secrecy	Impractically supported	Supported	Supported between client-server communication
Disk Encryption	Not supported	Supported	Supported
Secure Group Chat	Not supported	Supported up to 200 participants	Supported up to 20 users
Multiple Device Support	Supported, but secure messages are received by only one device	Not supported	Not supported
Fingerprint Verification	The symmetric key used for the session is showed as a QR code like picture on the device screen	Showing their fingerprints in text format to each other, or by scanning QR code of their finger prints	Verifying each other via QR code
Contact List Sync.	Sends the contact list of the user to the servers in a clear text format	Sends the contact list of the user to the servers in a clear text format	Sends the hash values of phone numbers and e-mail addresses in the contact list of the user to the server.
Open Source	Open source software	Open source software	Proprietary software
Self-Destruction	Supported	Not supported	Not supported
Emergency Passphrase	Not supported	Not supported	Not supported

REFERENCES

- [1] Official Android Page, <http://www.android.com>
- [2] Official iOS Page, <https://www.apple.com/ios>
- [3] BlackBerry 10 OS <http://us.blackberry.com/software/smartphones/blackberry-10-os.html>
- [4] Official Windows Phone Page, www.windowsphone.com
- [5] Telegram, <https://telegram.org/>
- [6] TextSecure, <https://whispersystems.org/>
- [7] Threema, <https://threema.ch/en/>
- [8] The Guardian Project, <https://guardianproject.info/>
- [9] MTProto Mobile Protocol, <https://core.telegram.org/mtproto>
- [10] RSA Cryptosystem, <http://en.wikipedia.org/wiki/RSA>
- [11] AES Block Cipher, <http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>
- [12] Diffie-Hellman, <http://www.ietf.org/rfc/rfc2631.txt>
- [13] Curve25519: high-speed elliptic-curve cryptography, <http://cr.yp.to/ecdh.html>
- [14] The Salsa20 core, <http://cr.yp.to/salsa20.html>
- [15] Nikita Borisov, Ian Goldberg, Eric Brewer (2004-10-28), *Off-the-Record Communication, or, Why Not To Use PGP*, Workshop on Privacy in the Electronic Society. Retrieved 2014-03-06
- [16] NaCl: Networking and Cryptography library <http://nacl.cr.yp.to/>
- [17] Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu, *Finding collisions in the full SHA-1*, in Advances in Cryptology, CRYPTO'05

Halil Kemal Taşkın Halil Kemal Taşkın (S'14) graduated from Department of Mathematics Teaching at Gazi University, Turkey in 2009. He then received his M.Sc. degree in Cryptography from Institute of Applied Mathematics at Middle East Technical University in 2011 and he has been continuing his Ph.D. studies at the same department since 2011. During his studies, he has worked on Block Cipher Cryptanalysis and involved in a project about Differential Cryptanalysis funded by TÜBİTAK. Since 2013, he has been working as Cyber Security Specialist in Oran Teknoloji, Turkey.

Salim Sarımurat Salim Sarımurat graduated from Computer Engineering Department of Bilkent University, Turkey, in 2011. He then received his M.S. degree from Computer Science and Engineering Department of Sabancı University, Turkey, 2013. During his M.S. studies, he was working on a project, funded by Scientific and Technological Research Council of Turkey (TÜBİTAK), to develop secure key predistribution methods for mobile and multiphase Wireless Sensor Networks that improves resiliency performance against node capture attacks. Salim currently works as an Information Security Consultant.

Murat Demircioğlu Murat Demircioğlu (S'14) was born in Istanbul, Turkey, in 1986. He graduated from Department of Mathematics at Middle East Technical University, Turkey, in 2009. He then received his M.Sc. degree in Cryptography from Institute of Applied Mathematics at Middle East Technical University, Turkey in 2011 and he has been continuing his Ph.D. studies at the same department since 2011. During his studies, he has worked on Quantum cryptography and also involved in a project about Differential Cryptanalysis funded by TÜBİTAK. He worked as a Research Assistant in Institute of Applied Mathematics of Middle East Technical University, Turkey, from 2012 to 2013. Since 2013, he has been working as Cyber Security Specialist in Oran Teknoloji, Turkey.

Farklı Güvenlik Seviyesindeki Ağların Bağlanması İçin Bütüncül Bir Model

M. Kara

Özet—Kurumsal bilgilerin bilgisayar ağları üzerinde işlenmeye, iletmeye ve saklanmaya başlaması ile birlikte kurumlar arası veri paylaşımı da büyük önem kazanmıştır. Gizlilik seviyesi olmayan bilgiler, bilinen güvenlik teknolojileri ile paylaşılmasına karşın farklı güvenlik seviyesindeki ağların birbiri ile veri paylaşımı için bu güvenlik önlemleri yeterli olmamaktadır. Farklı güvenlik seviyesindeki ağ bağlantılarını bazı özel durumlar çerçevesinde ele alan ve özel ihtiyaçlara cevap birkaç ürün dışında konuyu hem yönetsel hem teknik olarak ele alan bütüncül bir bakış açısına sahip yaklaşımlar bulunmamaktadır. Bu makalede farklı güvenlik seviyesinden ağların birbirine bağlanması bütüncül bakış açısı ile ele alınmış ve genel bir model sunulmuştur.

Abstract- all information of Organizations are processed on computer networks. This is increase importance of information sharing. Unclassified information can be shared with traditional security solution at internet but traditional security solutions is not secure for data sharing between different security level networks. There are a few special technical solutions connecting different security level networks but none of them is not provide general solution which is include technical and managing concepts. In this paper, a totalitarian model is presented for different security level network connection.

Anahtar Kelimeler—Farklı Güvenlik Seviyesine Sahip Ağlar, Bilgi Değişim Geçidi, Diyet, Air Gap, Gizlilik Seviyesi, Güvenlik Önlemleri

I. GİRİŞ

Günümüzde kurumlara ait veriler hızla kağıt ortamından sayısal ortama taşınmaktadır. Bu da bilgilerin kolay bir şekilde erişilebilir, işlenebilir, saklanabilir ve iletilebilir olmasına imkan vermektedir. Bilgilerin sayısal ortama taşınmış olması, kurumun kendi bilgilerine hızlı erişimi sağlaması yanında diğer kurumlarla da güvenli bir biçimde paylaşılması ihtiyacını doğurmaktadır. Örneğin, Nüfus Vatandaşlık İşlerindeki (NVİ) bazı kişisel bilgilere, Adalet Bakanlığı, Sosyal Güvenlik Kurumu gibi kurumların ihtiyacı olabilmektedir. Suçlulara ve suçlara ait bilgilerin Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü (EGM) tarafından paylaşılması gerekebilmektedir. E-Devlet uygulamaları ile bu paylaşım ihtiyaçları her geçen gün artmaktadır.

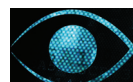
Hali hazırda TUBİTAK BİLGEM’de yürütülen Kelepçe projesi kapsamında kurumları veri paylaşım analizi ihtiyaçları

ve uygulamaları ele alınmıştır. Bu çalışmada kurumlar arasında bilgi paylaşımının çoğunlukla kağıt, sabit disk, taşınabilir bellek veya CD/DVD gibi çevrim dışı (offline) saklama ortamlarında veya resmi yazılarla ilettiği görülmektedir. Bu çevrim dışı veri iletim yönetimi ile veriler ilgili kuruma zamanında ulaşamamakta ve hızlı bir şekilde işlenememektedir. Bazı uygulamalarda kurumlar arasında kiralık hat çekilerek veya internet üzerinde sistemlere/uygulamalara sınırlı haklar verilerek yapılmaktadır. Bu paylaşımları kapsamlı olarak ele alan yasalar, yönetmelikler bulunmamaktadır.

Veri paylaşım ihtiyacı, gizli veya gizli olmayan bilginin paylaşarak bilginin ekonomiyeye kazandırılması düşüncesiyle ortaya atılmıştır. Bu yaklaşımda kamuda toplanan verilerin farklı kurumlar tarafından değerlendirilerek yeni ve topluma faydalı sonuçlar elde edilmesi hedeflenmiştir. Bu paylaşım verilerin ve uygulamaları doğası gereği beraberinde çeşitli kısıtlama ihtiyaçlarını da gündeme getirmektedir. Kısıtlar bilginin mahremiyeti, ticari sırların ve özel hayatın korunması, devletin güvenliği, fikri mülkiyet gibi kavramlar ekseninde gelişmiş, bu çerçevede özellikle hukuk alanında yeni düzenlemeler ihdas edilmiş ve önleyici bir taktikle olası zararların önüne geçecek yapılar kurulmuştur. Kamu sektörü bilgisinin yeniden kullanımı konusu, hukuki düzenlemelerle de iç içe geçmiş olup, bu kapsamda ülkeler yasal düzenlemeler yapmaktadır[1]. Literatürde ve uygulamalarda daha çok tasnif dışı, hizmete özel ve özel verilerin paylaşıldığı görülmektedir. Ülkemizde de kamu kurumlarının birbirleri arasında tasnif dışı, hizmete özel, özel ve gizli bilgileri paylaşma ihtiyacı bulunmaktadır.

Bilgisayar ağlarında işlenen, iletilen ve saklanan bilgilerin gizlilik seviyeleri ve koruma önlemleri farklı olmasına karşın, bu ağların birbirleri ile veri paylaşması ve veri aktarması günümüzde bir ihtiyaç haline gelmiştir. Bu ağların güvenlik seviyeleri aynı dahi olsa farklı kurumların verileri olduğu için doğrudan bağlanmaları mümkün olmamaktadır. Veri paylaşımı için kurumlar birbirinden özel ek teknik ve yönetsel güvenlik önlemleri talep edilebilmektedir. Bu kapsamda bu makalede, farklı ağlar arasında olası bağlantılar ve bunların sağlanması gereken güvenlik önlemleri hem teknik hem yönetsel olarak bütüncül bir bakış açısı ile ele alınmıştır.

Günümüzde farklı kurumların veri paylaşım ihtiyacının aşağıdaki yapılarda olduğu Kelepçe projesi kapsamında yapılan veri paylaşım ihtiyaç analizi çalışmasında ortaya çıkmıştır.



FARKLI GÜVENLİK SEVİYESİNDEKİ AĞLARIN BAĞLANMASI İÇİN BÜTÜNCÜL BİR MODEL

KAMU ↔ KAMU
 KAMU ↔ TÜZEL KİŞİ
 KAMU ↔ TSK
 KAMU ↔ YABANCI ÜLKE KURUMLARI
 TSK ↔ NATO

Bu ağların gizlilik seviyeleri göz önüne alındığında ağlar arasında olabilecek bağlantı türleri Tablo 1’de verilmiştir. Genel uygulamalara bakıldığında günümüz güvenlik teknolojileri ile çok gizli ağlara erişimin verilmemesi yönündedir. Farklı güvenlik seviyelerine sahip ağların bağlantısında yüksek seviyede olan ağın güvenlik gereksinimlerini karşılayacak şekilde yapılandırma gereklidir. Bunun yanında ağların birbirine bağlanmasını sağlayan bilgi değişim ağ geçidi (Information Exchange Gateway- IEG) büyük önem taşımaktadır [2].

		KURUM A				
		Çok Gizli	Gizli	Özel	Hizmete Özel	Tasnif Dışı
KURUM B	Çok Gizli	X	X	X	X	X
	Gizli	X	✓	✓	✓	✓
	Özel	X	✓	✓	✓	✓
	Hizmete Özel	X	✓	✓	✓	✓
	Tasnif Dışı	X	✓	✓	✓	✓

Tablo 1 Farklı güvenlik seviyesindeki ağlar arası iletişimde güvenlik gereksinimleri

Farklı güvenlik seviyesindeki ağlar arasındaki bilgi paylaşımı, bütüncül bakışa açısı ile olmalıdır. Bu makale bu bakış açısını koruyacak şekilde tasarlanmıştır.

Bölüm 2’de literatür taraması ele alınmıştır.

Bölüm 3’de bu konuda geliştirilen teknolojiler tanıtılmıştır.

Bölüm 4’de farklı güvenlik seviyesindeki ağların bütüncül bakış açısını ele alınması için yapılması gerekenler ele alınmıştır.

Bölüm 5’de sonuç ve öneriler verilmiştir.

II. LİTERATÜR TARAMASI (NP)

A. Bilimsel Makaleler ve Standartlar

Bu konularda yayınlana ve öncelikli makaleler konularında bilgi verilecek.

Gelecek askeri operasyonların etkin ve efektif yapılabilmesi için veri paylaşımı çok önemlidir. Network Enabled Capability (NEC) olarak adlandırılan bu sistemlerle NATO, NATO üyesi ve partner ülkeler arasında bilgi paylaşımı tanımlanmaktadır. Bu tür karmaşık sistemler aslında veri paylaşımı oldukça zordur. Boonstra ve arkadaşları bu tür sistemler arasında veri

paylaşımını ağ güvenlik unsurlarını çok küçük güvenlik parçalarına bölünerek her bir noktada sadece gerekli güvenlik unsurlarını içeren bir donanım/yazılım kullanılmasını içeren bir model sunulmuşlardır [3,4,5].

Farklı kurumlar arasında güvenli veri paylaşımı için XML etiketleme ve meta verileri kullanan çözümler geliştirilmiştir[4,6,7]. Bu konuda NATO’da XML kontrolü sağlayan bir koruma profili tanımlanmıştır.

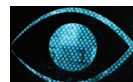
NEXOR firması NATO tarafından güvenli veri haberleşmesinin temini için IEG konsepti, bileşenleri ve amacı konusunda üst seviyeden ele alan referans dokümanını oluşturmuştur [2]. Apiecionek ve arkadaşları Nexor firmasının geliştirdiği IEG’nin yeteneklerine ek olarak Extensible Messaging and Presence Protocol (XMPP), FTP, HTTP gibi birçok protokolü destekleyen çözümü geliştirmişlerdir [8].

Serrano ve arkadaşları genel hatlarıyla NATO ülkeleri ve diğer paydaşlar arasında bilgi paylaşımına yönelik zorluklar irdelemiştir. Böyle bir paylaşım için öncelikli olarak yanıtlanması gereken "Ne paylaşmak isteniyor?", "Hangi durumlarda paylaşım yapılmalı?", "Hangi protokol veya araçlarla yapılabilir?" vb. gibi bazı soruları ele almışlar. NATO için bu tür bir bilgi paylaşımı farklı alanlardaki proje ve organizasyonlardaki girişimler ölçeğinde olup gereksinimlerin sadece bir alt kümesini sağlayan kısmi çözümler önermektedirler. Aynı zamanda NATO bilgi paylaşımı için bir yok haritası çıkarılmıştır. Bunlar her paydaş için farklı cevaplara sahip durumdadır. Paydaşlar arasında bu soruların cevapları hususunda tek bir mutabakata varılması ve ölçeklenebilirlik güç olduğundan bütünsel bir çözüm sağlanmasını kısmen karşılamaktadır [9].

Bu raporda, gizlilik seviyesi yüksek olan savunma, istihbarat ve milli güvenlik kurumlarının ağları ile gizli olmayan kamu ağlarının gerçek zamanlı iş birliği için birbirleri arasındaki etkili ve güvenli veri paylaşımına yönelik gerekli olan güncel ihtiyaçlardan bahsedilmektedir. Aynı zamanda Ezenia InfoWorkSpace (IWS) sisteminin temel yeteneklerine ve MLS (Multi Level Security) ile olan ilişkilerine değinilmektedir [10].

Dean arkadaşları yüksek ve düşük güvenli bölge arasındaki iki yönlü, güvenli bilgi transferi sağlayan air-gap dışındaki alternatif tekniklerden bahsedilmiştir. Bu teknikler format kontrolü, ağ güvenlik seviyesi kontrolü ve kullanıcı onayı gibi teknolojileri içermektedir. Birleşik Krallık Savunma Bakanlığı sorumluluğunda yürütülen araştırmalarda, QinetiQ firması çift yönlü ve güvenli haberleşme için çeşitli teknolojiler üzerinde çalışmaktadır [11]. James ve arkadaşları bulut üzerinden gizlilik seviyesi olan verilerin güvenli olarak paylaşılması ele alınmaktadır [12].

Asseco Poland tarafından gizlilik dereceleri değişen sivil ve askeri kurumlara arasındaki güvenli haberleşmenin sağlanması için Multi Level Security System sistemleri



tasarlamıştır. Bu yapı SOA (Service Oriented Architecture) mimarisi doğrultusunda tasarlanmıştır **Error! Reference source not found.**

Harris ve arkadaşları, halk sağlığı konusunda devlet kurumları, finans kurumları, üniversiteler ya da hastaneler arası güvenli veri paylaşım standartlarını ele almıştır. Makalede veri paylaşımı için etkili bir organizasyon gerekliliği vurgulanmıştır. Ayrıca güvenli veri paylaşım teknikleri ve esnek mimari hakkında belli standartlara dayanarak yapılan yaklaşımlar ele alınmıştır **Error! Reference source not found.**

Chen ve arkadaşları Çin'in kamu ve endüstriye ait geniş ağlarının birbirine bağlanması ihtiyacının giderilmesi için güvenlik koruması ve ağ sınır kontrol sisteminin tasarlanması üzerinde durulmuştur. Güvenlik koruması ve ağ sınır kontrol sistemleri, yazılımsal ve donanımsal araçlar ile beraber güvenlik standartları ve politikalarını da kapsamaktadır [15].

B. Ülke ve organizasyonların Genel Yaklaşımları

AGB, Norveç, Japonya, Çin, Avrupa Birliği ülkeleri kamuya ait verileri etkin bir şekilde paylaşılması bu paylaşımdan kamunun ve ülkenin fayda sağlaması için yasal düzenlemeler ve paylaşım standartları oluşturmaktadır. Türkiye'de bilişim sistemlerinin yaygın kullanılmaya başlaması ile birlikte bu ihtiyaç artmıştır. Bu ihtiyacı karşılamak için kurumlar kendi yönetmeliklerini çıkarmakta ileri doğru kapsamlı düzenlemeler ve standartların ortaya konulması beklenmektedir.

ABD, kamu sektörü bilgisinin paylaşılması ve tekrar kullanılması yoluyla değer üretiminin öncüsü olarak kabul edilmektedir. Uygulanan açık erişim politikası ve vergi sisteminin sağlıklı işlemesi ile ABD'de kamu sektörü bilgisinin kullanımından büyük fayda sağlamaktadır. Kamu sektörü bilgisini kullanarak katma değer üreten şirketlerin elde ettikleri gelirlerinden dolayı devlete ödedikleri vergiler kamunun bu bilgileri satması durumunda elde edeceği gelirden fazladır. Kamu sektörü bilgisini katma değerli ürüne dönüştüren özel sektör, devlete daha fazla vergi vermekte, istihdamda artışa neden olmakta, dolayısıyla gelirler artarken istihdama, ulusal ve küresel ölçekte rekabet edebilirliğe ve kalkınmaya katkı sağlanmaktadır [1].

Avrupa Birliği üyesi ülkeler arasında topluma ait açık bilginin paylaşımı için 2003/98/AT sayılı Direktifi oluşturulmuştur. 2008 yılına kadar AB ülkelerinin bazıları, kanun şeklinde yeni düzenlemeler bazıları da mevcut kanunlarda tadilat yaparak direktife uyum sağlamışlardır. 26 Haziran 2013 2003/98/AT tarihinde doküman yeniden güncellenmiştir [17]. Avrupa Birliği'nin siber güvenlik programlarından sorumlu olan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) da birbirine bağlı ağların güvenliği konusunda çalışmalar yürütmektedir[18].

NATO organizasyon yapısı gereği gizlilik bilgiyi birçok seviyede işlemesi ve başka ülke ve kurumlarla paylaşması gerekmektedir. Bunu için de uzun yıllardır veri haberleşmesi için teknik ve yönetsel çözümler geliştirmeye çalışmaktadır. Hali hazırda gizli ve hizmete özel verilerin paylaşılması için çözümler geliştirmektedir [7, 16].

III. TEKNOLOJİLER VE ÜRÜNLER

İncelenen bilimsel dokümanlar, IEG ürünleri hakkında internetten elde edilen bilgiler ve üreticilerden alınan ürün ve kullanıcı kılavuzlarından edinilen bilgiler doğrultusunda ağlar arası bilgi akışı cihazlarının diyet çözümleri, air gap çözümleri ve akış kontrolü çözümleri olarak sınıflandırılabilceği tespit edilmiştir.

Akış kontrolü çözümleri, literatürde bilinen adıyla Guard, farklı ağlardaki sistemleri haberleşmesini sağlarken içerik analizi yapabilen, uygulama katmanında trafiği yönlendirebilen cihaz veya sistemlerdir. Klasik güvenlik duvarlarına ve yönlendiricilere benzetmekle beraber, uygulama katmanında trafiğin içeriğini kontrol ederek etiket, sınıflandırma veya zararlı yazılım kontrolü de yapabilmektedirler. Akış kontrol sistemleri sadece üzerinde uygulanan kural ve politikalara uygun olan trafiğin geçmesine izin vererek yüksek güvenlik derecesine sahip ağları korumaktadır. Bu güvenlik kuralları veya politikaları, zararlı yazılım analizi, etiket kontrolü, yetki kontrolü, dosya tipi kontrolü, sayısal imza kontrolü gibi derinlemesine paket analizlerini içermektedir.

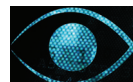
Diyot (Diode), iki ağ arasında donanımsal olarak ters yönde veri akışını engelleyerek, tek yönlü bir bağlantı sağlayan çözümlerdir. Bu çözümler sayesinde güvenli bir ağın, genel amaçlı bir iç ağdan ters yönde veri akışı riski olmayacak şekilde veri çekebilmesi mümkündür. Böylece kullanıcıların güvenli olmayan kaynaklardan güvenli ağa veri transferine izin verilmektedir. Veri kaynağı tarafındaki kullanıcılar bilgiyi dış diyet sunucusuna gönderir. Daha sonra veri diyottan geçerek iç diyet sunucusuna ulaşır.

Diyot cihazı öncesinde, dışarıdan gelen bilginin kaydedilmesi ve sonra diyet üzerinden içeriye gönderilmesi amacıyla ara sunucular kullanılıyorsa, uçlar arasındaki iletişim gecikmeli çevrimiçi şekilde gerçekleşir.

Air Gap (hava boşluğu), güvenli bir bilgisayar ağının fiziksel, elektriksel ve elektromanyetik açıdan diğer güvenli/güvensiz ağlardan izole edilmiş olmasına dayanan bir güvenlik kavramıdır. Normal koşullarda bir bilgisayar ağı ile diğer dış ortamlar arasında hava boşluğundan bahsedilebilmesi için, bu ağa bilgi aktarımının sadece harici bilgi taşıma ortamlarıyla (disket, USB disk vb.) gerçekleştirilebileceği garanti edilmelidir.

IV. AĞ BAĞLANTILARI İÇİN GENEL GEREKSİNİMLER

Literatür incelendiğinde doğrudan farklı güvenli seviyesinde ağların bağlanmasına yönelik bütüncül bakış açısına sahip



FARKLI GÜVENLİK SEVİYESİNDEKİ AĞLARIN BAĞLANMASI İÇİN BÜTÜNCÜL BİR MODEL

model bulunmuyor. Literatür taramasında da görüldüğü gibi genellikle bu bağlantının özel alanlarına (Bilgi değişim Geçitleri, İçerik Kontrolü, vb.) odaklanmış çözümler bulunmaktadır. Bu makalede farklı güvenlik seviyesine sahip ağların bağlanmasında teknik ve yönetsel tüm konuları ele alan bir model sunulmaktadır. Bu modelin gerektirdiği temel konular bu bölüm altında ele alınmıştır.

A. Ağ Bağlantılarına Yönelik Zafiyetler, Tehditler ve Riskler

Ağ bağlantılarına yönelik zafiyetler, tehditler ve riskler bu bölümde ele alınmasının nedeni modeli uygulayacak sistem yöneticilerinin bu konuda bilgilendirilmelerini sağlamaktır. Ağlar arasında bağlantıya özel sistem riskleri bu bağlantı için tanımlanan tehditlerin gerçekleşme olasılığına bağlı olarak belirlenmelidir. Tehditlerin gerçekleşme olasılıkları, tehdit ortamı, mevcut güvenlik önlemleri, bağlantı modeli, bağlantı ihtiyacı vb. etkenlere bağlı olarak değişecektir. Tehdit altında olan sistem bileşenlerinin/verilerinin değeri de kurumdan kuruma değişmektedir. Risk değerlendirmesi çalışması, her bağlantı senaryosu için planlama safhasında yapılmalıdır. Güvenlik tedbirleri, sadece burada tanımlanan tehditlerden kaynaklanacak risklerin değil, ağlar arası bağlantı öncesinde gerçekleştirilecek olan risk değerlendirme çalışması sonucunda sistemin tümü için belirlenen risklerin en aza indirgenmesini hedeflemelidir.

B. Ağ Gizlilik Seviyeleri ve Güvenlik Önlemleri

Ağlar arasında paylaşılacak bilginin gizlilik, bütünlük ve erişilebilirlik ihtiyaçlarının bilgi paylaşan kurumlar adına güvence altına alınması amacıyla göz önünde bulundurulması gereken teknik ve yönetsel güvenlik önlemleri mevcuttur.

Ağların bütüncül bakış açısı ile güvenliğinin sağlanabilmesi için aşağıdaki güvenlik önlemlerinin alınması gerekmektedir.

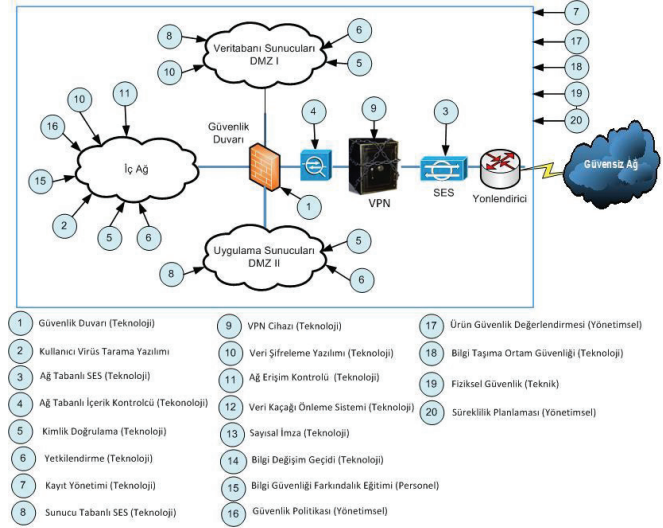
- Güvenlik Duvarı
- Zararlı Yazılıma Karşı Koruma
- Saldırı Tespiti ve Önleme
- İçerik Kontrolcüsü
- Yönlendirici
- VPN
- Kimlik Doğrulama
- Erişim Kontrolü
- İnkâr Edememe
- Güvenlik Sıkılaştırmaları
- Denetleme Kayıtları
- Bilgi Değişim Geçidi
- Farkındalık ve Eğitim
- Fiziksel ve Çevresel Güvenlik
- Güvenlik Değerlendirmesi
- Konfigürasyon Yönetimi
- Süreklilik Planlaması
- Acil Durum Müdahale

- Bakım
- Bilgi Taşıma Ortamlarının Korunması
- Personel Güvenliği

Temel olarak gizliliği belirleyen kıstas o ağda bulunan bilginin niteliğidir. Ağda saklanan işlenen, iletilen verinin gizliliği ağın gizliliğini doğrudan etkilemektedir. Bu yüzden farklı güvenlik seviyesindeki ağlarda bulunması gereken güvenlik önlemleri de farklıdır. Farklı güvenlik seviyesindeki ağları birbirine bağlamak isteyen kurumlar risk analizi yaparak her bir güvenlik seviyesi için alınması gereken teknik ve yönetsel güvenlik önlemlerini belirlemeli bu güvenlik önlemlerini içeren topolojiler oluşturmalıdır.

Askeri ve kamu kurumlarında bilgi Tasnif Dışı, Hizmete özel, Özel, Gizli ve çok Gizli olmak üzere 5 sınıfta ele alınmaktadır [19].

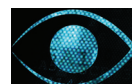
Şekil 1’de Hizmete Özel bir ağın topolojisi ve ağda alınması gereken önlemler bulunmaktadır.



Şekil 1 Hizmete Özel ağın topolojisi

Ağlar arası bağlantı yapacak sistem yöneticilerinin güvenlik önlemlerini kolay ve etkin bir şekilde anlayıp uygulayabilmeleri amacıyla tekelle ve donanım/yazılım tabanlı (Güvenlik Duvarı, Saldırı engelleme Sistemi vb) bir gösterim yapılmaya çalışılmıştır. İşletim sistemi gibi birçok güvenlik unsurunu bünyesinde barındırması gereken varlıklar için kimlik doğrulama, yetkilendirme, olay kaydı izleme gibi kavramlar da kullanılmıştır. Bu kavramların ağın gizlilik seviyesine göre varlıklarda da bulunup bulunamayacağı ağ mimarilerinde belirtilmiştir. Ağda güvenliğin sağlanabilmesi için teknik önlemler yanında yönetsel önlemlerin de alınması gerekmektedir. Ağlarda alınacak yönetsel önlemler de ayrıca belirtilmiştir.

Bilgi sistemlerinde kademeli güvenlik (Defense in Depth), bilgi güvenliğinin sağlanması amacıyla farklı kademelerde birbirini tamamlayıcı güvenlik önlemlerinin alınmasıdır.



FARKLI GÜVENLİK SEVİYESİNDEKİ AĞLARIN BAĞLANMASI İÇİN BÜTÜNCÜL BİR MODEL

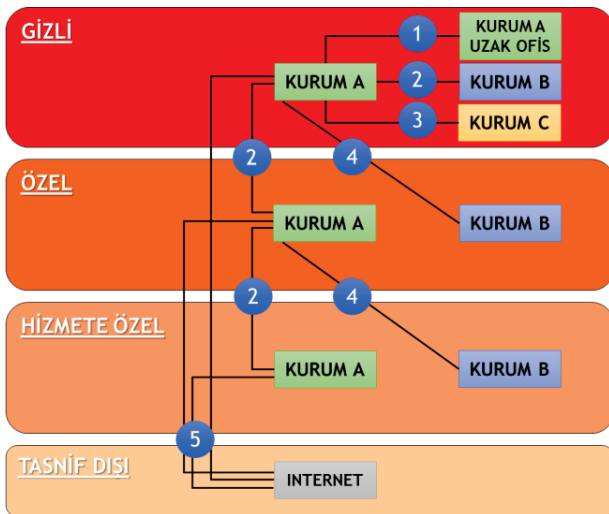
Sistem yaşam döngüsü içerisinde personel, teknoloji ve işletme açısından güvenlik önlemleri alınmalıdır. Farkı gizlilik seviyesindeki ağlar için belirlenen güvenlik önlemleri kademeli güvenlik bakış açısı ile oluşturulmalıdır.

C. Ağlar Arası Bilgi Akışı

Ağlar arası bağlantının güvenli şekilde temini için gizli kanalın varlığı, bilgi sızması, ağ atakları, ağın izlenmesi ve güvenlik etiketlerinin değiştirilmesi gibi güvenlik tehditlerine karşı teknik koruma sağlanması, gerekli politika ve direktiflerin oluşturulması ve uygulanması önemlidir.

Farklı güvenlik seviyelerine sahip ağların bağlantısında yüksek seviyede olan ağın güvenlik gereksinimlerini karşılayacak şekilde yapılandırma gereklidir. Bunun yanında ağların bir birine bağlanmasını sağlayan bilgi değişim geçidi (IEG) büyük önem taşımaktadır.

Şekil 2’de bağlanacakları ağların güvenlik sınıflandırmaları yanında ağların güvenlik ilkelerini, sahiplerini ve yöneticilerini de dikkate alan beş farklı senaryo belirtilmiştir.



Şekil 2 Farklı güvenlik seviyesindeki ağlar arası iletişim senaryoları

Senaryo 1: Aynı güvenlik sınıflandırma seviyesinde ve aynı KURUM etki alanında fakat farklı otoriteler tarafından yönetilen iki etki alanının birbirine bağlanmasını göstermektedir. Örnek olarak aynı kurumun merkez ve uzak ofisinin bağlantısı verilebilir.

Senaryo 2: Aynı güvenlik sınıflandırma seviyesinde fakat farklı güvenlik ilkelerine sahip iki etki alanının birbirine bağlanmasını göstermektedir. Aynı güvenlik seviyelerini kabul eden iki kamu kurumunun bağlantısı buna örnek olarak verilmektedir. Bu senaryonun diğer bir durumu da aynı kurumun farklı güvenlik sınıflandırma seviyesindeki ağlarının bağlanmasıdır.

Senaryo 3: Aynı güvenlik seviyesindeki kamu kurumu ve özel bir kurumun etki alanlarının kurduğu bağlantıyı göstermektedir.

Senaryo 4: Aynı güvenlik sınıflandırma sistemini kabul eden iki farklı kurumun iki farklı seviyedeki ağının bağlantısını ifade eder.

Senaryo 5: Kurum ağının Internet'e veya diğer tasnif dışı sistemlere bağlantısını göstermektedir. Burada farklı seviyelerden tasnif dışına bağlantı söz konusu olduğundan her durum ayrı olarak ele alınmalıdır.

Bu noktada genel olarak daha fazla ihtiyaç duyulduğu belirlenen Senaryo 4 üzerinden sistemin nasıl olması gerektiği yönünde öneriler yer alacaktır.

Yüksek güvenli li etki alanının b t nl k ve kullanılabilirli i, d   k güvenli li etki alanından sadece beyaz listeye alınmı  mesaj formatına sahip mesajlarının ge mesine izin verilerek sa lanabilir. Bilgi akı  sistemi vir  /zararlı yazılım taraması gibi i erik taramalarını dı  g venlik bile enlerine bırakabilir. Bilgilerin gizlili i ise sadece izin verilen etikete sahip mesajların ge mesine izin verilerek sa lanır.

D. Paylaşılacak Bilgiler ve Müşterek Sınıflandırma

Genel gereksinimler açısından ilk dikkate alınacak husus kurumlar arasında paylaşılacak verilerin belirlenmesidir. Kullanım durumlarına bağlı olarak bilgi paylaşım amacı da ortaya konulmalıdır. Paylaşılacak bilgiler kategorize edilerek listelenmelidir. Sistemlerin gizlilik seviyelerinin müşterek kriterler üzerinden tespiti, alınması gereken önlemlerin standartlaşması açısından önemlidir. Bu şekilde kurumdan kuruma değişen gizlilik seviyesi kriterleri için ortak bir nokta belirlenebilmektedir.

Birçok durumda bilgi otomatik olarak toplanmakta ve belirli durumlarda paylaşılmaktadır. Bu işlemlerin manuel olarak gerçekleştirildiği durumlar da mevzu bahistir. Dolayısıyla verinin hangi durumda ne şekilde toplandığı net şekilde ifade edilmelidir.

E. Risk Analizi

Veri paylaşımının sınırsız bir şekilde yapılmasının önündeki en büyük engel veriye ve sistemlere yönelik risklerdir. Her bir bağlantı kuruluşu kendine özel şartlar altında değerlendirilmeli ve süreç buna göre işletilmelidir. Genel tek bir bağlantı çözümünün bütün durumlar için yeterli olacağı varsayımında bulunmak doğru değildir.

F. Ortak Prosedürler

Bilgi değişimini yöneten kurallar tanımlanmalıdır. Ne zaman ve nasıl paylaşım yapılacağı, bilginin iletim esnasında nasıl korunacağı ve işleneceği belirlenmelidir. Bu şekilde uçlar arasında güven (trust) ilişkisi kurulmalıdır. Bunun için ikili veya çoklu anlaşmalar imzalanmalıdır. Eğer mevcutsa ulusal



FARKLI GÜVENLİK SEVİYESİNDEKİ AĞLARIN BAĞLANMASI İÇİN BÜTÜNCÜL BİR MODEL

bilgi güvenliği makamından görüş talep edilmeli veya yeterli olgunlukta ise bilgi paylaşımı kapsamında kurumlar arası ilişkileri düzenleyen mevzuata başvurulmalıdır. Ayrıca iletişim gereksinimi durumunda bağlantı kurulacak noktaların belirlenmesi gerekmektedir.

G. Standart ve Formatlar

Sürekli veri paylaşım ilişkisinin ve birlikte çalışabilirliğin devam etmesi için veri formatı ve ortak standartlar üzerinde fikir birliği olmalıdır. Uyumsuz standartlar gelecek için verimli paylaşım hususunda sıkıntı oluşturacağı için mümkünse uluslararası veri standartları kullanılmalı değilse iki kurumun anlaştığı veri formatı oluşturulmalıdır. Bu veri formatının uygulama seviyesinde içerik kontrolünün yapılabilmesi önemlidir. Örneğin Bilgisayar Olaylarına Müdahale Ekipleri arasında bilgi paylaşımına yönelik Incident Object Description Exchange Format (IODEF) formatı bu konuda örnek olarak verilebilir.

H. Paylaşım Altyapıları/Sistemleri

Özellikle tasarım aşamasından başlanarak paylaşımın yapılacağı altyapının ve sistemin nasıl olması gerektiği analiz edilmelidir. Bu paylaşımlara için geliştirilmiş sistemler varsa onlar tercih edilmeli yoksa risk analiz sonucunda teknik riskleri minimize edecek bir çözüm geliştirilmelidir. Böyle bir yapıya NATO bünyesinde zararlı yazılım bilgilerini paylaşarak korelasyon kuran ve üye ülkeleri bilgilendiren MISP paylaşım altyapısı örnek olarak verilebilir.

1) İletim Protokolleri

Grafiksel kullanıcı arayüzü bulunabileceği gibi aynı işlevler ve isteğe bağlı geliştirmeler, uygulamanın sunduğu API (Application Programme Interface) vasıtasıyla da gerçekleştirilebilir.

Bütünlük ve gizliliğin temini, bilginin iletiminde zorunluluk olduğu için hangi taşıma protokolünün kullanılması gerektiği belirlenmelidir. İletim protokolü seçimine göre Paylaşım Altyapıları/Sistemleri başlığında belirtilen sistemin özellikleri tanımlanırken iletim protokolleri de göz önüne alınmalıdır. Burada söz konusu protokoller HTTP, XMPP veya SMTP olabilir.

2) Ortak Ağlar

Verinin hangi tipteki ağlar üzerinde (tasnif dışı, hizmete özel, gizli, internet, kiralık hat vb.) iletildiği analiz edilmelidir. İnternet veya kurum gizli ağı kullanılmakla birlikte her bir kullanım durumu için hangi ağın kullanılacağı tanımlanmalıdır. Söz konusu ağ İnternet olabileceği gibi sadece gizli haberleşmelerin yapılacağı gizli ağ da olabilir.

3) Bağlantı Sistemlerinin Güvenlik Test Politikaları

Bilgi sistemlerinin güvenlik testlerinin nasıl ve hangi aralıklarla yapılacağı tanımlanmalıdır. Örneğin ağlar arası bağlantı amacıyla kullanılan sunucular ve ağ içerisinde ilişki kurdukları diğer bütün sunucu, aktif ağ cihazları ve

uygulamalar için güvenlik testleri planlanmalı ve plana uygun şekilde periyodik olarak gerçekleştirilmelidir. Testler uygulama, uygulama platformu, işletim sistemi ve ağ olmak üzere dört seviyede gerçekleştirilebilir.

4) Bağlantı Sistemi Akreditasyonu

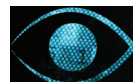
Bu doküman göz önünde bulundurularak iki kurumun uzmanlarının ortak kuracağı bir komisyon veya üçüncü bir tarafça sistemin istenilen gereksinimleri karşıladığının tespit edilerek akredite edilmesi gerekmektedir.

V. SONUÇ VE ÖNERİLER

Bilgilerin sayısal ortama taşınmış olması, kurumların ve ülkelerin kendi bilgilerine hızlı erişimi sağlaması yanında diğer kurumlarla ya da ülkelerle güvenli bir biçimde paylaşılması ihtiyacını doğurmaktadır. Özellikle gizli gizlilik dereceli bilgilerin paylaşılması için uzun yıllardır çalışmalar sürdürülmesine karşın somut uygulanabilir teknolojik ve yönetsel araçlar bulunmamaktadır. Çoğunlukla özel durumlar için özel çözümler önerilmektedir. Fiziksel güvenlik için Air-Gap, Diyet gibi teknolojiler, içerik kontrolü için de akış kontrol sistemleri uygulanmaktadır. Bu teknolojik çözümler yanında güvenli veri paylaşımının sağlanması için risk analizi, ortak prosedürler, standart formatlar, ikili anlaşmalar, paylaşım alt yapıları, iletişim protokolleri gibi hususların göz önüne alınacağı bir bütüncül bir model oluşturulmuştur. Bu modelin kurumlara uygulanmasında o kurumlara özgü verilerin çıkarılması, verilerin standart hale getirilmesi içeriğinin kontrol edilmesi önem arz etmektedir. Sonraki çalışmalarda bu model veri paylaşmak isteyen değişik kurum verilerine uygulanabilir.

KAYNAKLAR

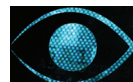
- [1] D. Civelek, Ö. Aşık, "Kamu Sektörü Bilgisinin Paylaşımı ve Yeniden Kullanımı", DPT Çalışma Raporu, Şubat 2011
- [2] Nexor, *IEG Reference Architecture*, 2013 [Online], Available: <http://www.nexor.com/white-papers/nato-ieg-reference-architecture>
- [3] D. Boonstra, H.A. Schotanus, C.A.A. Verkoelen, A.C.M. Smulders; "A Methodology for the Structured Security Analysis of Interconnections" The 2011 Military Communications Conference
- [4] A. J. Blažič, S. Šaljić; "Security and Confidentiality in Interconnected Networks" *ICDS 2011: The Fifth International Conference on Digital Society*
- [5] T. Grance, J. Hash, S. Peck, "Security Guide for Interconnecting Information Technology Systems", NIST; 2002
- [6] Sander Oudkerk, Ian Bryant, Anders Eggen, Raymond Haakseth, "A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects", NATO RTO-MP-IST-091; 2009
- [7] K. Wrona, S. Oudkerk, G. Hallingstad; "Designing Medium Assurance XML-Labeling Guards for NATO" NATO Consultation, Command&Control Agency
- [8] L. Apiecionek, M. Romantowski, J. Sliwa "Safe Exchange of Information for Civil-Military Operations" Military Communication Institute, Poland; 2011
- [9] O. Serrano, P. Lagadec, L. Dandurand, F. Jordan, "CIS Security Information Sharing Challenges"; NATO NCIA, 2013
- [10] Ezenia Inc, "The Future Evolution of Multi-Level Security for the Federal Government", Ezenia Inc.; 2007



FARKLI GÜVENLİK SEVİYESİNDEKİ AĞLARIN BAĞLANMASI İÇİN BÜTÜNCÜL BİR MODEL

- [11] T. Dean, G. Wyatt, "Information Exchange Between Resilient and High-Threat Networks: Techniques for Threat Mitigation", QinetiQ; 2004
- [12] J. R. James, F. Mabry, "Seeing the Real World: Sharing Protected Data In Real Time", 45th Hawaii International Conference on System Sciences; 2012
- [13] Multilevel Security Services European Defence Agency; Asseco Poland; 2011
- [14] D. Harris, L. Khan, R. Paul, Bhavani Thuraisingham, "Standards for secure data sharing across organizations", Computer Standards & Interfaces archive, Volume 29 Issue 1, January, 2007
- [15] B. Chen, B. Jin, X. Zou; "The Security Protection and Control Systems of Network Boundary"; The 3rd Research Institute of Ministry of Public Security, China; 2009
- [16] NATO, "Information Assurance Technical and Implementation Directive for the Interconnection of CIS", 2008
- [17] European Union, "Directive 2003/98/EC on the re-use of public sector information", 2013, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:175:0001:0008:EN:PDF>
- [18] Online Available: <http://www.nexor.com/data-diodes>
- [19] SSM, "Gizlilik Derecelendirme Kılavuzu" Hazırlama Rehberi, 2007, [Online], Available, <http://www.ssm.gov.tr/anasayfa/kurumsal/Documents/GizlilikDerecelendirmeKilavuzu.pdf>

M. Kara, 1993 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümünden mezun oldu. 1996 yılında Yüksek Lisansını, 2002 yılında da Doktorasını Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Anabilim dalında tamamladı. Doktora tezini Bilgisayar Ağlarında Çok Yollu Yönlendirme konusunda yaptı. 1994-2000 yılları arasında Kocaeli Üniversitesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak, 2000-2001 yıllarında Armada Bilgisayar AŞ'de Sistem Mühendisi olarak çalıştı. 2001'den beri TÜBİTAK BİLGEM'de çalışmaktadır. Bulanık mantık, siber güvenlik, ağ ve sistem, protokol güvenlik analizi, kritik altyapı güvenliği, güvenli yazılım geliştirme, Ortak Kriterler, sistem, yazılım/donanım güvenlik testleri konularında çalışmaktadır. Ulusal ve uluslararası dergi ve konferanslarda yayınları bulunmaktadır.



JavaScript Kütüphanelerinin Güvenilir Olmayan Verilere Karşı Hazır Olma Durumlarının Bayesian Ağları ile Ölçülmesi

E. Ufuktepe, T. Tuğlular

Özet—Yazılımın güvenilir olmayan verilere karşı hazır olma durumunun ölçülmesi zordur ve bu alanda çalışmalar halen devam etmektedir. Bunun nedeni yazılım geliştirme ve tasarlama aşamasında geliştiricilerin girdileri doğrulamada başarısız olmasıdır. Bu bildiride, bir yazılımın güvenilir olmayan verilere karşı hazır olma durumunun ölçülmesinde Bayesian Ağlarını kullanan bir yöntem sunulmaktadır. Önerilen yöntemde, seçilen yazılıma ait fonksiyonlar veya metotlar üzerinde çalışılmaktadır. Seçilen fonksiyonların girdi doğrulama bilgileri kullanılmaktadır. Böylece, Bayesian Ağları ile yazılımın güvenilir olmayan verilere karşı hazır olma durumunun ölçümü sağlanmaktadır. Örnek çalışmada, değerlendirme için artan popüleritesinden dolayı JavaScript dilinde geliştirilmiş ve tanınmış olan bir yazılım kütüphanesi olan JQuery seçilmiştir. Önerilen yöntem ile yazılım geliştirme takımları, geliştirdikleri yazılımın güvenilir olmayan verilere karşı önlem almayı izleyebilir.

Index Terms—Yazılım Güvenliği, Girdi Zafiyetleri, Bayesian Ağları, Hazırlığının Ölçümü

I. GİRİŞ

GİRDİ zafiyetleri, Open Web Application Security Project (OWASP)[1] ve National Vulnerability Database (NVD) [2] tarafından en tehlikeli ve sık karşılaşılan zafiyetlerden biri olarak tanımlanmıştır. Geliştirici tasarım, kodlama ve girdi zafiyetlerini doğrulamasında test yetersiz kaldığında, yazılım geliştirme yaşam döngüsü içerisinde tasarım ve geliştirme aşamalarında gerçekleşmektedir. Bu bildiride, ele alınan bir yazılımın güvenilir olmayan verilere karşı hazır olma durumunun ölçülmesine yönelik bir yöntem sunulmuştur. Yöntem, ele alınan yazılımdaki hazır olma durumunun ölçülmesinde girdi olarak kabul ettiği her fonksiyonun parametrelerinin sebep ve sonuç ilişkilerini dikkate alarak Bayesian Ağlarını (BA) kullanmaktadır. Wagner'ın[3] yazılım kalite tahmini ve değerlendirmesinde kullanılan etkinliğe dayalı kalite modeli takip edilerek BA oluşturulmuştur.

OWASP 2013 yılında ilk on zafiyeti tanımlamıştır [1]. Birçok girdi zafiyeti ilk on içerisinde yer almıştır. Bu çalışmada girdi zafiyetleri hedef alınmış ve XSS, SQL Injection, OS Command Injection, Input Validation, Code Injection ve Path Traversal zafiyetleri seçilmiştir. Christey [4] yazılım zafiyetlerini ağaç yapısı ile sınıflandırmıştır. Bu

çalışmada benzer bir yöntem kullanılarak, girdi doğrulama zafiyetlerinin karar ağacını oluşturulmuştur.

Tablo I'de görüldüğü gibi Ocak 2000'de Ocak 2014'e kadar NVD [2] üzerinden rapor edilmiş girdi doğrulama zafiyetlerin verileri toplanmıştır. Böylece bu değerleri ileride oluşturulacak Bayesian Ağında ağırlık olarak verilecektir.

Bildiride 2. Bölüm'de benzer çalışmaların özetleri verilmiştir. 3. Bölüm'de yazılımın güvenilir olmayan verilere karşı hazır olma durumunun ölçülmesi için önerilen Bayesian Ağının oluşturulma yöntemi açıklanmıştır. 4. Bölüm'de ise örnek olayın incelenmesi sunulmuş ve sonuçlar 5. Bölüm'de açıklanmıştır.

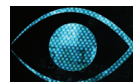
Tablo I. Ocak 2000'den Ocak 2014'e kadar rapor edilmiş girdi zafiyetlerinin dağılımı (Kaynak: NVD[2])

Girdi Doğrulama Zafiyetleri	Toplam Rapor Edilmiş Zafiyetler	Yüzde
XSS	4584	32%
SQL Injection	3652	25%
Input Validation	2665	19%
Code Injection	1818	13%
Path Traversal	1511	10%
OS Command Injection	108	1%
TOTAL	14338	100%

II. İLGİLİ ÇALIŞMALAR

Frigault ve Wang [5] bir saldırı çizgesinde kodlanmış zafiyetler arasındaki nedensel ilişkileri araştırmıştır. Ancak, zafiyet ve ağların gelişen doğası gereği büyük ölçüde göz ardı edilmiştir. İstisna edilmiş kodları veya yamaların geçerliliği gibi zamansal faktörleri birleştirmek için bir Dinamik Bayesian Ağ tabanlı model önermişlerdir. Modelden başlayarak, potansiyel uygulamaları göstermek için iki somut olgu üzerinde çalışmışlardır. Bu yeni model sürekli dinamik bir ortamda ağ güvenliğini ölçmek için teorik bir temel ve pratik bir yapı oluşturmuşlardır.

Kondakçı [6] Bayesian Ağlarını kullanarak bir ağ güvenliği risk değerlendirme modeli önermiştir. Çeşitli Bilgi Teknolojileri (BT) varlıklarını ve güvenilir hesaplamalı ortamlarda risk hesaplamalarının uygulanılabileceği genel bir tehdit modeli ortaya atmıştır. Bilgi güvenliği tehditlerini (insan-ilişkili, iç ve dış) sınıflandırarak dört güvenilir parametre ile birleşik bir yapı oluşturup modellemiştir. Ayrıca



hangi risk düzeylerini kolayca tahmin ve farklı değerlendirme sistemler için puan ortalaması düzeni ve koşullu olasılık metotlarını kullanarak yeni bir risk yayılım modeli geliştirmiştir. Öte yandan Bayesian Ağların bilgiyi ifade ediş şekli ile otomatik olarak akıl yürütme yapısından dolayı çalışmasında kullandığını, BT ortamlarının dinamik ve değişen yapısı gereği geleneksel yorumlama metotların sonraki risk faktörleri dağılımında uygulanmasının daha güç olduğunu belirtmiştir. Bu nedenle birbirine bağımlı analizlerde Bayesian yaklaşımının geniş ölçekli ağlarda uygulanabilirliğini kolay olduğunu ifade etmiştir.

Wagner [3] faaliyet temelli kalite modelleri üzerinden yazılım değerlendirmesi ve kalite tahmininde Bayesian Ağlarını kullanmıştır. Bayesian Ağını oluştururken üç tip düğüm tanımlamıştır ve dört temel adımda belirtmiştir. İlk adımda ilgili faaliyetlerin ve göstergelerin hedef tabanlı türetilmesidir. İkinci adımda faktörlerin ve alt faaliyetlerin belirlenmesidir. Üçüncü adımda faktörler için uygun göstergeler içerilmiştir. Dördüncü adımda düğüm olasılık tabloları tanımlanıp kantitatif ilişkiler gösterilmiştir. Düğümler yazılımın “Durumlar ve Faaliyetler” haritasına göre oluşturulmuştur. “Faaliyetler” sistem üzerinde etkisinin bilgilerinin tutar. Örneğin; bakım ve kullanım yüksek dereceli birer faaliyettir. “Durumlar” ise bir sistemin ortamı ve geliştirme organizasyonunu içermektedir. Faaliyet üzerinde pozitif ya da negatif etkisi olan her durum için faktörlere bir düğüm eklenir. Eğer durumun faaliyet üzerinde hiçbir etkisi yoksa düğüm eklenmez. Ancak unutmamalıyız ki faaliyet üzerinde etkisi olan her alt faaliyet ve faktör için faaliyet düğümü eklenmelidir.

Guarnieri ve Livshits [7] statik analizin program optimizasyonundan hata tespit etmeye kadar kadar kullanışlı bir teknik olduğunu dile getirmiştir. Bu çalışmaları JavaScript programlarındaki akış aşamalı statik analizi incelemişlerdir. Çalışmalarında hızdan dolayı çevirim içi ve çevirim dışı statik analizlerini birleştirerek kullanımını savunmuşlardır. Çevirim dışı kullanımı sunucunun ötesinde bir zamanda kullanılabilir, oysaki çevirim içi analizi web tarayıcısına entegre edilebilir olduğunu düşünmüşlerdir. Gerçek hayattan ve sentetik JavaScript kodu üzerinden gerçekleştirilen geniş kapsamlı deneylerden sonra, koddaki güncellemelerin az olduğu yerlerde kullanımı daha normal görmüşlerdir. Güncel statik analiz sonuçlarının her gün kullanımı için tarayıcıda kullanımını hızını kabul edilebilir olarak görmüşlerdir. Bu formdaki aşamalı statik analizi yaklaşımının birçok alanda, özellikle mobil cihazlarda avantajlı olduğunu iddia etmişlerdir.

Jensen ve arkadaşları [8] TAJIS adında geliştirdikleri statik analiz aracı ile JavaScript dilinde veri tipi analizini gerçekleştirmiştir. Tip analizini “Değer” örgüsü üzerinden ve transfer fonksiyonların veri akışı analizi ve akış çizgeleri üzerinden gerçekleştirmişlerdir. Örneğin; eğer bir fonksiyon “toString()” fonksiyonu ile çağırılıyorsa, veri tipini “String” olarak yorumlanmıştır. Bu çalışmalarında, tip analizcilerinin JavaScript için ilk ses bazlı ve detaylandırılmış araç olduğunu ifade etmişlerdir. Monoton yapının ayrıntılı örgü yapısı ile

kullanımı yeni soyutlama ile birleştirildiğinde istenilen ölçütte analiz sonuçların hassasiyetini iyileştirdiğini gözlemlemişlerdir.

III. GÜVENİLİR OLMAYAN VERİLERE KARŞI HAZIRLIĞININ ÖLÇÜLMESİ İÇİN BAYESİAN AĞININ OLUŞTURULMASI

Çalışmamızın temelinden Bayesian Ağlarının kullanılma nedeni, BA’ların belirsizliklerin açıklanmasında tutarlı anlamlar sunması ve çeşitli etkileşimlerin sebep ve sonuç ilişkilerine dayalı sezgisel çizgelerle ifade edilebilmesidir [9].

İlk adımda faaliyetler tanımlanmıştır. Faaliyetler tanımlanmış olduğumuz altı girdi doğrulama zafiyetine karşılık gelmektedir; XSS, SQL Injection, OS Command Injection, Input Validation, Code Injection ve Path Traversal. Daha sonra tanımlanmış faaliyetlere ilişkin faktörler tanımlanmıştır. Bu durumda Bayesian Ağında bu çalışma kapsamında tanımlanan faktörler, ele alınan yazılımda tespit etmiş olduğumuz zedelenilebilir fonksiyonlara karşılık gelmektedir. Son adımda indikatörler tanımlanmıştır. Özel olarak ölçmek istenilen faaliyet veya faktörden ek bir düğüm çıkartılarak indikatörler tanımlanır. Wagner [3] indikatörlerin Bayesian Ağlarında yerini şöyle tanımlar, “faaliyet veya faktörlerden indikatöre bir ayırıt ile tanımlanır. İndikatörler faaliyetler ve faktörlere bağlıdır. İndikatörler sadece altta yatan anlatımların ifade ediliş şeklidir”.

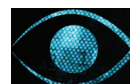
Bayesian Ağını oluştururken, düğümler arasındaki ilişkiler gösterilmiştir (bknz Şekil 3. Her öncel düğüm takipçi düğümün Olasılıksal Düğüm Tablosunu (ODT) etkiler. BA’da toplamda oluşacak ODT sayısı BA’da bulunan düğüm sayısı kadar olacaktır. Toplamda bulunacak ODT sayısı formülü:

$$1 + (\text{zafiyet_sayısı}) + (\text{fonksiyon_sayısı}) = (\text{toplam_ODT'ler})(1)$$

Formül 1’deki (1) 1 değeri “Uygulama düğümüne” karşılık gelmektedir. Çalışmada 6 girdi doğrulama zafiyeti tanımlandığından zafiyet sayısı 6 olacaktır. Fonksiyon sayısı ise yazılımdan seçilen fonksiyonların sayısına denk gelmektedir. Yazılımda bulunan fonksiyonlar fazla olacağından, seçilen fonksiyonlar sık kullanılan ve yazılımda yayılmış olan fonksiyonlar tercih edilmiştir. ODT’leri üç kategoride incelenmiştir; Uygulama ODT, (girdi doğrulama) Zafiyet ODT ve Fonksiyon ODT’leri. Şekil 3’de görüldüğü gibi, en üstteki tek düğüm uygulama düğümü olup Uygulama ODT’si içermektedir, altı zafiyet düğümlerinin bulunduğu ikinci katmanda Zafiyet ODT’lerini ve fonksiyon düğümlerinin bulunduğu üçüncü katmanda Fonksiyon ODT’lerini içermektedir.

A. Uygulama Düğümünün ODT Hesaplaması

Her zafiyetin uygulama üzerinde farklı etkisi olmaktadır. OWASP [1] üzerinde zafiyetlerin risk sıralaması Bölüm 1’de gösterilmiştir. Ancak risk bilgileri sadece sıralama olarak verilmiştir (bknz. Tablo II). Zafiyetlerin risk yüzdelerini elde etmek için sıralamalarına ilişkili olarak ağırlık atanarak “Ağırlıklı Yüzde Formül”ünü/Weighted Percentile Formula”(2) uygulanarak zafiyetlerin risk yüzdeleri elde edilmiştir.



$$S_n = \sum_{k=1}^n w_n \cdot P_n = \frac{100}{S_n} \left(S_n - \frac{w_n}{2} \right) \quad (2)$$

Girdi zafiyetleri üzerinde “Ağırlıklı Yüzde Formül’ü” uyguladıktan sonra Tablo II’deki değerler elde edilmiştir.

Tablo II. Risk yüzdeleri ile beraber girdi doğrulama zafiyetleri

Risk Sıralaması	Girdi Doğrulama Zafiyeti	Ağırlık	Risk %
1	SQL Injection	4	80%
1	Code Injection	4	80%
1	OS Command Injection	4	80%
2	XSS	3	75%
3	Path Traversal	2	66.7%
4	Input Validation	1	50%

Zafiyetlerin riskleri tanımlandıktan sonraki aşamada Uygulama düğümünün ODT’si hesaplanır. Uygulama düğümünün içerdiği değer sayısını 2^{n+1} olarak tanımlanmıştır, n değerini Uygulama düğümüne bağlı olan öncel düğümlerin (zafiyet kategorilerinin) sayısı olarak belirlenmiştir. 1 değeri ise yanlış değerlerin hesaplanmaya katılması için eklenmiştir.

$$(hesaplanmış doğru değer) + (hesaplanmış yanlış değer) = 1 \quad (3)$$

Aksi takdirde Bayesian Ağına sadece doğru değerleri tanımlanacaktır ve eksi yöndeki değişimleri görülemeyecektir. Bu durumda, Uygulama düğümünün ODT’si $2^{6+1} = 128$ içerecektir. Uygulama düğümünün ODT değerleri hesaplandıktan sonra Bayesian Ağlarına uygun formatta değerler sunabilmek için değerler üzerinde 1-0 normalizasyonunu (4) uygulanmıştır.

$$Normalized(e_i) = \frac{e_i - E_{min}}{E_{max} - E_{min}} \quad (4)$$

B. Zafiyet Düğümlerinin ODT’lerinin Hesaplanması

Bayesian Ağındaki bütün fonksiyon düğümleri her zafiyet düğümüne yönelik ayırt ile bağlanmıştır. Böylece zafiyetlerin ODT değerlerini fonksiyon düğümleri belirleyecek anlamına gelmektedir. Zafiyetlerin ODT değerlerini 3 tip fonksiyon bilgisi ile değerlendirilmiştir.

İlk olarak Tablo I’de görüldüğü gibi NVD [2] üzerinden toplanan Ocak 2000’den Ocak 2014’e kadar zafiyetlerin sıklıkları hesaplanmış, fonksiyonları hangi olasılıkla karşılaştığı bilgisini çıkarılmıştır. Bu bilgiyi fonksiyon bilgisi olarak kullanılmanın nedeni, rapor edilen zafiyetlerin kod üzerinden yapılmış olmasından kaynaklanmaktadır. Ek olarak, Bayesian Ağlarının doğası gereği öncel (fonksiyon) düğümlerin bilgilerini takipçi (zafiyet) düğümlerine kalıtsal olarak aktarır. Böylece takipçi düğümler zafiyet sıklığı bilgisinden mahrum kalmayacaktır.

İkinci bilgi olarak, fonksiyonları derinlik bilgisi kullanılmıştır. Derinlik terimini detaylandırıldığında, bir fonksiyonun çağrı çizgesi çıkarıldığında, bir fonksiyonun

çağırma ilişkilerini bir yönlendirilmiş çizge ile elde edilir. Çağrı çizgesindeki döngüleri görmezden gelerek, fonksiyonun çağırılma anından yaprak düğümüne kadar en uzun mesafesi alınarak derinliği hesaplanır. Bir fonksiyonun çağrı çizgesinde bulunan diğer fonksiyonları da göz önünde bulundurarak, bir fonksiyonun derinliği arttıkça doğru orantılı olarak potansiyel zararının da artacağı varsayılmaktadır.

Üçüncü ve son bilgi olarak, belli bir fonksiyonun kod içerisinde kaç kez çağırıldığının bilgisidir. Eğer bir fonksiyon kod içerisinde birçok kez çağırılıyorsa, çağırılan fonksiyonun kod içerisindeki kapsanması da artacaktır.

C. Fonksiyon Düğümlerinin ODT’lerinin Hesaplanması

Bayesian yaklaşımı kanı temellidir ve belirsiz sonuçlar sunmaktadır. Belirsizlik, bir durumdan %100 emin olmama anlamına gelmektedir. Bu yüzden BA’larda olasılık değerlerinde küçük bir standart sapma verilmektedir. Aksi takdirde 1 ve 0 gibi kesin değerlerin verilmesi ile Bayesian yaklaşımdan ziyade bir Sıklıkçı/Frequentist yaklaşım olmaktadır. Bir Sıklıkçı yaklaşım, bir olayların frekanslarına bağlı olarak rastgele durumlara değer atamaktadır. Bir Bayesian yaklaşım ise belirsiz durumlara göre olasılık değerleri atamaktadır.

Bu sebeple fonksiyon düğümlerinin ODT’da *doğru* ve *yanlış* durumları vardır. *Doğru* durumuna “0.95” değeri atanarak, fonksiyonun herhangi bir doğrulama kodu kullanmadığını, *yanlış* durumu için “0.05” değeri atanarak, fonksiyonun doğrulama kodu kullandığını belirtilmiştir. Bayesian yaklaşımına sadık kalmak için 1 ve 0 gibi kesin değerler verilmemiştir. Ayrıca kesin değerler verilmeyerek bazı özel durumlar da katmıştır. Örneğin; dil kodlanması atakları ve tip bazlı doğrulamaların atlatılması vb.

D. Otomatik Bayesian Ağ Oluşturucusunun Geliştirilmesi

Bayesian Ağın oluşturulmasında gerekli bilgilerin tutulması için bir araç önemli bir faktör. BA’nın düğüm bağlantılarını ve her düğümün ODT değerlerini tutacak bir dosya olmasıdır. Bu nedenle Java ile yazılmış açık kaynak bir yazılım aracı olan OpenMarkov [11] kullanılmıştır. Okunması ve yazması kolay olan XML formatına yakın bir dosya sağlamaktadır. Böylece OpenMarkov’un dosya formatı ile Bayesian Ağ oluşturulabilmektedir. OpenMarkov Java dilinde yazıldığından Bayesian Ağ Oluşturucusu Java dilinde geliştirilmiştir. BA’da ODT’lerin hesaplanmasında bağlantıların sağlanması ve dosya operasyon yapılması kolaylaştırıldı.

Otomatik Bayesian Ağının dinamik, otomatik ve esnek bir BA sağlaması hedeflenmektedir. Böylece geliştiriciler BA’larını JavaScript uygulamalarına göre dilediği gibi modifiye edebilecektir. Bunu sağlamak için, öncelikle geliştirilen aracın okuyacağı bir kurulum dosyası hazırlanmıştır. Geliştiricilere zafiyet ve fonksiyon eklemeleri ve çıkarmaları için imkan sağlamaktadır. Bir başka avantaj ise, kurulum dosyasının fonksiyon ve zafiyet bilgilerini içermesidir. Bu da geliştirilen aracın güncel kalmasını sağlamaktadır. Fonksiyon ya da zafiyet istatistiklerinde herhangi bir değişiklik ile karşılaşıldığında, kurulum dosyası değiştirilip şimdiki zaman değerlerine adapte edilebilmektedir.

İlerleyen aşamalarda algoritmalar (her zafiyet ve fonksiyonun ODT'lerin değerlendirilmesi) araca entegre edilmektedir. Daha sonra düğümler tanımlanarak BA oluşturulmaktadır. Bir sonraki aşamada düğümlerin ilişkileri ve bağlantıları sağlanmaktadır ve BA'nın mimarisinin nasıl olacağı tanımlanmaktadır. BA üç katmanla tanımlanmaktadır; Uygulama, Zafiyet ve Fonksiyon. Özetle, düğümlerin ilişkilerini araca tanımlarken, bütün zafiyet düğümlerini Uygulama düğümüne yönlendirilmektedir ve bütün fonksiyon düğümleri her bir zafiyete yönlendirilerek tam ikili parçalı bir çizge elde edilmektedir. Son olarak, hesaplanmış ODT'leri düğümler atanmaktadır.

IV. ÖRNEK ÇALIŞMA

Örnek çalışma olarak jQuery'nin sürüm 1.9.1 kütüphanesi seçilmiştir. jQuery sık kullanılan ve web uygulama geliştiricilerin tercih ettiği bir kütüphanedir. Geliştiricilerin jQuery'i tercih etmelerindeki en büyük etken hızlı, küçük ve zengin içerikli olmasıdır. Geliştiricilere yardımcı olabilecek birçok fonksiyon içermektedir, örneğin; olay işleme, HTML doküman gezinmeleri, manipülasyon ve animasyon vb. Bununla beraber birçok popüler web sayfalarında kullanılmaktadır; Amazon, Microsoft, WordPress, Reddit, Instagram, Stack Overflow, the Guardian, Fox New vb. Öncelik olarak fonksiyonların bilgilerinin toplanması üzerine yoğunlaşılmaktadır.

A. Seçilen jQuery Fonksiyonları

İlk adımda 10 tane en sık kullanılan ve geliştiriciler tarafından en çok tercih edilen fonksiyonlar seçilmektedir. Ek olarak, Cooper [12] Bayesian Ağların sonuç çıkarımlarının NP-hard problem olarak tanımladığı için fonksiyon seçimi 10 ile kısıtlanmıştır. Seçilen fonksiyonlar üzerinden fonksiyonların parametrelerinin kullanılmadan önce doğrulanıp doğrulanmadığını kontrol edilir. Parametrelerin doğrulanıp doğrulanmadığını öğrenmek için TAJ'S'nin [8] akış çizgesi özelliği üzerinden herhangi bir doğrulama bloğun olup olmadığı elle de kontrol edilmiştir.

Şekil 1'de, TAJ'S ile "attr()" fonksiyonunun akış çizgesi çıkartılmıştır. Herhangi bir girdi doğrulama işleminin yapıp yapılmadığını kontrol edilmeden önce her parametreyi birer girdi olarak kabul edilmiştir. Daha sonra parametrelerin kullanılmadan önce doğrulanıp doğrulanmadığını kontrol edilmiştir. Şekil 1'de kırmızı çerçeve içerisinde fonksiyonun parametreleri görülebilmektedir. Kırmızı çerçeveye bakıldığında parametreler üzerinde "okuma/read" operasyonu uygulanmaktadır, bir başka deyişle parametrelerin kullanılmaya başladığının bir göstergesidir. Bu yüzden kırmızı çerçevenin üstüne bakıp öncesinde parametreler üstünde herhangi bir doğrulama yapılmış mı kontrol edilmektedir. Akış çizgesine bakıldığında parametreler kullanılmadan önce herhangi bir doğrulama işlemi ile karşılaşılmamaktadır. Şekil 2'ye bakıldığında, aynı fonksiyonun çizgesinin bu sefer bir doğrulama işleminin yapıldığı sürümü incelenmektedir. Bu incelendiğinde parametrelerin kullanıldığı kırmızı ve yeşil çerçeveler görülmektedir. Ancak, yeşil çerçevedeki "okunma/read" operasyonu doğrulama için bir "if/sorgu-blok'u" için uygulanmaktadır. Eğer parametre koşulları

sağlamıyorsa, akışı bir başka duruma yönlendirilerek yazılımın zarara uğramasını engellemektedir.

İkinci aşamada, fonksiyonun jQuery içerisinde kaç kez çağırıldığı sayılmaktadır. Sonuçları el ile de kontrol ederek bir fonksiyonu bulmak ve kaç kez çağırıldığını saymak için Eclipse'in Refactor özelliği ile JSRefactor [13] kullanılmaktadır. Üçüncü aşamada, fonksiyonların derinliklerini hesaplamak için çağrı çizgeleri çıkartılarak, çağırıldığı andan en uzun yaprak düğümüne kadar olan mesafe alınmaktadır. Fonksiyonların çağrı çizgelerini elde etmek için TAJ'S'nin çağrı çizgelerini çıkartma özelliğinden faydalanılmaktadır. Seçilen 10 fonksiyon hakkında elde edilen bilgiler Tablo III'de görülmektedir.

Tablo III. Program fonksiyon bilgileri.

Fonksiyonun Adı	Fonksiyonun jQuery içerisinde kaç kez çağırıldığı	Derinlik
html()	2	2
text()	1	2
css()	32	4
attr()	3	2
val()	5	0
each()	59	0
data()	5	2
hasData()	2	0
removeData()	1	2
find()	19	0

B. jQuery'nin Güvenilir Olmayan Verilere Karşı Hazırlığı

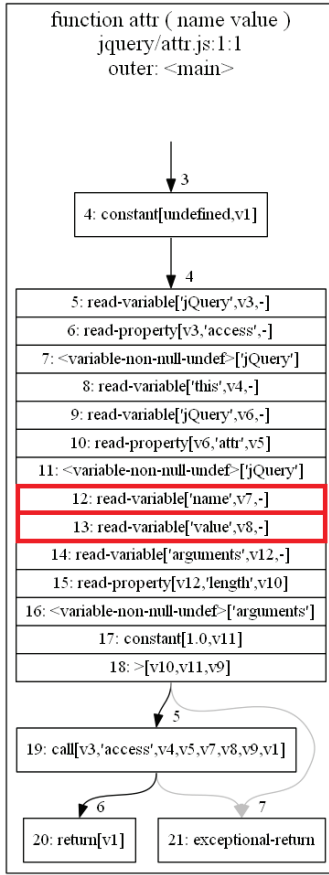
Bayesian Ağının Bayesian Ağ Oluşturucusu ile çalıştırıldığında sadece hangi tip zafiyetler ile karşılaşılacağı bilgisi değil aynı zamanda uygulamanın güvenilir olmayan verilere karşı hazırlığını da incelenmektedir. Tablo IV'de BA'nın verdiği değerler görülmektedir.

Tablo IV. Uygulamanın girdi doğrulama zafiyeti içermesi olasılıkları

Zafiyet	Zafiyetin uygulama içerisinde karşılaşımla olasılığı
XSS	0.95
SQL Injection	0.74
Input Validation	0.56
Code Injection	0.39
Path Traversal	0.29
OS Command Injection	0.03

Bayesian Ağ üzerinde herhangi bir değişiklik yapılmadığı takdirde jQuery'nin seçilmiş 10 fonksiyonuna göre, güvenilir olmayan verilere karşı hazırlığını 0.51 olarak ölçülmektedir. Bu sonuç üzerinden jQuery'nin güvenilir olmayan verilere karşı %51 hazır olarak yorumlanmaktadır.

Ancak, fonksiyonları "Not Used/Kullanılmamış" durumları seçerek hazırlık değerleri değiştirilebilmektedir. Bununla beraber, eğer bir uygulama herhangi bir veritabanı kullanmamış ise, geliştirici "SQL Injection" zafiyet düğümünün durumunu "Not Contains/İçermiyor'a" çevirip hazırlık değerini değiştirebilmektedir, çünkü veritabanı olmayan bir uygulamanın SQL Injection saldırılarına karşı bir etkisi olmayacaktır. Şekil 3'de Bayesian Ağ Oluşturucusunun

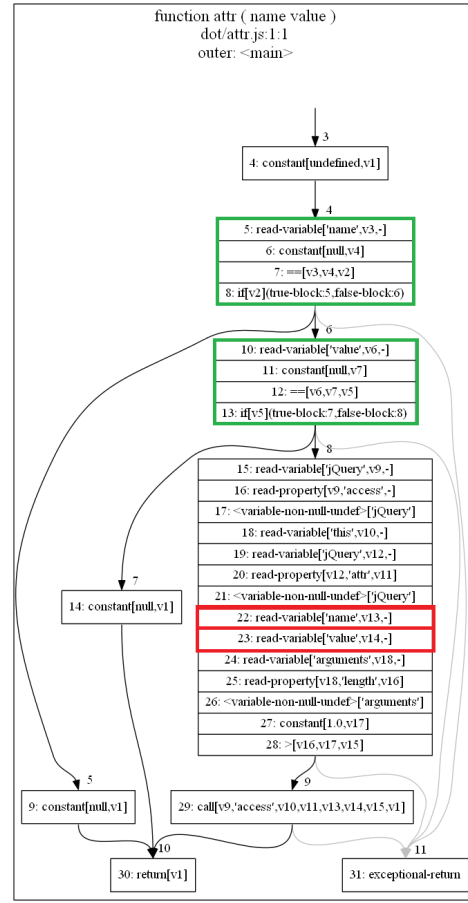


Şekil 1. Doğrulanmamış parametrelerin akış çizgesi örneği.

fonksiyonların “Not Used/Kullanılmamış” ve zafiyetlerin “Not Contains/İçermiyor” ekran alıntısı görülmektedir. Yapılan seçimlerle ve ayarlarla hazırlık değerinin 0.41 olduğu görülmektedir. Gri düğümler geliştiricinin seçilmiş düğümlerini ifade etmektedir. Fonksiyon düğümlerinde ise seçim için iki durum tanımlanmıştır; doğrulanmış parametreler/girdiler ve doğrulanmamış parametreler/girdiler. Geliştirici “Not Used/Kullanılmamış” durumunu işaretlediğinde, otomatik olarak zafiyet düğümlerini içermeye yüzdeleri yükselecek ve uygulama düğümünün hazırlık yüzdesi azalacaktır. Çünkü “Not Used/Kullanılmamış” durumu seçilerek, geliştirici fonksiyonun parametreleri için gerekli doğrulama işlemlerini yapmadığını onaylamaktadır. Ancak geliştirici fonksiyon parametreleri için gerekli doğrulama operasyonlarını tamamlamışsa “Used/Kullanılmış” durumunu seçerek zafiyet düğümlerinin yüzdelerini düşürebilir ve uygulama düğümünün hazırlık yüzdesini yükseltebilmektedir.

V. SONUÇ

Bu bildiride Bayesian Ağları ile JavaScript uygulamalarında güvenilir olmayan verilere karşı hazırlığının ölçülmesi için bir yöntem ve bunu yapabilecek otomatize edilmiş Bayesian Ağ Oluşturucusu geliştirilmiştir. Güvenilir olmayan verileri tanımlandığında, toplamış olduğumuz verilerden (14 yıllık rapor edilmiş zafiyetlerin istatistikleri) girdi doğrulama



Şekil 2. Doğrulanmış parametrelerin akış çizgesi örneği.

zafiyetlerin davranışları gözlemlenmiştir. Her zafiyetin yazılım geliştirme yaşam döngüsü içerisindeki zarar azaltma istatistikleri incelenmiştir. İncelemeler sonucunda 6 tane girdi zafiyeti bir karar ağacı ile sınıflandırılmıştır. Yazılım geliştirme yaşam döngüsünün tasarım ve geliştirme aşamalarında, girdi doğrulama zafiyetleri için önerilen zarar hafifletme işlemi girdilerin doğrulanmasıdır. Bu nedenle statik analizi sadece potansiyel girdi doğrulama zafiyetlerini tespit etmek için değil, aynı zamanda uygulamanın fonksiyonları analiz ederek derinliklerinin çıkarılması için de kullanılmıştır. Ek olarak, fonksiyonların kaç kez çağırıldıklarını bulabilmek için refactoring kullanılmıştır.

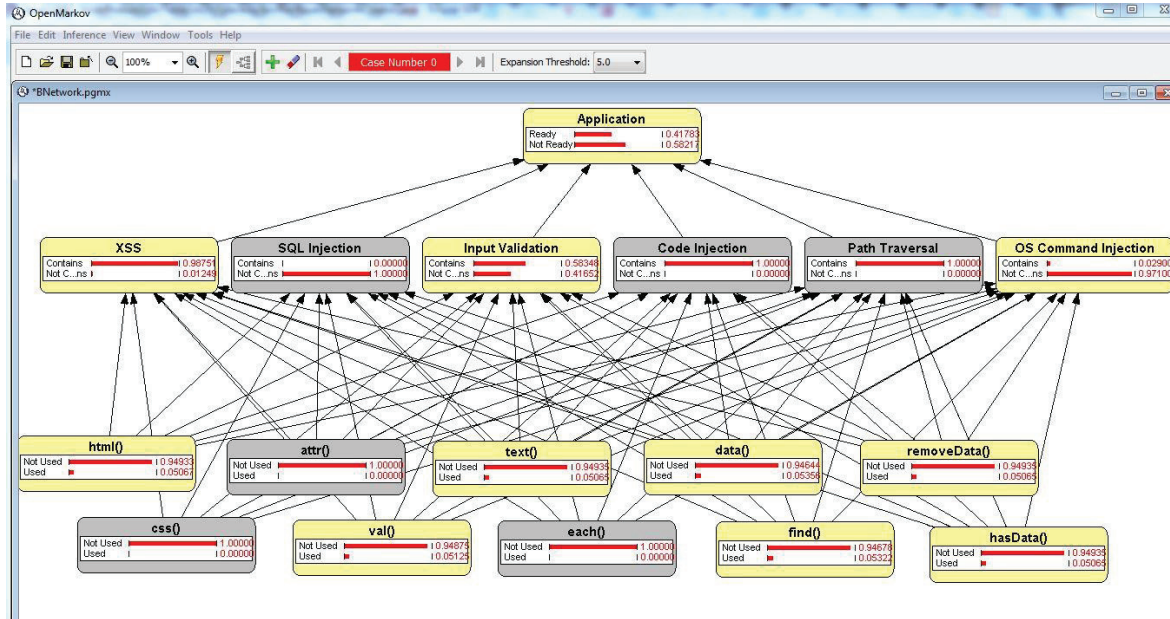
Bayesian Ağını oluşturulurken üç aşama ile tanımlanmıştır; faktörler, aktiviteler ve uygulamanın hazırlığı. Faktörler, girdi zafiyetlerin sıklığını, fonksiyonun derinliği ve fonksiyonun kaç kez çağırıldığının bilgilerinin tutan fonksiyon düğümlerine karşılık gelmektedir. Faaliyet aşaması, zafiyetlerin zarar verme yüzdelerini tutan girdi zafiyetleri düğümlerine denk gelmektedir. Son aşama ise, uygulamanın güvenilir olmayan verilere karşı hazır olma durumunun ölçümünü veren çıkış düğümüdür.

Örnek çalışmada, testler JavaScript geliştiricilerinin kullanımından ve sık tercih etmelerinden dolayı JavaScript’in en popüler kütüphanesi olan jQuery üzerinde

gerçekleştirilmiştir. Son olarak, jQuery'nin en sık kullanılan 10 fonksiyonu üzerinden deneyler gerçekleştirilerek, Bayesian Ağındaki düğümlerindeki durumlarda hiçbir değişiklik yapmadan, jQuery'nin güvenilir olmayan verilere karşı hazırlığı %51 olarak ölçülmüştür. Sadece güvenilir olmayan verilere karşı hazırlığının ölçülmesi ile kalmayıp, uygulamanın içerisinde hangi zafiyetin ne kadar olasılıkla bulunma durumlarını da gözlemlemiştir.

Netice olarak, Bayesian Ağlarını kullanan birçok çalışmada bilgi eşit olarak dağıtılmıştır. Ancak önerilen model ve

geliştirilen araçta gerçek bilgi ve istatistikler kullanıldığından sunulan ölçüm ve çalışma diğer çalışmalardan ayrılmaktadır. Bir başka avantaj ise sunulan aracın esnek ve dinamik olmasıdır. Böylece geliştirici kolaylıkla kendi fonksiyon, zafiyet ve bilgilerini tanıtabilmektedir. Bu bildiride geliştiricilerin yazılımlarının güvenilir olmayan verilere karşı ne kadar hazır olduğu ölçen bir model ve bir araç geliştirilmiştir. Böylece geliştiriciler ölçüm sonuçlarını gözlemleyip uygulamalarını buna göre geliştirebilmektedir.



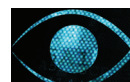
Şekil 3. Bayesian Ağ Oluşturucu Ekran Alıntısı.

KAYNAKLAR

- [1] N. Smithline, OWASP Top 10 2013, https://www.owasp.org/index.php/Top_10_2013-Top_10_2013.
- [2] National Vulnerability Database, <http://web.nvd.nist.gov/view/vuln/statistics>, 2014.
- [3] S. Wagner, A Bayesian Network Approach to Assess and Predict Software Quality using Activity-based Quality Models. Information and Software Technology, 52, pp.1230-1241, 2010.
- [4] S. Christey, Preliminary List Of Vulnerability Examples for Researchers, NIST Workshop Defining the State of the Art of Software Security Tools, Gaithersburg, MD, August 2005.
- [5] M. Frigault and L. Wang . Measuring network security using bayesian network-based attack graphs (pp. 698-703). IEEE, 2008.
- [6] S. Kondakçı. Network Security Risk Assessment Using Bayesian Belief Networks, IEEE International Conference on Privacy, Security, Risk and Trust, 978-0-7695-4211-9/10, 2010.
- [7] S. Guarnieri and V.B. Livshits. Gulfstream: Incremental static analysis for streaming JavaScript applications. In Proceedings of the USENIX Conference on Web Application Development, 2010.
- [8] S. H. Jensen, A. Möller, and P. Thiemann. Type analysis for JavaScript. In Proc. 16th International Static Analysis Symposium, SAS '09, volume 5673 of LNCS, pages 238–255. Springer-Verlag, August 2009, 2009.
- [9] D. Heckerman. A Tutorial on Learning With Bayesian Networks, Technical Report, Microsoft Research, no. MSR-TR-96-06, <http://research.microsoft.com/apps/pubs/?id=69588>, 1996
- [10] K.B. Korb and A.E. Nicholson. Bayesian artificial intelligence. cRC Press, 2003.
- [11] OpenMarkov, <http://www.openmarkov.org/>, 2014.
- [12] G.F. Cooper. "The computational complexity of probabilistic inference using Bayesian belief networks." Artificial intelligence 42, no. 2: 393-405, 1990.
- [13] JSRefactor, <http://www.brics.dk/jsrefactor/>, 2014.

Ekincan UFUKTEPE İzmir Ekonomi Üniversitesi Bilgisayar Mühendisliği Bölümü'nden 2011 yılında mezun oldu. İzmir Yüksek Teknoloji Enstitüsü'nde Bilgisayar Mühendisliği Bölümünden 2014 Eylül ayında Yüksek Mühendis olarak mezun oldu. Halen İzmir Yüksek Teknoloji Enstitüsü'nde Araştırma Görevlisi olarak görevine devam etmektedir.

Tuğkan TUĞLULAR Ege Üniversitesi Bilgisayar Mühendisliği Bölümü'nden doktoraını 1999 yılında aldı. 2000 yılında İzmir Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü'ne katılan Tuğlular aynı bölümde Öğretim Üyesi olarak görevine devam etmektedir.



On the security of Lo *et al.*'s ownership transfer protocol

Nasour Bagheri, Masoumeh Safkhani

Abstract—Recently Lo *et al.* have proposed an ownership transfer protocol for RFID objects using lightweight computing operators and claim their protocol provides stronger security robustness and higher performance efficiency in comparison with existing solutions. However, in this paper we show that their claim unfortunately does not hold. More precisely, we present tag's secret disclosure attack, new owner's secret disclosure and fraud attack against the Lo *et al.*'s ownership transfer protocol. The success probability of all attacks is "1" while the complexity is only one run of protocol. Our observation shows that this protocol compromise the privacy of the tag and the new owner.

Index Terms—RFID, Ownership Transfer Protocol, Disclosure Attack, Fraud Attack.

I. INTRODUCTION

Radio Frequency Identification (or in short term RFID) has many applications for both business and private individuals. Several of these applications will include items that change owners at least once in their lifetime. The swapping and resale of items is a practice that is likely to be popular in the future, and so any item that depends on RFID for function or convenience should be equipped to deal with change of ownership.

In the case of ownership transfer, we want to prevent the old owner of a tag from accessing that tag or the services that the tag provides to the current owner. For instance, an old owner should not be able to use any keys or identifying values to impersonate the tag to make a purchase, open a door, or even change the ownership back to him. In summary, a secure ownership transfer protocol must satisfy the following properties:

- The old owner should not be able to access the tag after the ownership transfer has taken place.

Nasour Bagheri and Masoumeh Safkhani are with the Department of Electrical Engineering, Shahid Rajaee Teachers Training University, Tehran, Iran.

- The new owner should be able to perform mutual authentication with the tag after the ownership transfer has taken place.

Ownership transfer presents its own set of threats and therefore demands the attention of security researchers. Observing that tags may become highly ubiquitous in the future, with tagged object changing hands often, secure owner transfer would be essential to the RFID systems. Hence, several ownership transfer protocols have been proposed in the literatures [8], [11], [3], [16], [9], [7], [1], [12], [4], [2], [6], [15]. However, the later analysis [14], [5], [13] demonstrated security flaws on some of them that shows that it is not an easy task to design a secure ownership transfer protocol.

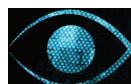
A. Overview of the Current Work

Recently Lo *et al.* have proposed an ownership transfer protocol using lightweight computing operators [10]. They have claimed their protocol provides suitable security and performance in comparison to other schemes in this field. However, in this paper we provide a detailed security analysis of the protocol which leads to several efficient attacks against the protocol, i.e. tag's/new owner's secret disclosure attack and fraud attack.

Paper Organization: Notations used in the paper are presented in Section II. Lo *et al.*'s ownership transfer protocol is described in Section III. Section IV and Section V describe our tag's secret disclosure attack and fraud attack respectively. Finally, we conclude the paper in Section VI.

II. PRELIMINARIES

Throughout the paper, we use the following notations:



- TTP : The trusted third party server.
- O_C : The current owner of the tagged object.
- O_N : The new owner of the tagged object after ownership transfer.
- A : Adversary.
- Tag_i : An RFID tag i .
- TID_i : Unique identifier of tag i .
- OID_j : The identifier of owner j .
- $TTPID$: The identifier of TTP .
- C_j : The credential of the owner j .
- KT_i : The shared secret key between Tag_i and TTP .
- KO_i : The shared secret key between Tag_i and O_C .
- $h()$: One way hash function.
- r_x : The x -th random number where $x \in Z^+$.
- $\oplus$: The exclusive-or operation.
- $Nun(m, n)$: A lightweight function which is built with bit-shift and add operations.

$Nun(m, n)$ function has two input values, m and n , where m is the value to be verified and n is a random number to reshuffle the original input value m . The pseudo-code of Nun is shown as below:

```
string Nun(bit string m, bit string n){
    string X=m
    int L=bit length of X value
    for(int i=0;i<L;i++){
        {
            X=(X>>1)+(X<<1)+n
        }
    }
    return X
}
```

III. LO *et al.*'S OWNERSHIP TRANSFER PROTOCOL DESCRIPTION

Lo *et al.*'s [10] protocol, has three phases including registration phase, current ownership suspension phase and new ownership establishment phase. The details of Lo *et al.* protocol is described as below:

- **Registration Phase** All tags will be initialized before using and all object owners have to register their identities at TTP . TTP shares a secret key KT_i with each tag i , where KT_i is preloaded into the memory of tag i and neither current owner nor new owner can access (or know) the key. Each owner j has a credential key $C_i = h(TTPID || OID_j)$ such

that TTP can verify the identity of requesting owner when receiving an ownership transfer request from an object owner. In addition, the current owner and the Tag_i are set to share the same secret key KO_i .

- **Current Ownership Suspension Phase** The details of current ownership suspension phase which is depicted in Fig. 1 are as follows:

- 1) O_C generates a random number r_1 and sends $(OID_C, OID_N, TID_i, r_1, C_C)$ to TTP .
- 2) Once receipt the message, TTP calculates $C'_C = h(TTPID || OID_C)$. If $C'_C \neq C_C$, TTP will terminate this session. Otherwise, TTP :
 - Finds corresponding KT_i for Tag_i ,
 - Generates a temporary secret key K_{temp} ,
 - Computes $M_1 = KT_i \oplus K_{temp} \oplus r_1$ and a verification message $V_1 = Nun(M_1, r_1)$,
 - Sends M_1 and V_1 to O_C .
- 3) Upon receipt the message, O_C computes $M_2 = M_1 \oplus KO_i$ and forwards (V_1, M_2, r_1) to Tag_i through its reader and starts a timer to control the tag's responding time.
- 4) When Tag_i receives the message, extracts $M'_1 = M_2 \oplus KO_i$ and computes $V'_1 = Nun(M'_1, r_1)$. If $V'_1 = V_1$, Tag_i extracts K_{temp} as $K_{temp} = M_1 \oplus KT_i \oplus r_1$ and assignes it to its secret KO_i and sends $ACK_1 = Nun(KT_i, r_1) \oplus K_{temp}$ to O_C , as its response. However, if $V'_1 \neq V_1$, tag sends a random number r_2 as ACK_1 .
- 5) If O_C receives the tag response in the appropriate time(before timeout occurs) it forwards ACK_1 to TTP . Otherwise, O_C tries to use the old key KO_i to access Tag_i . If O_C cannot access the tag, it sends $ACK_1 = OID_C$ to TTP . Otherwise, it restarts Step 4.
- 6) Once TTP receives the message, it verifies whether $ACK_1 = Nun(KT_i, r_1) \oplus K_{temp}$ or $ACK_1 = OID_C$. In the case of equality, TTP passes $ACK_2 = \text{'success'}$ to O_C . In addition, TTP transfers K_{temp} and TID_i to O_N . Otherwise, TTP passes a failure message, $ACK_2 = \text{'go to step 4'}$, to O_C to restart the process from Step 4.

- **New Ownership Establishment Phase** The details of this phase which is depicted in Fig. 2 are as

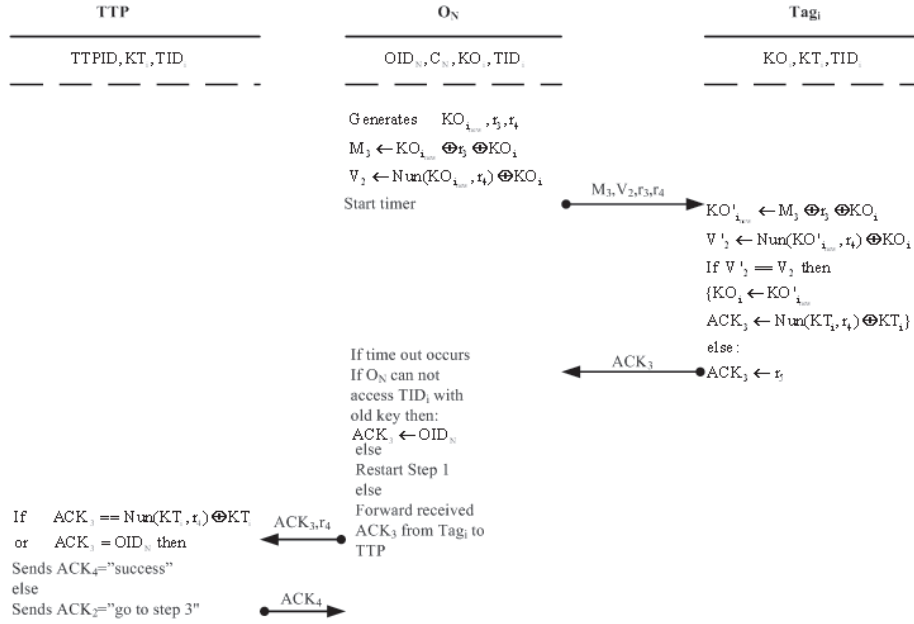


Fig. 2. The New Ownership Establishment Phase in Lo *et al.*'s Ownership Transfer Protocol.

to transfer the tags ownership from O_C to O_N . KT_i is a secret parameter and neither O_C nor O_N are expected to be able to retrieve it. However, in this section we show that how a curious owner can disclose the secret of the tag, KT_i . In this attack O_C transfers the ownership of Tag_i to itself once and based on the transferred messages, it can retrieve KT_i . To extract KT_i , curious owner O_C can do as follow:

- 1) O_C starts a new ownership transfer protocol and sends $(OID_C, OID_N, TID_i, r_1, C_C)$ to TTP .
- 2) On receiving the message, TTP authenticates O_C and does as follows:
 - Finds corresponding KT_i for Tag_i ,
 - Generates a temporary secret key K_{temp} ,
 - Computes $M_1 = KT_i \oplus K_{temp} \oplus r_1$ and a verification message $V_1 = Nun(M_1, r_1)$,
 - Sends $M_1 = KT_i \oplus K_{temp} \oplus r_1$ and V_1 to O_C .
- 3) Once O_C receives (M_1, V_1) , it sends OID_C as ACK_1 to the TTP .
- 4) On receiving the message, since ACK_1 equals OID_C , TTP passes $ACK_2 = \text{'success'}$ to O_C . In addition, TTP transfers K_{temp} and TID_i to

O_N which is also O_C .

- 5) Given M_1 , r_1 and K_{temp} , O_C extracts KT_i as $KT_i = M_1 \oplus K_{temp} \oplus r_1$.

Hence, the curious owner O_C can disclose secret of the Tag_i , i.e. KT_i . The success probability of the given attack is "1" and the attack complexity is only one run of protocol. If KT_i is known by O_C , then whenever O_C transferred the ownership of Tag_i to a new owner O_N , O_C would be able to trace Tag_i which compromise the privacy of the new owner O_N . Even worse, the adversary can extract the secret key of the new owner $KO_{i_{new}}$ as follows:

- 1) O_C generates a random number r_1 and sends $(OID_C, OID_N, TID_i, r_1, C_C)$ to TTP .
- 2) Upon receipt the message, TTP authenticates O_C and does as follows:
 - Finds corresponding KT_i for Tag_i ,
 - Generates a temporary secret key K_{temp} ,
 - Computes $M_1 = KT_i \oplus K_{temp} \oplus r_1$ and a verification message $V_1 = Nun(M_1, r_1)$,
 - Sends M_1 and V_1 to O_C .
- 3) Upon receipt the message, O_C computes $K_{temp} =$

- $M_1 \oplus KT_i \oplus r_1$.
- 4) The rest of the second phase of protocol continue as it has described in section III.
 - 5) Once O_N receives K_{temp} , it does as follows:
 - Generates the new secret key $KO_{i_{new}}$ and random numbers r_3 and r_4 ,
 - Computes $M_3 = KO_{i_{new}} \oplus r_3 \oplus KO_i$ and $V_2 = Nun(KO_{i_{new}}, r_4) \oplus KO_i$ and sends (M_3, V_2, r_3, r_4) to Tag_i .
 - 6) O_C eavesdrops the transferred message (M_3, V_2, r_3, r_4) and does as follows :
 - Given K_{temp} from step 5 and the eavesdropped M_3 and r_3 , computes $KO_{i_{new}}$ as $KO_{i_{new}} = M_3 \oplus r_3 \oplus K_{temp}$.
 - 7) O_C does not disrupt the rest of the protocol and Tag_i and O_N finish the protocol successfully.

Hence, following the given attack, the old owner O_C can disclose the secret key of the new owner O_N . Given the owner secret key it would be easy to do what you want, trace the tag, impersonate the owner, etc. It must be noted that the success probability of the given attack is “1” and the attack complexity is only one run of protocol.

Remark 1: . One may argue that to prevent the curious O_C to retrieve the tag’s secret key and therefore the new owner’s secret key, we can force TTP to not allow the owner to transfer the ownership to itself. However, then two person, e.g. O_C and O'_N , can collude to retrieve the tag secret and then transfer its ownership to the victim owner O_N .

V. FRAUD ATTACK

In this section we present another attack against Lo *et al.*’s protocol in which the owner O_C can satisfy the new owner O_N , confirmed by TTP certification, while after ownership transformation O_N cannot access Tag_i but O_C can do. Hence, O_C can sell the same tag to several person. Whenever insincere O_C decides to sell the ownership of Tag_i to a victim owner O_N , it does as below:

- 1) O_C generates a random number r_1 and sends $(OID_C, OID_N, TID_i, r_1, C_C)$ to TTP .
- 2) On receiving the message, TTP authenticates O_C and does as follows:
 - Finds corresponding KT_i for Tag_i ,
 - Generates a temporary secret key K_{temp} ,

- Computes $M_1 = KT_i \oplus K_{temp} \oplus r_1$ and a verification message $V_1 = Nun(M_1, r_1)$,
- Sends M_1 and V_1 to O_C .

- 3) Upon receipt the message, O_C does not send anything to Tag_i and just sends its OID_C as ACK_1 to the TTP .
- 4) When TTP receives the message, since ACK_1 equals OID_C , passes $ACK_2 = \text{‘success’}$ to O_C . In addition, TTP transfers K_{temp} and TID_i to O_N .
- 5) Once O_N receives K_{temp} and TID_i replaces KO_i by the new generated secret key $KO_{i_{new}}$. Then, it generates the tuple (M_3, V_2, r_3, r_4) following the given procedure in section III and sends it to Tag_i .
- 6) O_C blocks (M_3, V_2, r_3, r_4) .
- 7) Since O_N does not receive the tag response in the appropriate time(before timeout occurs), O_N tries to use the old key KO_i to access Tag_i . However, O_N cannot access the tag, so it sends $ACK_3 = OID_N$ and r_4 to TTP ,
- 8) Once receipt the message, TTP verifies $ACK_3 = OID_N$ and sends $ACK_4 = \text{‘success’}$ to O_N .
- 9) When O_N receives a success message, it replaces KO_i with $KO_{i_{new}}$ and ensures that it has received the Tag_i ownership successfully.

Hence, following the given attack, the new owner beliefs that the ownership transfer has been done successfully and he is only one which can identify Tag_i and access the information inside the tag and the old owner cannot identify and control the tag any more. However, the given attack shows that a dishonest owner can deceive new owners, sell his tagged objects while he still has possession of them, because the tag has not updated its owner key yet. The success probability of our fraud attack is “1” while the complexity is only one run of protocol for each tag sell.

Remark 2: . The given attack works properly if any owner which has a record in TTP decides to deceive a new owner O_N that it can transfer the ownership of Tag_i to O_N . It comes from this fact that in Lo *et al.*’s protocol, TTP does not check whether O_C has the permission to transfer the ownership of Tag_i and it just verifies whether O_C has a record in the TTP database, while that record can be not necessarily to access Tag_i .

VI. CONCLUSION

In this paper we considered Lo *et al.*'s RFID ownership transfer protocol and demonstrated that, in contrary to its designers' claims, this protocol does not provide resistance tag's and new owner's secrets disclosure and fraud attacks. The success probability of all attacks are "1" while the cost of all is only one run of protocol.

REFERENCES

- [1] C. Chen, Y. Lai, C. Chen, Y. Y. Deng, , and Y. C. Hwang. Rfid ownership transfer authorization systems conforming epcglobal class-1 generation-2 standards. In *International Journal of Network Security*, volume 13, pages 41–48, 2011.
- [2] C.-L. Chen and C.-F. Chien. An ownership transfer scheme using mobile rfids. *Wireless Personal Communications*, pages 1–27, 2012.
- [3] S. Fouladgar, , and H. Afifi. An efficient delegation and transfer of ownership protocol for rfid tags. In *The First International EURASIP Workshop on RFID Technology, Vienna, Austria, 2007*.
- [4] S. Fouladgar and H. Afifi. A Simple Privacy Protecting Scheme Enabling Delegation and Ownership Transfer for RFID Tags. In *JOURNAL OF COMMUNICATIONS*, volume 2, pages 1502–1508, 2007.
- [5] Gaurav Kapoor and Selwyn Piramuthu. Vulnerabilities in Some Recently Proposed RFID Ownership Transfer Protocols . In *Networks and Communications, 2009. NETCOM '09. First International Conference on*, pages 354–357, 2009.
- [6] M. Hoque, F. Rahman, S. Ahamed, and J. Park. Enhancing privacy and security of rfid system with serverless authentication and search protocols in pervasive environments. *Wireless Personal Communications*, 55:65–79, 2010.
- [7] G. Kapoor and S. Piramuthu. Single rfid tag ownership transfer protocols. In *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2010*, pages 1–10, 2010.
- [8] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan. Lightweight Mutual Authentication and Ownership Transfer for RFID systems. In *The proceedings of IEEE INFOCOM 2010*, pages 1–5, March 2010.
- [9] H. Lei and T. Cao. Rfid protocol enabling ownership transfer to protect against traceability and dos attacks. In *The First International Symposium on Data, Privacy, and E-Commerce, Chengdu, China, 2007*, pages 508–510, 2007.
- [10] N.-W. Lo, S.-H. Ruan, and T.-C. Wu. Ownership transfer protocol for rfid objects using lightweight computing operators. In *6 th International Conference on Interney Technology and Secured Transactions, 11–14 December 2011, Abu Dhabi, United Arab Emirates*, pages 484–489, 2011.
- [11] K. Osaka, T. Takagi, K. Yamazaki, , and O. Takahashi. An efficient and secure rfid security method with ownership transfer. In *International Conference on Computational Intelligence and Security, Guangzhou, China*, pages 1090–1095, 2006.
- [12] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, T. Li, and Y. Li. vulnerability analysis of rfid protocols for tag ownership transfer. In *Computer Networks*, volume 54, pages 1502–1508, 2010.
- [13] M. Safkhani, M. Naderi, N. Bagheri, and S. K. Sanadhya. Cryptanalysis of Some Protocols for RFID Systems. Cryptology ePrint Archive, Report 2011/061, 2011. <http://eprint.iacr.org/>.
- [14] Suleyman Kardaş and Mete Akgun and Mehmet Sabr Kiraz and Huseyin Demirci. Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In *2011 Workshop on Lightweight Security& Privacy: Devices, Protocols, and Applications*, pages 20–25, 2011.
- [15] S.-S. Yeo, S.-C. Kim, S. Kim, G. Park, S. Kim, K.-S. Yang, and S.-E. Cho. Protecting your privacy with a mobile agent device in rfid environment. *Wireless Personal Communications*, 51:165–178, 2009.
- [16] Y. Zuo. Changing hands together: a secure group ownership transfer protocol for rfid tags. In *Hawaii International Conference on System Sciences, Koloa, Kauai, HI, 2010*,, pages 1–10, 2010.

The Past and Future of Mobile Malwares

M. O. Topgul, E. I. Tatli

Abstract—Cyber criminals are interested in developing malicious software in order to infect personal computers and gain financial benefits from infected users. With the evolution of mobile technologies, sophisticated malwares with more advanced features have been developed. In this paper, we list and explain the mobile malwares which target different mobile platforms (i.e. Symbian, Blackberry, J2ME, Android, iOS) in the past. The functional behaviors and future aspects of the mobile malwares are discussed in the paper as well.

Index Terms— mobile malwares, wearable malwares, malware analysis

I. MOTIVATION

MALWARE (aka "malicious software") refers to software programs designed to disrupt computer operations, gather sensitive information, or gain access to private computer systems [1]. Viruses, worms, trojan horses, adwares, spywares and rootkits are typical examples of such malicious software.

In the early 1980s the first viruses affected many computers and operating systems. At that time they were fortunately not as dangerous as today's malwares. Cyber criminals developing today new generation malwares aim financial benefits. They would like to get unauthorized access to personal information, credit card information, confidential user credentials etc. Worse still, they try to infect personal computers and mobile smart phones and make them zombie computers within their bot networks to misuse them for their illegal activities and cyber-attacks.

In the mobile smart phones era, malwares targeting mobile operating systems and mobile applications have become very popular. Since mobile smart phones contain mostly personal sensitive information (e.g. pictures, SMS messages, confidential application data, user credentials, etc.) and are also exploited for two-factor strong authentication by confidential applications like online banking or administration interface accesses, cyber criminals have a big interest to target mobile users and devices.

In this paper, we explain the past and future aspects of mobile malwares. In Section 2, the evolution of different mobile technologies, mobile devices and, parallel to this, mobile malwares are explained. In Section 3, mobile

malwares that were identified in the past for Symbian, Blackberry, J2ME, iOS and Android platforms are explained in details. In Section 4, the future aspects of mobile malwares and their new targets are discussed. Section 5 concludes the paper.

II. EVOLUTION OF TECHNOLOGIES AND MOBILE MALWARES

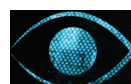
It has been 10 years since the first proof of concept mobile malware Caribe [2] was seen in the wild. From then, capabilities of mobile malwares have dramatically increased in the last years with the technological improvements proportionally. Between 2004 and 2006 Symbian was the main target of mobile malware developers. But this was changed after Apple's iOS (formerly iPhone OS) and Google's Android in 2007 were announced. Symbian, Windows CE, J2ME, iOS and Android platforms existed at these days, but none of them was a major target. Because malware developers considered the fact that none of the platforms were big enough to develop malware and gain financial benefit. Despite there was not a major target, J2ME was the most popular platform for the mobile malware developers between 2006 and 2009. After 2009, smartphone era began and the number of mobile malwares started to increase rapidly. Since smart phones were equipped with high capabilities, mobile malwares became more competent and dangerous day by day.

In 2010, mobile malware developers found a new target, namely Android. The first Android malware DroidSMS [23] was developed in August 2010. DroidSMS was the first sign of an evolving mobile malware market. 2011 and 2012 were the rising period of Android malwares. In 2011, Android malwares continued to surge and the total number of mobile malwares increased 6.4 times over just one year [3]. As a result, Android became the most targeted platform in 2011 with the growth of 200 times [4].

But the dramatic growth of mobile malwares was seen actually in 2012, particularly due to Android malwares. In some months of 2012 the number of detected mobile malwares was more than the total number of malwares in 2012. As a result, Android got the first place with more than 90% rate as the main target of mobile malwares [5] and this did never go down since 2012. The Figure 1 shows the total number of malware samples collected from January to December in 2012.

M.O. Topgul is a senior security researcher at TÜBİTAK-BİLGEM Cyber Security Institute. He continues his Ph.D. study in Electrical and Electronics Engineering at İstanbul Medipol University, 34810 İstanbul/Turkey, (e-mail: oguzhan.topgul@tubitak.gov.tr).

E.İ.Tatli is with the Department of Electrical and Electronics Engineering, İstanbul Medipol University, 34810 İstanbul/Turkey, (e-mail: eitlatli@medipol.edu.tr).



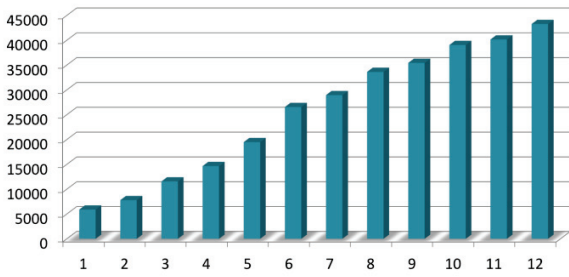


Figure 1. Malware sample numbers from January to December in 2012 [5]

The years of 2013 and 2014 were called the years of advanced mobile devices and advanced malwares. In 2013, mobile malware industry focused mostly on making profit from attacks. Malware developers focused mostly on financial gain attacks like premium service SMS trojans, credit card information thefts, e-wallet attacks, mobile banking trojans etc. The total number of online banking trojans increased up to 20 times [6]. In addition, most of the mobile malwares did include Command and Control Server (C&C) connections and have fully botnet capabilities. At the end of 2013, Android was still the main target of mobile malware with the rate of 98.05% as shown in Figure 2.

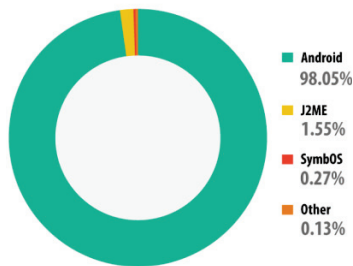


Figure 2. Malware rates of mobile platforms in 2013 [6]

There is actually a reason why Android has become the target platform for mobile malwares. Having the aim of being flexible, Android allows installation of applications from third party application markets. Since Google has no control over these third party app markets, mobile malware developers copy legitimate applications and copy especially well-known mobile games from the official Google Play Store, put their malicious codes within these applications, upload them to third party application markets, spread their malwares and infect Android users around the world.

In 2013 mobile malware developers started also applying anti-detection and anti-analysis techniques in their advanced malwares. Sophisticated mobile malwares can exploit zero-day vulnerabilities in order to gain high privileges on mobile devices and evade from anti-malware tools. Anti-VM techniques have been also added to new generation mobile malwares in order to bypass behavioral analysis sandboxes. Furthermore, malware developers use code obfuscation to make static code analysis much harder.

Despite the fact that, nearly all of mobile malwares are targeting Android platform, some iOS malware samples were

seen in the wild as well [7]. The total number of detected iOS malwares is so far only 11. Two of the eleven iOS malware samples appeared in the first half of 2014.

In 2014, there is another platform that has become attractive for mobile malware developers: Wearables. The first Google glass proof of concept malware namely Malnote was developed in March 2014. With the introduction of Android Wear in June 2014 and the Apple Watch in September 2014, it is not so hard to say, wearables will be one of the main targets of mobile malwares so called wearwares [8].

III. MOBILE MALWARES IN THE PAST

In 2014, ten years after the first mobile malware detection, mobile malwares became so sophisticated and the number of targeted platforms has considerably increased. It started with Symbian, continued with J2ME and today Android became the most targeted platform.

Within these past ten years, thousands of mobile malwares were developed with various kinds. While some of them are just proof of concept codes but some were personal data stealers and spyware malwares. In the beginning there were various vandal type destructive trojans and viruses, but they have become more financial oriented day by day. Nowadays there exist premium service abusers, financial-gain attackers and even ransom malwares, so called ransomwares, in the wild. After 2010, mobile malwares have become more advanced and complicated. They are equipped with sophisticated zero day privilege escalation attacks and botnet capabilities. As a result, today's mobile malwares are more dangerous than their ancestors.

In the following, some of the mobile malwares from the past are going to be examined and the mobile malware trend is studied.

A. 2004 The Symbian Age

The mobile malware era started with Symbian malwares in 2004. Caribe, Dust, Mosquito and Skulls are some examples of Symbian malwares:

- *Caribe/Cabir*: The first mobile malware was born in 2004. It was called Caribe/Cabir [9], which was just a proof of concept malware [21]. It spreads over Bluetooth connections and shows a message after infection (see Figure 3).

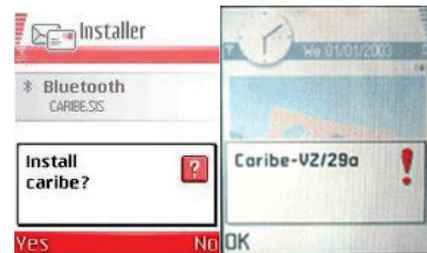


Figure 3. Infection with Caribe

- *Dust*: Dust [10][21] is a proof of concept malware that affects mobile devices running WindowsCE mobile operating

systems. It infects .exe files that are larger than 4 Kbytes. It spreads over Bluetooth and shows the message “Dear User, am I allowed to spread?” by infected devices.

- **Mosquito:** Mosquito [11][21] is a mobile malware that targets Symbian mobile devices. It spreads via peer-to-peer sharing services as a pirate version of a game called “Mosquitos”. Its main objective is sending SMS messages to premium services. It is the first instance of premium service abuser malwares.
- **Skulls /Skuller:** Skuller [12][21] is a vandal Trojan that targets Symbian as well. It appears as a theme file but by execution it changes all file icons (see Figure 4) and deletes phone contents. It is the first instance of destructive malwares.

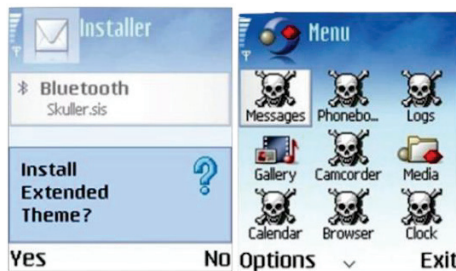


Figure 4. Infection with Skuller

B. 2005 The Symbian Age Continues

In 2015 Several Symbian malwares appeared in the wild as well. Lasco, PbStealer, Commwarrior, Booton, Cardblock are examples of Symbian malwares in 2005.

- **Lasco/Velasco:** After the source code of Caribe was revealed in 2005, many Caribe variants with different capabilities came out. Lasco [13][21] is one of the Caribe variants. It spreads over Bluetooth and infects all Symbian executables.
- **PbStealer/PbExplorer:** PbStealer [14] is one of the Caribe variants as well. It promises to compress user contacts and increase storage capacity, but it steals the phone book and sends all contacts to the nearest device via Bluetooth. It is the first instance of information stealer mobile trojans.
- **Commwarrior:** Commwarrior [15] is one of the most spread Symbian malware. It was detected in more than 20 countries around the world in the same period. It is the first mobile malware that uses MMS messages for infection (see Figure 5). It uses Bluetooth as a spread channel as well.

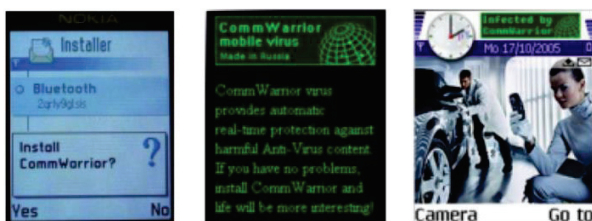


Figure 5. Infection with Commwarrior

- **Booton and Blackfont:** Booton and Blackfont malwares are both Skuller variants and destructive vandal trojans. They

spread over Bluetooth like their ancestors. Booton changes application icons. If any of the infected application is executed, the device is rebooted [16]. Blackfont deletes all font files so that all texts on the display become invisible.

- **CardBlock:** CardBlock [17] is another destructive vandal trojan. It is the first instance of ransomware malwares. But its main motivation is not financial benefit. It encrypts all MMC card contents and makes all the files useless. In addition, it deletes system files of the device.

C. 2006 The J2ME Age

Between 2006 and 2008, mobile malware developers discovered a new target and this is J2ME (Java Micro Edition). It is a technology independent platform which enables running codes on almost all other platforms like Symbian, Windows Mobile, etc. As a result, mobile malware developers focused on J2ME platform from 2006 till 2009.

- **RedBrowser:** RedBrowser [18] is the first J2ME malware in the history. It pretends to be a WAP browser, which offers free WAP browsing using SMS messages. However, what RedBrowser actually does is sending huge amount of SMS messages to premium services.

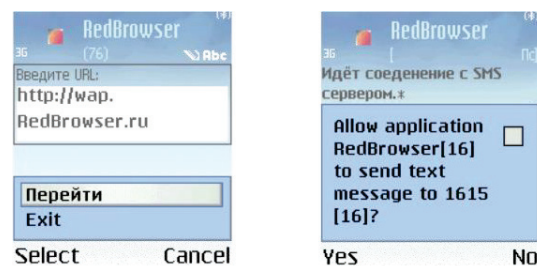


Figure 6. Infection with Redbrowser

- **FlexSpy/FlexiSpy:** FlexSpy [19] is one of the first mobile spywares. It is developed to capture phone call details, SMS, MMS, GPRS, email details and send them to a remote server. It has a web interface to access collected information via Internet. In 2006, FlexSpy did target only Symbian platform but today it threatens also iOS, Android and Blackberry platforms.

D. 2007-2009 A New Era with iOS and Android Begins

2007 was a special year regarding mobile technologies. Firstly, Apple's CEO Steve Jobs announced iPhone, which has affected the whole mobile device industry. Secondly, Google introduced Android v0.5 for mobile phones.

Apple's first generation iPhone was sold about 6.1 million units and the second-generation iPhone 3G was sold 6.9 million units until the end of 2008 [20]. As a result, Apple became one of third most selling mobile device manufacturers in 2008. In September 2008, the first commercial version of the Android operating system Android 1.0 and the first mobile phone powered by Android T-Mobile G1 were released.

At the end of 2008 and at the beginning of 2009, the attack

surface became much wider. In addition to Symbian, Windows Mobile, J2ME and Blackberry RIM, Android and iOS platforms became targets for mobile malware developers. However, none of these platforms became the only main target. Until the end of 2009, there appeared several Symbian, J2ME and WindowsCE targeting malwares in the wild.

- **iOS_KEE:** The most significant mobile malware of 2009 was iOS_KEE [27]. It is the first known iOS malware. It infects jailbroken devices by making an SSH connection with the default credentials. It changes the default SSH password and scans the network for other jailbroken iOS devices to infect. It changes also the wallpaper of the device to Rick Astley's photo - a pop singer of 80's (see Figure 7).



Figure 7. Infection with iOS_KEE

E. 2010 The Smartphone Era

Smart phones having advanced features like touch screen displays, advanced web browsers, app market support etc. became target of mobile malwares starting from 2010.

- **DroidSMS:** After the announcement of Android 1.0 in 2008, malware developers started targeting Android platforms. DroidSMS [23], as the first Android malware appeared in 2010, introduces itself as a movie player but its main objective is sending premium SMS messages for financial gains. As shown in Figure 8, DroidSMS requests permission for sending SMS messages during installation.

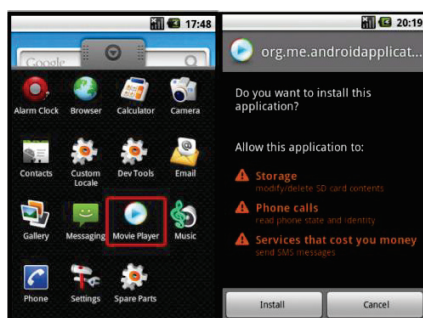


Figure 8. Infection with DroidSMS

- **DroidSnake:** DroidSnake [24] is the first identified Android spyware in the history. It spread over Google's official Android Market and disguised as a well-known snake game. In the background, it spies GPS coordinates and forwards them through Internet. As shown in Figure 9, DroidSnake requests access to location information during installation.

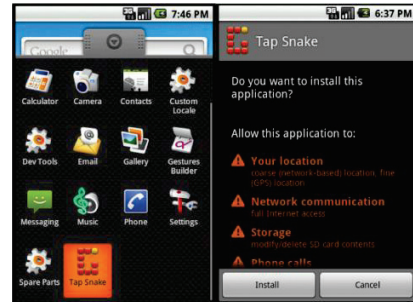


Figure 9. Infection with DroidSnake

- **ZitMo/ZeuS in the Mobile:** ZitMo [26] is the mobile part of the ZeuS trojan, which steals information from computers. ZitMo targets all Android, Blackberry RIM, iOS and Symbian platforms. It poses as a password security application, but it steals one-time SMS tokens for online banking [25][53]. If the PC user tries to login to his bank account from a ZeuS infected machine, a pop-up appears and the user is convinced to download so called mobile security app in order to progress. Once the ZitMo is downloaded, SMS messages that are coming from the bank are redirected to the attacker.

- **LBTM:** LBTM [28] is an iOS application that shows funny jokes and texts in French. But when a user taps to the opening adds splash screen it calls premium services and causes high costs for the device owner. The important reality about LBTM malware is that not only jailbroken but also original devices are threatened by LBTM since it was downloaded from the official iOS App Store.

- **Geinimi:** Geinimi [29] is the first Android malware with botnet capabilities. It was created by repackaging contents of legitimate applications with malicious codes. It basically opens a backdoor and transmits sensitive information from the device to a remote server. These repackaged apps are distributed over unofficial third party application stores.

F. 2011 - 2012 The Rise of Smartphones

Between 2011 and 2012 the number of mobile malwares was exploded with the increase of smartphone users, especially Android users. Third party stores were filled with pirate and repackaged versions of legitimate free and paid apps. Malwares gained more advanced features and botnet capabilities[22] [53].

▪ **DroidDream/DroidKungFu:** DroidDream [30] is one of the first instances of advanced mobile malwares. It targets Android platforms. It was available in the official Android market by impersonating legitimate applications. It uses two Android vulnerabilities in order to gain root privileges. It also uses code obfuscation to hide itself and exploits encryption to communicate with the command and control server.

DroidDream consist of two payloads. The first payload tries to root the device and download the second payload, which collects all device information and sends them to the C&C server. The second payload is also capable of downloading and installing anything that the C&C managers want. DroidKungFu [38][53] is also another mobile malware that uses the same exploits to get root privileges. The main difference is that DroidKungFu applies anti-virus evasion techniques and successfully evades antivirus applications.

▪ **Arspsam/Alsalah:** Alsalah [31] is another interesting malware in the mobile malware history. It is the first hacktivist mobile malware in the wild. It targets Android platform and sends spam SMS messages to contacts of the infected device. The interesting thing about the spam SMS messages is its content which contains a link about Mohamed Bouazizi's protest who set himself on fire by the Arab Spring events. In addition, Alsalah checks the location and shows the human rights violations report if the device is located in Bahrain.

▪ **Find And Call:** Find and Call [32] is another malware that spreads over official application stores. It targets both Android and iOS platforms and sends its download link to each contact in the contact list. Additionally, it sends the contacts list to a remote server. It is one of the malwares, which bypassed the iOS App Store security controls.

G. 2013 - 2014 More Advanced Devices and Malwares

After 2013, mobile malwares became more financial gain oriented. Money stealers, banking trojans and premium service abusers became very widespread.

▪ **Riskware/Tracer:** Tracer [33] is a commercial spyware that is sold for \$79 annually. It affects all Android, iOS, Blackberry RIM and Symbian platforms. It targets especially rooted and jailbroken devices. Tracer can access to all sensitive information like phonebook, SMS messages, e-mails, application information, location, device information, photos etc. It has the capability of downloading and installing applications and recording phone calls. It can also access to Whatsapp, Skype, Facebook chats and Facebook photos. Infected devices can be managed via a HTTP control panel (see Figure 10).

▪ **OBAD:** OBAD [34] is a trojan, which uses 0-day vulnerabilities to exploit and gain high privileges, and adds itself to the device administrator's list. As a result, mobile anti-virus applications cannot detect OBAD and it cannot be uninstalled or deleted from the device. It contains anti-decompile and anti-VM controls, therefore static and dynamic analysis become very difficult task. It can retrieve sensitive data, install application, send SMS, collect device information,

and even execute shell commands by communicating with a command and control server.



Figure 10. Infection with Tracer

▪ **Waller:** Waller [36] is a trojan that sends SMS messages to premium services. Additionally, it steals funds from QIWI which is an e-wallet technology powered by VISA. Waller sends SMS messages to check the balance of QIWI, forwards the returning SMS to the command and control server and steals money from QIWI. It also has capabilities of downloading and installing applications, intercepting SMS messages, surfing web pages.

▪ **Stealer:** Stealer [37] is another instance of botnet mobile malware. It became the leader in terms of number of infected devices. It was detected almost all around the world. It changes the content of the app according to the country of residence.

▪ **OldBoot:** OldBoot [48] is the first known Android rootkit in the history. It infects boot partitions. Since none of the commercial anti-virus applications have access to boot partitions, they classify GoogleKernel as a malware as shown in Figure 11.

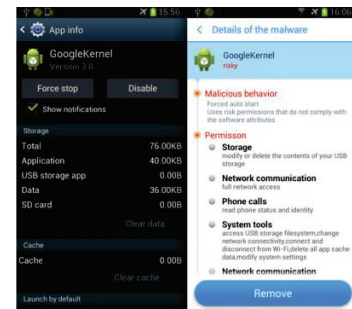


Figure 11. Infection of Bootloader with OldBoot

▪ **Dendroid:** Dendroid [39] is a remote access trojan with advanced malware capabilities. It also has voice and video recording feature by using microphone and camera of the device. It communicates with a remote C&C server over Internet. The trojan and its C&C server are sold for around 300\$ in the black-market. Dendroid hides itself within a legitimate app called Parental Control in Google Play Store.

▪ **Koler/Police Locker:** Koler [40] is ransom mobile malware and the mobile version of Netra PC malware. It locks mobile devices and requests \$300 to unlock. It shows a message as if

it comes from a police department. It can change the content of the message according to the country of residence.

- *Unflod Baby Panda*: This is the most recent iOS malware that affects jailbroken iOS devices [41]. The malware steals Apple-ID and password by hooking SSL buffer. The interesting part of the malware is the developer signature of the malware. It is signed by a registered iOS developer from China. It is considered that the malware developer signed the binary with a stolen certificate.
- *Malnotes*: Malnotes [42] is the first proof of concept Google Glass malware developed by two graduate students for an academic study. It takes a photo every ten minutes without the knowledge of wearers. It is the first instance of wearable malwares (called wearwares) in the history.
- *DSEncrypt*: DSEncrypt [43] is a spyware that comes along with an encrypted malware inside of its assets folder. It pretends to be a legitimate app from Google Play Store. It decrypts the encrypted malware part at runtime and asks for device administrator privileges in order to run with high privileges. It creates a background service, which steals bank accounts, signing certificates, and SMS messages that might contain sensitive information like one-time security tokens.

IV. FUTURE ASPECTS OF MOBILE MALWARES

With the evolution of new mobile platforms and new mobile device types, mobile malwares will have new targets in the near future. Spreading malwares through application markets is very attractive for black-hat hackers. The new Blackberry OS 10 and Windows Phone 8 technologies support application markets similar to app markets of iOS and Android platforms. Therefore, they would become more targets in the near future. In addition, Blackberry OS 10 supports installing and running Android applications on Blackberry devices. Using this feature, Android malwares can target Blackberry devices as well. There are already commercial tools [44] to manage mobile bot networks for Android and Blackberry devices. With the help such tools, cyber criminals aiming financial benefits can hijack incoming SMS messages for online banking security tokens and access to all sensitive data (e.g. SMS, call history, contacts, IMEI number, OS details).

In addition to mobile smart phones, there exist today other types of smart electronic devices at our homes, which are especially Android-based devices. Android radio, Android refrigerator, Android oven etc. are only some examples. In the future, these devices would be targets of mobile malwares as well. Being infected by a malware, such devices would function abnormally and even cause material damage within their environments. A smart oven whose functionality is manipulated by a malware may lose its control over the heating function and this might trigger destructive fire.

Similarly, more and more wearable smart devices like watches, glasses, shirts etc. will exist in our daily lives. Apple introduced its smart watch, called Apple Watch, in September 2014. Google has already released the wearable smart Google Glass and Wear. Apple has published the health kit APIs [49] which allows health and fitness apps to share their data with

other apps. Wearable medical devices will exploit this Health APIs in the future. On the other hand, these wearable devices would be targets of cyber-attacks and even threaten health and lives of people. A proof of concept attack has been already shown on wearable Google glass [42].

Developing mobile malwares have been so far very attractive especially for cyber criminals who try to gain financial benefits from their victims. But intelligence agencies in the world are also interested in malwares. In 2011, the Chaos-Computer-Club members [45] discovered the Staatstrojaner, which was installed secretly on suspects' computers in Germany by the government agencies to wiretap Internet telephony [46]. Further security analysis showed that the trojan enables remote controlling of the target computers, capturing screenshots and even running arbitrary extra code on victim computers. It is also a known fact that NSA is keen on sniffing the whole communication channels in the world. It was recently revealed that NSA planned to infect millions of computers by using automated systems [47]. Since hijacking incoming audio and video calls are very valuable information for intelligence agencies, more governmental institutions would be active to develop mobile malwares and infect mobile users for their spying activities.

While mobile malwares become more sophisticated, detection techniques of malwares evolve as well. There exist already several studies to identify mobile malwares at runtime [50],[51],[52]. With the development of smart wearables and smart electronic devices, this research topic will be studied more intensively in the future.

V. CONCLUSION

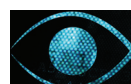
Since mobile devices and smart phones have become more popular for individual users in the last ten years, various mobile malwares targeting mobile platforms were developed and seen in the wild. In this paper, we explained the evolution of mobile technologies and mobile malwares targeting these technologies.

Comparing all mobile technologies and operating systems, Google's Android is today the most targeted platform by mobile malwares. Especially third party application markets by which Google has no control are used to spread applications with malicious codes.

In addition to smart phones, there exist today already smart home electronics devices like Android radio, Android refrigerator, Android oven and smart wearables like Google glass, Google wear, Apple Watch etc. In the near future, more smart devices equipped with mobile operating systems and especially with Android will exist. In parallel to this development new mobile malwares would target such smart home devices, manipulate their functionality and even cause financial and physical damages.

REFERENCES

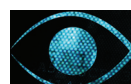
- [1] "Malware" in Wikipedia. Available: en.wikipedia.org/wiki/Malware
- [2] "The very first mobile malware". Kaspersky Labs. Available: <http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir>



- [3] "Mobile Malware Evolution, Part 5", SecureList. Available: <http://securelist.com/analysis/malware-evolution-monthly/36485/mobile-malware-evolution-part-5/>
- [4] "Android Malware". Kaspersky Labs. Available: http://www.kaspersky.com/au/images/kaspersky_lab_infographics_android_malware_growth-40-147099.png
- [5] "Android Threats in 2012". Kaspersky Labs. Available: http://www.kaspersky.com/au/images/Kaspersky_Lab_Infographics_Android_Threats_in_2012-40-188104.png
- [6] "Mobile Malware Evolution: 2013". SecureList. Available: <http://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/>
- [7] "iOS Malware Does Exist". Fortinet Blog. Available: <http://blog.fortinet.com/iOS-malware-do-exist/>
- [8] "Cybersecurity Trends for 2014 - Trend 3 - Wearable Malware". Blue Coat blog. Available: <https://www.bluecoat.com/blogs/2014-03-29/cybersecurity-trends-2014-trend-3-wearable-malware>
- [9] "Cabir". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/archive/malware/symbos_cabir.a
- [10] "Duts". F-Secure. Available: www.f-secure.com/v-descs/dtuts.shtml
- [11] "Trojan.Mos". Symantec. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2004-081009-2533-99
- [12] "Skulls". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/archive/malware/symbos_skulls.A
- [13] "Bluetooth-Worm: Lasco". F-Secure. Available: http://www.f-secure.com/v-descs/lasco_a.shtml
- [14] "SYMBOS_PBSTeal.A". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/archive/malware/symbos_pbsteal.a
- [15] "Commwarrior". F-Secure. Available: <http://www.f-secure.com/v-descs/commwarrior.shtml>
- [16] "Bootton". F-Secure. Available: http://www.f-secure.com/v-descs/trojan_symbos_bootton_a.shtml
- [17] "SYMBOS_CARDBLK.A". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/archive/malware/SYMBOS_CARDBLK.A
- [18] "Trojan:Java/Redbrowser.A". F-Secure. Available: http://www.f-secure.com/v-descs/redbrowser_a.shtml
- [19] "SYMBOS_FLEXSPY.A". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/archive/Malware.aspx?language=au&name=SYMBOS_FLEXSPY.A
- [20] "Apple Reports First Quarter Results". Apple Press Info. Available: <http://www.apple.com/pr/library/2009/01/21Apple-Reports-First-Quarter-Results.html>
- [21] Leavitt, N. "Mobile phones: The next frontier for hackers?", IEEE Computer 38, 2005, pp.20-23
- [22] A. Arabo, B. Pranggono, "Mobile Malware and Smart Devices' Security: Trends, Challenges and Solutions," Proceedings of the 19th International Conference on Control Systems and Computer Science (CSCS), 2013
- [23] "DROIDSMS". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/malware/androidos_droidsms.a
- [24] "ANDROIDOS_DROISNAKE.A". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/malware/androidos_droisnake.a
- [25] "Trojan.Zbot". Symantec. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99
- [26] "Zeus-in-the-Mobile for Android". SecureList. Available: <http://securelist.com/blog/virus-watch/29258/zeus-in-the-mobile-for-android-10/>
- [27] "IOS_IKEE.A". Trend Micro Threat Encyclopedia. Available: http://about-threats.trendmicro.com/us/malware/ios_ikee.a
- [28] "LBTM!iPhoneOS". FortiGuard Center. Available: <http://www.fortiguard.com/encyclopedia/virus/#id=2102975>
- [29] "Android.Geinimi". Symantec. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99
- [30] "DroidDream: How it Works". Lookout. Available: <https://blog.lookout.com/blog/2011/03/02/android-malware-droiddream-how-it-works/>
- [31] "Arspam". Symantec. www.symantec.com/security_response/writeup.jsp?docid=2011-121915-3251-99&tabid=2
- [32] "Find and Call app becomes first trojan to appear on iOS App Store". Ars Technica. Available: <http://arstechnica.com/apple/2012/07/find-and-call-app-becomes-first-trojan-to-appear-on-ios-app-store/>
- [33] "TRracer - commercial spyware". Contagio Mobile. Available: <http://contagiominidump.blogspot.com.tr/2013/07/trracer-commercial-spyware-pua-samples.html>
- [34] "Android OBAD". Comodo Technical Report. Available: www.comodo.com/resources/Android_OBAD_Tech_Reportv3.pdf
- [35] "Yeni Nesil Android Zararlı Yazılımı". TÜBİTAK-BİLGEM Ulusal Bilgi Güvenliği Kapısı. Available: <http://www.bilgiguvencigi.gov.tr/mobil- cihaz-guvenligi/yeni-nesil-android-zararli-yazilimi-obad.html>
- [36] "Android Trojan Waller Sends Premium SMSs, Steals Money from QIWI Wallets". Softpedia. Available: <http://news.softpedia.com/news/Android-Trojan-Waller-Sends-Premium-SMSs-Steals-Money-from-QIWI-Wallets-435898.shtml>
- [37] "New threat: Trojan-SMS.AndroidOS.Stealer.a". SecureList. Available: <http://securelist.com/blog/incidents/59384/new-threat-trojan-sms-androidos-stealer-a/>
- [38] Xuxian Jiang. "Security Alert: New DroidKungFu Variants Found in Alternative Chinese Android Markets". July 2011. Available: <http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu2/>
- [39] "Dendroid malware can take over your camera, record audio, and sneak into Google Play". Lookout Blog. Available: <https://blog.lookout.com/blog/2014/03/06/dendroid/>
- [40] "Police Locker land on Android Devices". Blog: Malware don't need Coffee. Available: <http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.html>
- [41] "iOS Malware Campaign Unflod Baby Panda". SektionEins Blog. Available: <https://www.sektioneins.de/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html>
- [42] "Using your eyes to spy". Mustang News. Available: <http://mustangnews.net/using-your-eyes-to-spy/>
- [43] "What are you doing? - DSEncrypt Malware". FireEye Blog. Available: <http://www.fireeye.com/blog/technical/2014/06/what-are-you-doing-dsencrypt-malware.html>
- [44] "Cybercriminals release new commercially available Android/ BlackBerry supporting mobile malware bot". Webroot Threat Blog. www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/
- [45] Chaos Computer Club. Available: <http://www.ccc.de>
- [46] "Staatstrojaner". Wikipedia. Available: http://en.wikipedia.org/wiki/Chaos_Computer_Club#Staatstrojaner
- [47] "How the NSA Plans to Infect 'Millions' of Computers with Malware". The Intercept News. Available: <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware>
- [48] "Oldboot: the first bootkit on Android". 30 Mobile Security Blog. Available: <http://blogs.360.cn/360mobile/2014/01/17/oldboot-the-first-bootkit-on-android/>
- [49] Apple HealthKit. Available: <https://developer.apple.com/healthkit/>
- [50] M. Becher, F. Freiling, "Towards Dynamic Malware Analysis to Increase Mobile Device Security", in Proc. GI Sicherheit, 2008, pp.423-433.
- [51] Lok Kwong Yan, Heng Yin, "DroidScope: Seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis", Proceedings of the 21st USENIX conference on Security symposium, 2012, Bellevue, WA.
- [52] T. Bläsing, L. Batyuk, A. Schmidt, S.A. Çamtepe, and S. Albayrak, "An Android Application Sandbox system for suspicious software detection", Proceedings of the MALWARE, 2010, pp.55-62.
- [53] Y. Zhou, X. Jiang, "Dissecting Android Malware: Characterization and Evolution," Proceedings of the 33rd IEEE Symposium on Security and Privacy (Oakland 2012), San Francisco, CA, May 2012

M.Öğuzhan Topgöl is a senior security researcher at TÜBİTAK-BİLGEM Cyber Security Institute. He is a Ph.D student of Medipol University Electrical and Electronics Engineering department. His research interests include malware analysis, mobile security and security testing.

Emin İslam Tath is Assistant Professor with the Department of Electrical and Electronics Engineering, İstanbul Medipol University, İstanbul, Turkey. He received the Ph.D. degree in computer science from the University of Mannheim (Germany) in 2009. He worked as information security expert by different security consultancy firms between 2009 and 2013. His research interests include mobile security, web application security, security testing, security management and privacy.



Call of Duty: Can Turkey Benefit from Crowd-Sourced Serious Games to Strengthen Its Cyber Security Capabilities?

Ümit Tellioğlu, Bilal Kartal, Mehmet Şimşek, Ömer Eryılmaz

Abstract—The software verification process is cumbersome and currently requires highly trained experts and considerable time. This process is critical to eliminate bugs and to strengthen software systems. Military software systems are of utmost importance for national security. One way to improve this verification phase is to use a crowdsourcing paradigm to strengthen software systems. Turkey has an increasing number of the Internet users and online game players who spend more time per game session than the average user. In this paper, we propose using crowd-sourced serious games (CSSGs) to improve Turkey's national cyber security capabilities and examine the stakeholders of Turkey needed for a CSSG project.

Index Terms—Crowd-Sourced Serious Games, Cyber Security, Software Formal Verification

I. INTRODUCTION

Playing is an essential part of the human experience. It results in learning the required activities of life at an early age, and it is enjoyable. Humans have used games throughout history as an instrument of play activity. With the improvement of technology, the game-playing process has digitalized and become more immersive. Humans have created digital machines that run virtual software to interact, play, and enjoy. After the Internet boom, people had the opportunity to connect with others throughout the world. As a result, people have spent billions of hours dedicated to online computer games. Trends show that the time spent playing online games will continue to increase. Consequently, L. Von Ahn [1] developed the idea of *games with a purpose*, claiming that it may be beneficial for humanity if billions of game playing hours can be harvested to solve problems.

The aim of crowd-sourced serious games (CSSGs) is to harness non-expert citizens to solve scientific problems for which scientists do not have adequate resources as we will present many existing software systems proving the insufficiency of experts. Considering the aim of generating a side product from game playing, the term "citizen science" is introduced that aims to direct non-expert people into real-life scientific problem solving [2]. At that point, however, the issues arise as to how we benefit from the crowd's power for

a subject that is completely unfamiliar to them. The solution is to place a converter from the game to an algorithm between non-expert citizens and science, which will attract regular people, transforming them into citizen scientists [2]. There have been applications of CSSGs with different purposes such as *EyeWire*, *Phylo* and *Foldit*. For instance, non-expert *Foldit* players helped to solve the structure of an AIDS related enzyme within three weeks [3]. Scientists had sought to find a solution to this problem for ten years. In addition, *EyeWire* players have contributed to a complex neuroscience research on a problem remaining unsolved for 50 years [4].

As a developing country, Turkey has produced national technological systems that are highly software dependent, and CSSGs can be very beneficial as a tool to reduce software-caused vulnerabilities. The growth of technology usage is fast all over the world, and the situation is similar for Turkey as well. Technology usage and the ratio of people connecting to the Internet have been increasing in the country. With this progress, technological systems such as e-government and National Judiciary Informatics Systems (UYAP in Turkish) have been developed and are now being actively utilized. Moreover, Turkey has begun producing critical national military vehicles such as T129 ATAK Helicopter, Altay Tank, ANKA UAV and national warship (Milgem Project). All of these critical systems are potential targets for cyber-attacks. One of the important processes for vulnerability prevention of these critical systems is performed through software verification which is a possible application area for crowdsourcing.

Under these circumstances, a comprehensive strategy to strengthen the national-cyber-security by using national resources is imperative for Turkey. As an initial step in this direction, we will hypothesize two relational questions within this paper:

- 1) Is it possible to use CSSGs to improve cyber security?
- 2) Does Turkey have enough resources or stakeholders to harness CSSGs aimed at cyber security?

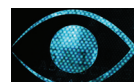
Organization The rest of this paper is organized as follows. Section 2 highlights the related work on this research topic and Section 3 presents existing software systems with discussion of military software usage. In Section 4, we show Turkey's stakeholders of a CSSG project. Section 5 concludes the paper, and we present future research directions in the final section.

Ümit Tellioğlu, Turkish Military Academy, The Defense Sciences Institute, Bakanlıklar, Ankara-Turkey, email: umittelli@gmail.com

Bilal Kartal, Turkish Military Academy, Computer Engineering Department, Bakanlıklar, Ankara-Turkey, email: blkrtl.cs@gmail.com

Mehmet Şimşek, War Colleges Command, Army War College, Yenilevent, Istanbul-Turkey, email: msimsekfg@gmail.com

Ömer Eryılmaz, War Colleges Command, Army War College, Yenilevent, Istanbul-Turkey, email: omereryilmaz83@gmail.com



II. RELATED WORK

In this section, we will present some discussion of crowdsourcing and software verification. Additionally we will show how crowdsourcing can advance cyber security through different applications.

A. Crowdsourcing

Crowdsourcing has been a game changer for solving difficult problems with a mass of ordinary, untrained people. Howe used “crowdsourcing” as a term with different application perspectives [5]. The range of application possibilities is huge, extending even to capabilities of changing how the Web works by pushing content creation and management activities to its ordinary users in Web 2.0 [5].

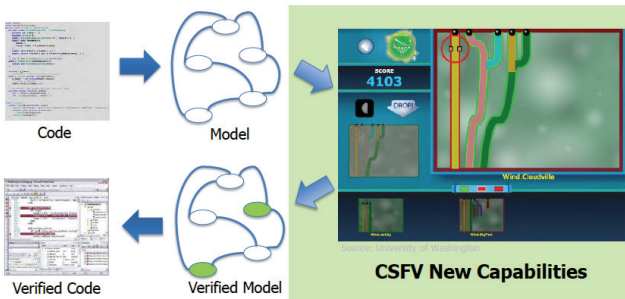


Fig. 1. An example of a converter model from game input to software verification process using a CSSG. [6]

The crowdsourcing approach employs a large number of agents, i.e., untrained people, with different reliability to accomplish a specific task. Therefore, statistical reliability requires a large number of agents in the system so that the impact of the outliers will be reduced. For most of the CSSGs, there will be a middle transformer layer that takes untrained ordinary people’s input and converts it to a solution, e.g., see *Foldit*, [3]. Yet, there are many other application domains of crowdsourcing. For example, it can be used for emergency response after disasters by creating a collective system [7]. However, there are also harmful applications of this technique when applied in a different fashion. For example, a study [8] analyzing the contents on the web portals in China revealed the existence of an application called *Human Flesh Search*. In this application [8], participating web users perform a collaborative cyber surveillance to find other people, or to obtain specific information about them through the portal. It is reported that this search generally results in harmful effects on the community.

One other application of crowdsourcing is specifically for business purposes. Companies can take advantage of the diverse perspective of the crowd to collect new ideas for their business strategies [9].

Finally, Mechanical Turk is a very widely used tool that is a great proof of concept example for crowdsourcing. In this case, individuals and businesses are able to push tasks to a task pool of compensated crowd workers. This way, businesses have their tasks completed and users are paid for the assistance they provide.

B. Software Verification

The software verification aims to guarantee correctness of the program as a disciplined phase within software engineering. This process ensures that the software performs only the tasks for which it is designed with no unintended tasks, which might be malicious [10]. In terms of cyber defense, the latter case, i.e. making sure that the software does not perform any unintended tasks is crucial. Non-developers should test software during verification phase [10], i.e. the exact step that we propose to be pushed to crowd. This improves the verification.

To have an overview of widely used software, let’s examine an operating system. Linux is one of the best-known and most popular open source operating systems and it has many derivatives with different distributions. According to the report shown in [11], five-computer science researchers examined 5.7 Million lines of *Linux* source code in four years. They concluded that the *Linux 6* kernel code was better and more secure than that of most proprietary software [11]. Throughout the study, the researchers worked on 2.6 *Linux* production kernel, which was used by Red Hat, Novell, and other popular vendors, and found 985 bugs in 5.7 million lines of code. On the other side, according to Carnegie Mellon University’s Cy-Lab Sustainable Computing Consortium, commercial closed source software have 20 to 30 bugs for every 1,000 lines, resulting in 114,000 to 171,000 possible bugs in the 40 million lines of code in *Windows XP* [11].

Software bugs can cause serious problems. First, systems using the software may stop working or fail to achieve its intended results, which historically has caused space shuttle crashes, millions dollars of financial loss for companies, fatal mistreatment of patients, power outages in cities and other serious incidences [12] [13]. If military systems fail, the results can be more tragic. For example, during the First Gulf War, the Patriot air defense system failed to prevent an incoming missile because of a bug in the software and caused the death of 28 soldiers [14]. Another example of a software bug resulted in death of 29 people in a Chinook helicopter crash [15].

Second, adversaries can exploit vulnerabilities caused by bugs. Hackers mostly use software bugs and *zero* day bugs to exploit systems. One of the most dangerous incidences from a global perspective is the “heart bleed bug” [16]. In this case, hackers were able to reach encrypted data by using this bug, which had impacted the *OpenSSL* cryptographic software library, i.e. the main security provider for quite a while. Hacking of military systems and vehicles is also possible. In particular, hackers have targeted unmanned vehicles (UVs) as they hacked a UAV in Afghanistan [17]. One crucial step to detect these vulnerabilities in software is through formal verification.

Considering the increase in use of technology in daily life and number of bugs in these technology systems, the crucial need to improve verification process to make these systems safer is very clear.

C. Cyber Security through Crowdsourcing

As e-services are increasingly used for government applications, the need to protect the services also increases as each bug is a possible chance for exploitation by malicious users. Apart from conventional testing processes to strengthen software, each country can use crowd-sourced applications in order to improve security of e-service software. For example, Paulhamus et al. [18] proposed a proof of concept game called *Flux Hunter* which is played in a network and utilizes crowd-sourcing to identify malicious web-sites for cyber security. The game aims to harness the employees' play experience to identify cyber threats. As we described earlier, in this type of application, there is a transformer layer that takes game playing input and feeds it into the problem-solving algorithm. From this point, *Flux Hunter* presents pictures to players that in fact represent some camouflaged network information, and the players must choose images based on their perception of threat. Also, the players are trained for the game with supervised images and sample answers beforehand.

Another application that uses crowdsourcing along with machine learning techniques is presented in [19], which allows personal web users to identify scam web sites to prevent any phishing type of attack. Through a custom module, users can post and share information about the websites and rate them, and ultimately logistic regression is applied to classify the websites. There are several other applications where crowd-sourcing can enhance the security of software to defend against cyber threats.

III. BACKGROUND ON EXISTING SOFTWARE SYSTEMS

Software sold on the market can contain up to 5 bugs per thousand line of code as reported in [20]. To reduce the number of bugs in software, verification needs to be performed in an improved and faster fashion. However, verification is a complex process that can be performed by a limited number of highly trained experts, leading to insufficient resources to verify a large number of software [21]. Also, while the line of code produced in the world has been increasing very rapidly, the number of experts for verification phase has not followed the same trend [21]. One study [22] suggests interesting code production figures, i.e. there are 6 million software developers in the world and they produce 300 millions lines of code weekly or 15 billion lines of code yearly. Thus, if all verification experts in the U.S. worked only on *Windows 8*'s source code to formally verify and find even 25 predefined vulnerabilities, it would take them more than 30 years [21]. This demonstrates just how time consuming the process is and insufficient supply to solve the problem in a traditional way. Additionally, there are several types of software, including operating systems, commercial off-the-shelf (COTS), and others, which further complicates the issue. When we look at the Table I, we can see that the size of the software needed to be verified is huge.

Verification is also critically important for military systems. Table I shows that military systems such as jet fighters, missiles, and future combat systems have software systems made of millions of lines of source code. Table II also supports

TABLE I
LOCs OF A GROUP OF SOFTWARE [23], [6]

Name	Lines of Code (LOC)
Windows XP	40 M
Windows 7	40 M
Linux 3.1	15 M
Mac OS X 10.4	86 M
Debian 5.0 (all software in package)	324 M
Android OS	12 M
Microsoft Office (2013)	45 M
F-22 Raptor Jet Fighter	1.7 M
F-35 Fighter	24 M
Patriot PAC-3 Missiles	Close to 2 M
US Army's Future Combat System	63.8 M
Hubble Space Telescope	2 M
Google Chrome (2011)	5.4 M
Boeing 787 Dreamliner	6.1 M
Firefox	9.7 M
Chevrolet Volt (Electric Car)	10 M
Apache Open Office	23 M
MySQL	12.5 M
Software in typical new car, 2013	100 M
Healthcare.gov	500 M

TABLE II
SOFTWARE DEPENDENCE OF MILITARY AIRPLANES BY YEARS [24]

Military Aircrafts	Year	Percentage of Functions Performed in Software
F-4	1960	8
A-7	1964	10
F-111	1970	20
F-15	1975	35
F-16	1982	45
B-2	1990	65
F-22	2000	80

this by demonstrating the increased reliance on software of jet fighters over the years. It is obvious from the trend in Tables I and II that this reliance will keep increasing due to the shift to both unmanned air vehicles and usage of artificial intelligence supported systems in battlefield. Thus, as the produced code continues to increase in volume, the need for alternative ways to handle verification will be more urgent.

Defense Advanced Research Projects Agency (DARPA) has been conducting the Crowd Sourced Formal Verification (CSFV) project since 2011, and developed five CSSGs to initially verify some small open source software [20]. The overall aim of the project is to find a way to formally verify software used in complex military systems without heavily relying on the insufficient amount of software verification experts. The games are hosted in a single portal called Verigames [20]. A software company named Topcoder, which develops software by using the crowdsourcing concept is forming this portal.

IV. STAKEHOLDERS OF A CSSG PROJECT IN TURKEY

As we stated in our hypothesis questions, harnessing crowd-sourcing models embedded in computer games in order to solve different problems is a new research trend similar to many applications, e.g., *EyeWire*, *Phylo*, *Foldit*. Moreover, a recent study [25] shows that Turkish game players consume more time for online games than world average (see Table III). This supports our hypothesis in the sense that Turkey can gain a great deal of benefits from CSSGs.

Three stakeholders are required to successfully create a project that formally verifies software by using CSSGs. They are game players, developers, and software verification experts. In this section, we will examine Turkey's current status related to these three stakeholders.

A. Game Players

The role of the gamers is crucial for CSSGs because without gamers, crowdsourcing projects cannot realize their goals. In addition, each player has different motivation to play games [27]. Recently, it is shown in [27] that CSSGs often have difficulty finding enough players, since the nature of the game is linked to specific problem solving rather than the players' personal pleasure. Therefore, in order to incentivize many Turkish players, there is need to find a common motive such as patriotism to support Turkish cyber defense capability. In the current study, we will examine Turkish game players. However, future research should define the possible motivational factors among Turkish players. Also, if the games are enjoyable, they will attract players from all over the world.

Figure 3 shows the data of Turkish game players based on the game platforms. CSSGs have been developed for various platforms. For example, *Foldit* is downloadable for PCs, *Xylem* is mobile (for iPads), and *EyeWire* and *Stormbound* are browser based online games. Also, one important factor here is to recognize the leading medium for game playing, e.g. social networks, high connectivity between the users provided by social networks should be utilized to increase preference for CSSGs. On the other hand, the ratio ranges from 12.8% to 22.3% of the overall population across the different platforms for Turkish players and Table III clearly shows that Turkish players tend to spend on average more time playing social, casual, and mobile games than any other countries' players in the world.

TABLE III

PLAYERS DATA OF A LIST OF COUNTRIES AND THE WORLD AVERAGE [25]

	Session Time Avg.	Avg. Session Count	Avg. Total Play Time
Turkey	45.9 mins	15.4	705 mins
Japan	30.4 mins	22.5	683 mins
South Korea	28.9 mins	17	492 mins
U.S.	21.9 mins	6.5	142.8 mins
Russia	23.2 mins	3.3	76.2 mins
China	2.7 mins	1.3	16.8 mins
World Avg.	26.7 mins	5.9	157.6 mins

In addition, CSSG projects can benefit from the increasing popularity of mobile devices in Turkey. Mobile games' complexity and quality get closer to PC or console games with the improved capabilities of the mobile devices (smart phones and tablet computers). Figure 2 briefly shows the popularity of mobile devices in Turkey. A report in 2013 showed that 19% of all phones sold in the country are smart phones [28]. In addition, 38% of smart phone owners use applications in their smart phones, and 32% of those phone owners play mobile games via those devices [28]. Moreover, tablet computers connected to the Internet have exceeded 1.5 million.

The Ministry of National Education (MONE) plans to gift tablet computers to all students and teachers below university level and has already distributed more than 700,000 of them [29]. Therefore, the number of tablet computers in Turkey is increasing. Although MONE currently restricted usage of game type applications from given tablets [29], if developers can produce education purposed games such as *Xylem*, this would be beneficial for both the students and the CSSG project. Of course, this is a future project that educators and pedagogues would need to discuss.

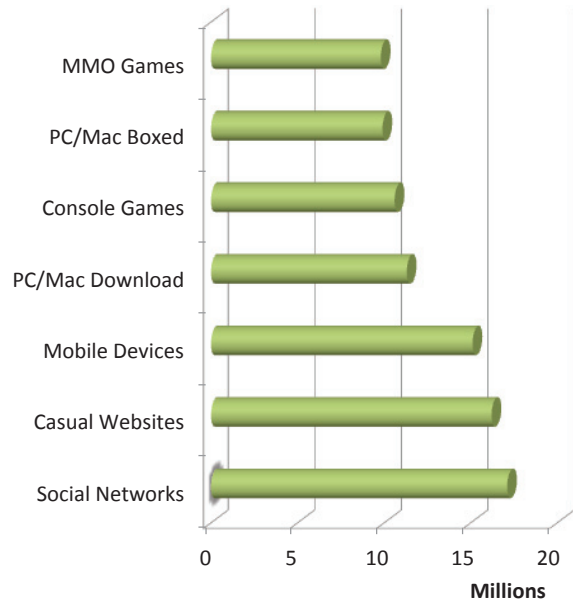


Fig. 3. Gamers in Turkey by game type [30]

B. Game Developers

The second stakeholders are game developers, so Turkey needs experts in game creation to achieve the ultimate purpose. Upon searching the literature, we saw that a Turkish gaming company, Peak Games, has developed social, mobile, and online browser games. It is a leading company not only in the Middle East, but globally. Table IV compares the number of players for Peak Games with the world's most popular game developers [31]. In addition, mostly young entrepreneurs in Turkey are building start-up firms related to gaming each year. For example, in *e-tohum* database, which is a portal that

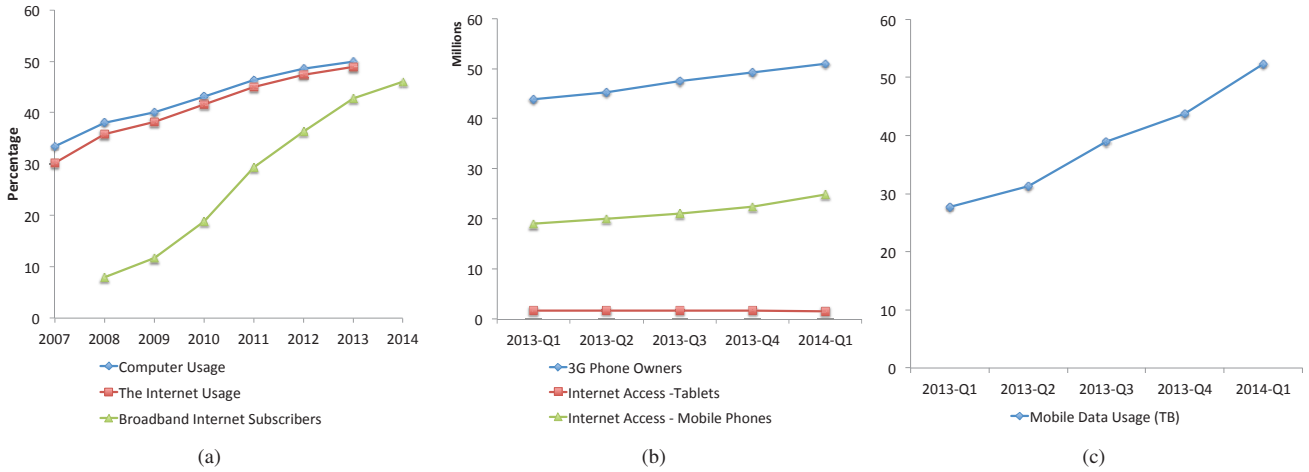


Fig. 2. (a) Computer usage and Internet access have steadily increased in Turkey in the last decade. Currently half of the population accesses it. (b) Similar to the trend worldwide, smart phone usage has also increased and tablet usage has exceeded 1.5 million, which justifies one of the reasons why games should be utilized for more important problems in addition to the joy of playing. (c) Mobile data usage also increases as it gets cheaper and more accessible by the public. [26]

gathers Turkish entrepreneurs, almost 20 electronic gaming start-ups have been recorded since 2010 [32]. Lastly, METU Animation Technologies and Game Development Center supports game developers, and young developers have created more than 200 games in Turkey since 2008 [33]. These recent events demonstrate that Turkey has also a young population who can contribute to the developing process.

TABLE IV
DAILY AND MONTHLY ACTIVE USERS (DAU, MAU) OF SOME LEADING MOBILE AND SOCIAL ONLINE GAME DEVELOPERS [27]

	DAU	MAU
Peak Games	11.8M	25M
Zynga	11.1M	292M
Storm8	4M	-
Glu Mobile	3.4M	29M
DeNa	-	16.9M
GREE	-	13.9M

C. Verification Experts

The third stakeholders are verification experts. Turkey currently has private sector firms working in software verification such as BEAM Technology and Altay Software. Universities can also support the private sector. For example, Koc University Multi-Core Software Engineering research center and METU Software Management Research Group both work on software formal verification. In addition, Turkey has individual academic experts on software verification.

V. CONCLUSION

Software bugs can cause huge risks for governmental, military (ATAK, MILGEM, ALTAY, etc.), and civilian systems (UYAP etc.) [20]. ATAK helicopters, Altay Tanks, Milgem, ANKA UAVs have been nationally developed. Each of these systems uses technology and inevitably run many lines of

software. Moreover, Turkey as a developing country is trying to build national military systems. According to the Turkish Department of Defense Strategy document, the country has also planned to increase the nationality of the current weapons systems and to produce high technology (meaning software dependent) systems such as air defense systems, unmanned sea-air-land vehicles, autonomous systems, satellites and cyber defense systems in medium and long-term [34]. All those indicate that software formal verification is critically important for Turkey.

In order to achieve these goals, National Cyberspace Security Policy, another cyber security document prepared in 2008 with the collaboration of government agencies, underlines the development of national cyber capabilities. It further stresses the importance of the protection of critical infrastructures and the cyber security of the public institutions.

In this research, we demonstrated that CSSGs are used to strengthen cyber security. One of them aims to formally verify software for which experts need source code. Obviously, source code is invaluable for critical systems. Therefore, to formally verify national software using domestic resources is invaluable, and CSSGs have the potential to support verification experts to achieve that goal. In addition, we examined Turkey's domestic assets that can provide resources for a crowd-sourced formal verification project. We propose that Turkey has capacity to conduct this project.

VI. FUTURE WORK

Crowd-sourced game projects have been conducted for less than a decade, and most of them have begun within the last two years. Consequently, we are unable to find a project that has completely achieved its goals, but some of them, such as *EyeWire* and *Foldit*, are progressing well. How to run a crowd-sourced game project, and how to incentivize the stakeholders for the project is subjects of future work.

Acknowledgment: We thank Yunus Küçük for his valuable feedbacks.

REFERENCES

- [1] L. Von Ahn, "Games with a purpose," *Computer*, vol. 39, no. 6, pp. 92–94, 2006.
- [2] A. Wiggins and K. Crowston, "From conservation to crowdsourcing: A typology of citizen science," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011, pp. 1–10.
- [3] M. J. Coren and F. Company, "Foldit gamers solve riddle of hiv enzyme within 3 weeks." [Online]. Available: <http://www.scientificamerican.com/article/foldit-gamers-solve-riddle/>
- [4] J. S. Kim, M. J. Greene, A. Zlateski, K. Lee, M. Richardson, S. C. Turaga, M. Purcaro, M. Balkam, A. Robinson, B. F. Behabadi *et al.*, "Space-time wiring specificity supports direction selectivity in the retina," *Nature*, vol. 509, no. 7500, pp. 331–336, 2014.
- [5] J. Howe, "The rise of crowdsourcing," *Wired magazine*, vol. 14, no. 6, pp. 1–4, 2006.
- [6] D. Dean, "Proceed and crowd-sourced formal verification," Nov. 2011. [Online]. Available: <http://www.dtic.mil/dtic/tr/fulltext/u2/a551949.pdf>
- [7] M. F. Goodchild and J. A. Glennon, "Crowdsourcing geographic information for disaster response: a research frontier," *International Journal of Digital Earth*, vol. 3, no. 3, pp. 231–241, 2010.
- [8] X. Pan, "Hunt by the crowd: an exploratory qualitative analysis on cyber surveillance in china," *Global Media Journal*, vol. 9, no. 16, pp. 1–19, 2010.
- [9] B. L. Bayus, "Crowdsourcing new product ideas over time: An analysis of the dell ideastorm community," *Management Science*, vol. 59, no. 1, pp. 226–244, 2013.
- [10] D. R. Wallace and R. U. Fujii, "Software verification and validation: an overview," *IEEE Software*, vol. 6, no. 3, pp. 10–17, 1989.
- [11] M. Delio, "Linux: Fewer bugs than rivals," 2004. [Online]. Available: <http://archive.wired.com/software/coolapps/news/2004/12/66022>
- [12] M. Lake, "Epic failures: 11 infamous software bugs," Sep. 2010. [Online]. Available: http://www.computerworld.com/s/article/9183580/Epic_failures_11_infamous_software_bugs?taxonomyId=18&pageNumber=2
- [13] K. Poulsen, "Software bug contributed to blackout." [Online]. Available: <http://www.securityfocus.com/news/8016>
- [14] A. Lum, "Verification software bug report patriot missile software problem." [Online]. Available: http://sydney.edu.au/engineering/it/~alum/patriot_bug.html
- [15] S. Rogerson, "The chinook helicopter disaster," *IMIS Journal*, vol. 12, no. 2, 2002.
- [16] "The heartbleed bug." [Online]. Available: <http://heartbleed.com/>
- [17] D. Cenciotti, "German heron drone hacked and crashed by taliban in afghanistan," Nov. 2013. [Online]. Available: <http://theaviationist.com/2013/11/13/heron-hacked-afghanistan/>
- [18] B. Paulhamus, A. Ebaugh, C. Boylls, N. Bos, S. Hider, and S. Giguere, "Crowdsourced cyber defense: lessons from a large-scale, game-based approach to threat identification on a live network," in *Social Computing, Behavioral-Cultural Modeling and Prediction*. Springer, 2012, pp. 35–42.
- [19] E. Fink, M. Sharifi, and J. G. Carbonell, "Application of machine learning and crowdsourcing to detection of cybersecurity threats," in *Proceedings of the US Department of Homeland Security Science Conference-Fifth Annual University Network Summit, Washington, DC*, 2011.
- [20] "Darpa." [Online]. Available: [http://www.darpa.mil/Our_Work/I2O/Programs/Crowd_Sourced_Formal_Verification_\(CSFV\).aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Crowd_Sourced_Formal_Verification_(CSFV).aspx)
- [21] D. E. Williams, "Gamers vs. hackers." [Online]. Available: http://www.verigames.com/Geek-May_2014-LEVEL_UP.pdf
- [22] J. Johnson, "The new industrial revolution (info-graphic)." [Online]. Available: <http://insights.wired.com/profiles/blogs/the-new-industrial-revolution>
- [23] D. McCandless, "Information is beautiful." [Online]. Available: <http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>
- [24] "Report of the defense task force on defense software." [Online]. Available: <http://www.acq.osd.mil/dsb/reports/ADA385923.pdf>
- [25] "Playnomics quarterly player engagement study." [Online]. Available: <http://www.playnomics.com/assets/Playnomics-Q1-2013-Engagement-Report.pdf>
- [26] "Turkey electronic communication sector quarterly report on market data," May 2014. [Online]. Available: http://www.tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik14_1.pdf
- [27] U. Tellioglu, G. Xie, J. Rohrer, and P. Charles, "Whale of a crowd: Quantifying the effectiveness of crowd-sourced serious games," to be published on the proceedings of 19th International Conference on Computer Games. [Online]. Available: <http://faculty.nps.edu/xie/papers/whale-effect-games14.pdf>
- [28] "The mobile consumer a global snapshot," Feb. 2013. [Online]. Available: <http://www.nielsen.com/content/dam/corporate/uk/en/documents/Mobile-Consumer-Report-2013.pdf>
- [29] "Fatih project." [Online]. Available: <http://fatihprojesi.meb.gov.tr/tr/icerikincele.php?id=6>
- [30] "Number of gamers in turkey in 2012, by platform." [Online]. Available: <http://www.statista.com/statistics/234793/number-of-gamers-in-turkey-by-platform/>
- [31] D. Takahashi, "Peak games dominates mobile social games in the middle east and turkey," Oct. 2013. [Online]. Available: <http://venturebeat.com/2013/10/15/peak-games-dominates-mobile-social-games-in-the-middle-east-and-turkey/>
- [32] "etohum web portal." [Online]. Available: <http://www.etohum.com/girisimler>
- [33] "Metutech animation technologies and game development center." [Online]. Available: http://oduteknokent.com.tr/portal/faces/atom-navigation/about?_adf.ctrl-state=ph4cxo751_122&_afLoop=3417505009042893
- [34] "Turkish undersecretariat for defense industries technology management strategy 2011-2016." [Online]. Available: http://www.ssm.gov.tr/anasayfa/kurumsal/Documents/201116_TYY.pdf

Kablosuz Algılayıcı Ağlarda Güvenli Yönlendirme Protokolleri Üzerine Bir İnceleme

F. Yıldırım Okay, S. Özdemir, Ş. Sağıroğlu

Özet—Kablosuz algılayıcı ağlarda (KAA) yönlendirme ağı enerji verimliliğini doğrudan etkilediği için oldukça önemli bir konudur. Çok geniş bir kullanım alanı olan KAA'ların genelde askeri, medikal, kimyasal, çevresel, endüstriyel gibi açık ortam uygulamaları olduğu için bu ağlar fiziksel saldırılara karşı savunmasızdır. Ayrıca, KAA'ların tüm uygulama alanlarına uygun tek bir yönlendirme protokolü geliştirilmesi uygulamaların gereksinimlerinden dolayı mümkün değildir. Kötü niyetli kişiler, sınırlı güç tüketimi olan algılayıcıların oluşturduğu KAA'ların güvenliğini, yönlendirme protokollerindeki açıklardan faydalanarak tehdit etmektedir. Özellikle, farklı saldırı yöntemleriyle saldırganlar ağı yaşam süresini kısaltmakta ya da ağ topolojisinde ciddi bozulmalar meydana getirebilmektedir. Bu makalede KAA'lardaki çeşitli yönlendirme saldırıları ve bu saldırılara karşı önerilen güvenli yönlendirme protokolleri incelenmiş, detaylı bir analiz yapılmıştır.

Anahtar Kelimeler— KAA; yönlendirme; güvenlik; enerji etkinliği

Abstract— Routing in wireless sensor networks (WSNs) is a very important issue due to its direct effects on the energy efficiency of network. WSNs, which has a wide spectrum of application fields such as military, medical, chemistry, environmental and industry, are so vulnerable to physical attacks. Also, it is not possible to develop a proper protocol for all application fields because of the distinct requirements of the applications. Malicious people may threat WSN security by taking advantage on routing protocol's vulnerability. In particular, attackers with different methods may reduce the lifetime of sensor networks or heavily corrupt network topology. In this article, various routing attacks and the proposed secure routing protocols against these attacks has been researched and analyzed in detail.

Key Words— WSN; routing; security; energy efficiency

I. GİRİŞ

KABLOSUZ algılayıcı ağlar (KAA) bir ortama yoğun bir şekilde dağıtılmış çok sayıda düğümden oluşmaktadır. Bu düğümlerin her biri düşük enerjili, düşük maliyetli, kısıtlı işleme ve hesaplama yeteneği olan çok fonksiyonlu küçük boyutlu cihazlardır. Düğümler algılama, hesaplama, haberleşme yeteneklerine sahiptir. Bu düğümler bir ortamdaki

veriyi algılayıp, yerel bir karar sürecine bağlı olarak diğer düğümlere ya da baz istasyonuna yönlendirebilirler [1-2].

Geleneksel ağlardan farklı olarak KAA'ların tasarım ve kaynak kısıtlamaları bulunmaktadır. Limitli enerji kaynakları, kısa iletişim aralığı, düşük bant genişliği, kısıtlı işleme ve depolama KAA'ların kaynak kısıtları arasındadır. KAA'ların tasarım kısıtı ise uygulamaya bağımlı olmasıdır. Yapılacak olan uygulama ya da gözlemlenecek ortama göre KAA'larda ağı boyutu, dağıtım şeması ve ağ topolojisi değişkenlik göstermektedir [2].

KAA'lar çok farklı alanlarda uygulanabilmektedir. Bunlardan bazıları, çevresel görüntüleme, ortam görüntüleme, askeri operasyonlar, bilimsel araştırmalar, oluşabilecek felaketleri tahmin etme, tıbbi görüntüleme vb. uygulamalardır. Ancak KAA'ların açık ortamlarda uygulanması düğümlerin fiziksel saldırılara açık hale gelmesine sebep olmaktadır [3]. Bununla birlikte, KAA'larda yönlendirmenin de güvenlik gereksinimlerini basit düzeyde sağlaması beklenmektedir. Yönlendirme üzerine yapılan çalışmalarda ilk olarak Karlof ve Wagner [4] güvenlik konusunu gündeme getirmiştir. Sonrasında ise çeşitli çalışmalarda güvenli yönlendirme protokolleri incelenmiştir. Geleneksel ağlarda yönlendirme protokolleri mesaj erişilebilirliği kriterini garantilemeyi amaçlamaktadır. Mesaj bütünlüğü, kimlik doğrulama ve gizlilik kriterleri daha yüksek seviyelerde SSH, SSL gibi uçtan uca güvenlik mekanizmaları ile sağlanmaktadır. Ancak KAA'larda orta düğümlerin mesaj içeriğine doğrudan erişim gereksinimlerinden dolayı uçtan uca güvenlik mekanizmalarının kullanımını zor hale getirmektedir [4].

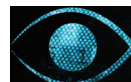
Literatürdeki çalışmalar incelendiğinde yapılmış olan çalışmaların daha çok KAA'lardaki yönlendirme protokollerinin güvenlik analizi üzerine olduğu görülmektedir [4,17-20]. Bu çalışmada KAA'lardaki yönlendirme üzerine yapılan saldırılar ve bu saldırılara karşı alınan önlemler üzerinde durulmaktadır. Literatürdeki KAA'lar için geliştirilmiş olan önemli yönlendirme protokolleri araştırılmış ve özetlenmiştir. İncelenen yönlendirme protokolleri özellikle güvenlik açısından ele alınmıştır. Öncelikle KAA'ların güvenliği üzerine yapılan araştırmalar incelenmiş, sonrasında yönlendirme protokolleri ile KAA'ların güvenliğinin nasıl sağlanabileceği konusundaki çalışmalar özetlenerek bir karşılaştırma verilmiştir. Ayrıca, ele alınan bu yönlendirme protokollerinin etkin oldukları saldırı türleri ve özellikleri belirtilmiştir.

Makalenin geri kalan kısmı şu şekilde düzenlenmiştir: II. Bölümde KAA'larda güvenlik konusu ele alınmıştır. III. Bölümde temel güvenlik gereksinimleri hakkında bilgi

F. Y.-O. Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (feyzakay@gazi.edu.tr).

S. Özdemir Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (suatozdemir@gazi.edu.tr).

Ş. S Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünde çalışmaktadır (ss@gazi.edu.tr).



verilmiştir. IV. Bölümde çeşitli yönlendirme saldırıları incelenmiş ve bu saldırılara karşı geliştirilen güvenlik mekanizmaları incelenmiştir. V. Bölümde literatürdeki güvenli ve enerji etkin yönlendirme protokolleri özetlenmiştir. Son olarak VI. Bölümde ise incelenen yönlendirme protokolleri üzerinden sonuç ve çıkarımlar yapıp, geleceğe yönelik araştırılabilir konular üzerinde durulmuştur.

II. KAA'LARDA GÜVENLİK

KAA düşman hatlarının ya da sınır bölgelerin gözetlenmesi gibi görev kritik uygulamalarda tasarım yapılırken güvenlik gereksinimi göz önünde bulundurulmalıdır. Ayrıca hassas kişisel bilgilerin olduğu çalışma uygulamalarında, sağlık uygulamalarında ya da bazı ticari uygulamalarda da güvenlik önem arz etmektedir [5]. KAA'ların düşman ortamlarında dağıtımlarının yapılması, çoğu algılayıcı ağı çevresindekileri gözlemlemesi ve bu bilginin kolayca açığa çıkarılması, istenmeyen bilgi sızmalarının ortamdaki kişilerin gizliliğini ihlal etmesi ve iletişimin düşmanlar tarafından kulak misafiri olma ya da paket enjeksiyonuna sebep olmasından dolayı KAA'larda güvenlik oldukça önemlidir. Ayrıca, KAA'lar kısıtlı hesaplama, enerji ve hafızaya sahip olmaları, asimetrik yaklaşımların çok pahalı olması, kulak misafiri olmanın kolay olmasından kaynaklı kötücül mesajların ağ içerisine kolayca enjekte edilebilmesi, büyük ölçekli dağıtımlarda ölçeklenememesi ve fiziksel saldırılara karşı duyarlı olmasından dolayı KAA'larda güvenlik gereksinimlerinin sağlanması oldukça zor ve karmaşık hale gelmektedir [6]. Önceki çalışmaların çoğunda algılayıcı ağların birbirleri arasında işbirliği ve güven ilişkisi sağladıkları varsayılmaktadır. Ancak gerçek uygulamalarda bu güven ilişkisinin sağlanabilmesi için güvenliğin sağlanması gerekmektedir [7].

Açık anahtar kriptografisinin çok pahalı olması ve KAA yapısının limitli hesaplama gücüne sahip olmasından dolayı tercih edilmemektedir. Simetrik kriptografi ise hızlı ve düşük enerji tüketiminden dolayı tercih edilmektedir. Ancak simetrik şifrelemedeki temel problemlerden bazıları ise KAA'larda gizli anahtarın düğümler arasında nasıl paylaşılacağı ve gizliliğinin nasıl sağlanacağıdır. İletilen mesajın önemli olduğu askeri ve benzeri uygulamalarda bilginin düşman tarafından ele geçirilmesi, değiştirilmesi ya da taklit edilmesi ciddi güvenlik hasarlarına sebebiyet verebilmektedir. Bu nedenle anahtar yönetimi ve anahtar dağıtımı KAA'lardaki güvenliğin korunmasındaki temel gereksinimlerdenidir [8,9].

III. KAA'LARDA GÜVENLİK GEREKSİNİMLERİ

Güvenlik gereksinimleri KAA'larda güvenlik üzerinde durulması gereken konulardan biridir. Bunun için çeşitli güvenlik gereksinimleri tanımlanmıştır. Gereksinimler bazı çalışmalarda birincil ve ikincil güvenlik hedefleri şeklinde ikiye ayrılmaktadır. Buna göre birincil gereksinimler gizlilik, bütünlük, kimlik doğrulama ve kullanılabilirlik gibi güvenliğin ana unsurlarıdır. İkincil gereksinimler ise, veri güncelliği,

kendi-kendini örgütlenme, zaman senkronizasyonu ve güvenli konumlandırma gibi etkenlerdir [7,11,12]. Bu gereksinimlerin dışında inkar edememe, güncellik gibi etkenler de bazı çalışmalarda incelenmektedir. Ayrıca ağdan ayrılan düğümlerin gelecek mesajları okunmasını ve ağa yeni katılan düğümlerin önceden gönderilmiş olan mesajları okumasını engelleyen ileri ve geri yönlü gizliliğin de olması önerilmektedir [15]. Gereksinimlerin çoğu geleneksel kablolu ve kablosuz ağlar için ortak olmasına karşın bu bölümde KAA'lardaki bazı gereksinimler üzerinde durulmaktadır [10].

A. Veri Gizliliği

KAA'larda veri gizliliği özellikle görev kritik uygulamalarda algılanan verinin yetkisiz kişilerce erişimlerinin engellenmesini garanti altına almaktır. Veri gizliliği ağ güvenliğindeki en önemli konudur. Çoğu uygulamada düğümler oldukça hassas bilgiler taşımaktadırlar. Bu bilginin güvenliğin sağlanması için bilginin taşındığı kanalın güvenliğin sağlanması gerekmektedir. Veri gizliliğindeki genel yaklaşımlar hassas bilginin gizli bir anahtar ile sadece alıcılar tarafından alınabilecek şekilde şifrelenmesidir, böylece güvenlik sağlanmaktadır. Dahası yönlendirme bilgisinin gizliliğinin sağlanması gerekmektedir. Çünkü kötücül kişiler tarafından yönlendirme bilgisi ile ağın performansı azaltılabilmektedir [13,14].

B. Bütünlük

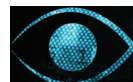
Veri gizliliği verinin sadece alıcı tarafından alınmasını garanti ederken, iletilen bilginin değiştirilmesinden koruyamaz. Veri bütünlüğü ise verinin hiçbir şekilde değiştirilmemesini garanti eder [14]. Veri üzerinde kötücül düğümlerin yanlış veri enjeksiyonu ya da kablosuz kanaldaki dengesiz durumlardan dolayı verideki bozulmalar ya da hata meydana gelmesi veri bütünlüğünü bozan etmenlerdir [11]. Bu nedenle mesaj kimlik doğrulama doğrulama kodları (message authentication codes) ya da dairesel kodları (cyclic codes) veri bütünlüğü korunabilmektedir [14].

C. Veri Kimlik Doğrulama

Veri kimlik doğrulama alıcıya kaynağın doğru bir şekilde göndericiden gönderildiğini doğrulamaktadır. KAA'lar ortak kablosuz ortamı kullandıklarından saldırganlar kolaylıkla mesaj enjekte edebilir. Bu nedenle alıcının verinin doğru kaynaktan geldiğini doğrulaması gerekmektedir. Bu doğrulama işlemi kimlik doğrulama mekanizmaları ile yapılmaktadır. Kimlik doğrulama olmadan kötücül düğüm başka düğümleri taklit edebilir ve ağa zarar verebilir. Eğer iki düğüm iletişim halindeyse simetrik anahtarlama ile kimlik doğrulama sağlanabilmektedir. Ancak yayımlama türü iletişimde daha güçlü güven varsayımlarına ihtiyaç vardır. Bu nedenle doğrulamalı yayılım için asimetrik mekanizmaların kullanımına ihtiyaç duyulmaktadır [13].

D. Kullanılabilirlik

Kullanılabilirlik ağ hizmetlerinin hizmet engelleme saldırıları (DoS) karşısında hayatta kalmasını garantilemektedir. DoS saldırıları KAA'ların herhangi bir katmanında meydana gelebilir ve herhangi bir düğümü kalıcı



bir şekilde etkisizleştirebilir. Ayrıca aşırı iletişim ve hesaplama yükü KAA'lardaki düğümlerin bataryalarının tükenmesine sebep olabilmektedir. Askeri bir uygulama için düşünüldüğünde düğümlerden bazılarının kullanılabilirlikleri düzgün bir şekilde sağlanmazsa, düşman bu kısım üzerinden ağa sızabilir ve istenmeyen sonuçlara sebep olabilmektedir [14].

E. Veri Güncelliği

Veri güncelliği verinin yeni olduğunu ve eski bir mesajın yeniden gönderilmediğini garanti altına almaktadır. Gizlilik ve bütünlüğün sağlanmasının yanı sıra her bir mesaj için veri güncelliğinin de sağlanması gerekmektedir [11]. İki tip veri güncelliği sağlanmaktadır. Bunlardan ilki zayıf güncelliktir. Zayıf güncelleme ile kısmi mesaj sıralaması sağlanır ancak herhangi bir gecikme bilgisi bulundurmaz. Bazı algılayıcı ölçümleri için gereklidir. Güçlü güncellemede ise istek-cevap çifti ile tam bir sıralama ve gecikme tahmini sağlar. Ağ içerisindeki zaman senkronizasyonu için kullanışlıdır [13].

IV. SALDIRI MODELLERİ

KAA'lar kullandıkları iletim ortamının yapısından (yayılım türü iletişim/broadcast) dolayı güvenlik saldırılarına karşı oldukça kırılgandırlar. Ayrıca riski yüksek ortamlarda düğümlerin dağıtımlarının yapılmasından dolayı fiziksel olarak korunma sağlanamamakta ve bu durum KAA'ların kırılganlığını artırmaktadır. Geniş ölçekli algılayıcı ağlarında her bir düğümü gözetlemek ve korumak mümkün olmadığından fiziksel ya da mantıksal saldırılara açık haldedir. Saldırganlar farklı güvenlik saldırılarıyla KAA'ların yapısını bozabilmektedir. KAA'lardaki saldırılar genel olarak iki bakış açısıyla değerlendirilmektedirler. Bunlardan ilki güvenlik mekanizmalarına karşı yapılan saldırılar diğeri ise ana mekanizmalara (örneğin yönlendirme mekanizmaları) karşı yapılan saldırılardır [16]. Ağ katmanı üzerinde yer alan saldırılara yönlendirme saldırıları denmektedir [11]. Bu kısımda ağ katmanı üzerinde yer alan çeşitli yönlendirme saldırıları üzerinde durulmaktadır.

A. Yönlendirme Saldırıları

1) Aldatılmış, değiştirilmiş veya tekrar edilmiş yönlendirme bilgisi

Yönlendirme protokollerine karşı yapılabilecek en doğrudan saldırı şekli yönlendirme bilgisini hedef alan saldırılardır. Saldırgan ağ trafiğini bozmak için yönlendirme bilgisini aldatabilir, değiştirebilir ya da tekrar edebilir. Ayrıca yönlendirme döngüleri, ağ trafiğinin kendine çekilmesi ya da püskürtülmesi, kaynak yönlendiricilerinin genişletilmesi ya da kısaltılması, hata oluşturulması, ağır bölümlendirilmesi veya uçtan uca gecikmelerin artırılması gibi durumlar da bozulmalara sebep olabilmektedir [17].

2) Seçici İletme

Çok sekmeli ağlardaki önemli varsayımlardan biri ağdaki tüm düğümlerin gelen mesajı doğru bir şekilde diğer düğümlere iletmesi şeklindedir. Seçici iletme saldırısında,

kötücül bir düğüm ağı ele geçirebilir ve bazı mesajları seçerek iletirken diğerlerini bırakabilmektedir [17].

3) Sinkhole

Sinkhole saldırısında düşman ele geçirdiği düğümlerle tüm ağın dikkatini çekerek ve yönlendirme bilgisi sahtekarlığı yaparak merkezde bir 'Sinkhole' oluşturur. Böylece komşu düğümler verilerini iletecekleri bir sonraki düğüm olarak ele geçirilmiş düğümü seçmektedirler. Bu saldırı türü kısaca komşu düğümlerin seçici iletmeyi kolay hale getirerek veri akışının ele geçirilmiş düğümler üzerinden olmasını sağlar [17]. Kablosuz ağlar özelleşmiş iletişim örüntüleri sayesinde sinkhole saldırılarına karşı duyarlıdırlar. Tüm paketler aynı varış noktasını paylaştıkları için ele geçirilmiş düğümün yalnızca baz istasyonuna tek bir yüksek kaliteli yönlendirme sağlaması yeterlidir. Böylece bu yönlendirme üzerinden veri iletimi sağlayan tüm düğümler etkilenecektir [18].

4) Sybil Saldırıları

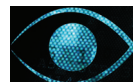
Sybil saldırıları bir düğümün ağ içerisinde birden fazla kimlik sunması durumudur. Bu düğümler 'Sybil' düğüm olarak adlandırılmaktadır [19]. Bu saldırı ile dağıtık depolama, dispersite, çoklu yol, yönlendirme ve topoloji sürdürülebilirliği gibi hata toleransı şemalarının etkinliğini büyük ölçüde düşmektedir [17]. Sybil saldırıları ile ayrık gibi gözükten yollar aslında kötücül bir düğümün çoklu kimlik sunmasıyla oluşmaktadır. Sybil saldırıları kullanılarak kötücül düğüm aynı anda birden fazla yerde olabilmektedir. Böylece coğrafi yönlendirmeler için ciddi bir tehdit oluşturmaktadır. Ayrıca blok saldırıları gibi yönlendirme saldırılarının tespitinde Sybil saldırı ile yanlış davranış tespit mekanizmalarından kaçınılabilir [19].

5) Solucan Deliği

Solucan deliği ağdaki iki kısım arasında düşük gecikmeli bağlantı sağlamaktadır ve ağ mesajlarını tekrarlamaktadır [17]. Buna göre saldırı ağdaki bir noktadan paketleri alır ve ağdaki diğer bir noktaya tünel açar. Bu noktadan mesajları tekrarlar. Birbirleri ile anlaşılan iki saldırı arasındaki tünel solucan deliği olarak adlandırılmaktadır. Solucan deliği ile tünelden geçirilen paketler diğer iletimi yapılan paketlerden daha çabuk iletilmektedir [20]. Bu saldırılar genelde seçici iletme ve kulak misafirliği ile birlikte kullanılmaktadır. Sybil saldırılar da bu birleşime eklendiğinde tespit edilmesi güç hale gelmektedir [17].

6) HELLO Taşkını

HELLO paketlerini kullanan çoğu protokol basit bir varsayımla paketlerin radyo iletim aralığı içerisinde gönderildiklerini yani gönderildikleri yerlerin komşu düğümler olduğunu kabul etmektedir. Ağ içerisindeki her bir düğüm komşularına HELLO paketleri göndererek varlığı hakkında bilgi vermektedir. HELLO taşkınında, saldırı yüksek güçlü bir iletici kullanarak çok sayıda düğümü kandırabilir ve onları komşuluk sınırları içerisinde olduğuna inandırabilir. Saldırgan diğer düğümlerin radyo aralığı dışında yer almasına rağmen baz istasyonuna hatalı bir şekilde daha kısa bir yönlendirme yayınlarak diğer düğümlerin



KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİ YÖNLENDİRME PROTOKOLLERİ ÜZERİNE BİR İNCELEME

saldırganın ait HELLO paketi almasını ve buraya iletim yapmalarını sağlar [17].

7) Onay mesajını aldatma

KAA'lardaki bazı yönlendirme algoritmaları onay paketlerinin iletimini gerektirmektedir. Saldırgan düğüm komşu düğümlerden paket iletimine kulak misafiri olabilir ve düğümü yanlış bilgi ile aldatılabilir. Böylece saldırı düğüm hakkında yanlış bilginin yayılmasına sebep olabilmektedir. Bu yanlış bilgilendirme zayıf bir düğümün güçlü gibi gösterilmesi ya da ölü bir düğümün canlı olarak gösterilmesi şeklindedir [17].

B. Saldırlara Karşı Geliştirilen Savunma Mekanizmaları

Aldatılmış, değiştirilmiş veya tekrar edilmiş saldırı türüne geliştirilmiş savunma mekanizması mesaj doğrulama kodlarının (MAC) kullanımıdır. Bu doğrulama kodları ile bir mesajın aldatılmış ya da değiştirilmiş olup olmadığı anlaşılabilir. Ayrıca tekrar etme saldırılarına karşı önlem olarak sayaçlar ya da zaman damgaları kullanılmaktadır [13]. Seçici ileme ataklarına karşı geliştirilen savunma mekanizması veriyi göndermek için çoklu yol kullanımıdır. Ayrıca kötücül düğümün tespiti ya da mesaj iletiminin başarısız olduğu kabul edilip alternatif yollardan gönderilmesi sağlanabilir [17]. Sybil saldırılarına karşı geliştirilmiş savunma mekanizmalarından biri doğrulamadır. İki tip doğrulama bulunmaktadır. Bunlardan ilki doğrudan doğrulama olup, her bir düğüm diğer düğümlerin kimliklerinin geçerli olduğunu doğrulamaktadır. Diğer ise dolaylı doğrulamadır. Buna göre düğümlerin kimlik birlikleri önceden doğrulanmıştır. Buna göre düğümler diğer düğümlerin doğruluğunu garanti eder ya da reddeder [19]. Paket bağlama ile solucan deliği saldırılarına karşı tespit ve savunma yapılmaktadır. Coğrafi ve geçici bağlamalar olmak üzere iki tip paket bağlama sunulmaktadır [20]. HELLO taşkını saldırısında bağlantı üzerinden alınan mesajla herhangi bir işlem yapılmadan önce bağlantının çift yönlülüğünün kontrolünü yapan mekanizmalar önerilmektedir [21]. Sinkhole saldırıları savunulması zor saldırılardandır. Bu nedenle yönlendirme protokollerinin bu saldırılara karşı tasarlanmış olması gerekmektedir. Bu saldırılara dayanıklı protokollerden biri coğrafi yönlendirme protokolüdür. Coğrafi yönlendirmeler baz istasyonundan başlatılmaksızın yerleşmiş ilişkileri ve bilgileri kullanan bir yapı oluşturur.

Trafik baz istasyonunun fiziksel konumu üzerinden kendiliğinden yönlendirildiği için sinkhole saldırıları ile başka

bir yere yönlendirmek oldukça zordur [17]. Ayrıca onay mesajını aldatma saldırılarına karşı kimlik doğrulama kullanılmaktadır ve güvenlikleri sağlanmaktadır [15]. Tablo1'de yönlendirme üzerine yapılan saldırılar ve bunlara karşı alınan önlemler listelenmektedir.

V. GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

KAA'larda güvenli yönlendirme protokollerinin amacı güvenliğin temel unsurlarını kapsayacak şekilde bir mesajın bütünlüğünü, kimlik doğrulamasını ve kullanılabilirliğini sağlamaktır. Karlof ve Wagner yapmış oldukları çalışmada [17] güvenli yönlendirme protokollerini üzerine dikkatleri çekmesiyle birlikte KAA'larda güvenli yönlendirme protokollerini üzerine bazı yenilikçi çalışmalar yapılmıştır. Bu çalışmalardan bazıları tamamen güvenliyi sağlarken, bazıları ise sadece seçili saldırı türlerine karşı güvenliyi sağlamaktadır. Ayrıca bazı çalışmalarda güvenliğin yanı sıra enerji etkinliğinin de sağlanması önerilen protokolün temel amaçları arasındadır. Çalışmaların çoğu simetrik anahtarlama mekanizmasına dayanmaktadır. Buna karşın açık anahtarlama şifreleme mekanizmasını kullanan çalışmalarda bulunmaktadır. Bu kısımda KAA'larda güvenli yönlendirme protokollerini üzerine detaylı bir inceleme yapılmaktadır.

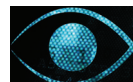
A. Güvenli Ortam Erişim Protokolleri

1) SIGF

Güvenli Üstü Kapalı Coğrafi İletim (GÜCİ/SIGF) [22] ayarlanabilir bir yönlendirme protokolü olup "yeterince iyi" bir güvenlik ve yüksek bir performans sağlamaktadır. Bu protokol Üstü Kapalı Coğrafi İletim (ÜCİ/IGF)'nin [23] güvenlik mekanizması eklenmiş halidir. Üç güvenlik seviyesini temsil eden üç farklı protokol içermektedir. Bunlar SIGF-0 (hiç durum olmaması), SIGF-1(yerel bir şekilde oluşturulmuş durum) ve SIGF-2 (komşuluk içerisinde ikili paylaşımlı durum) protokolleridir. SIGF-0 hiçbir yönlendirme bilgisinin devam ettirilmediği durum olmayan bir protokol olup IGF protokolünün basit düzeyde genişletilmiş halidir. IGF'deki bazı parametrelerin ayarlanabilir özellikte olmasını sağlar. Komşular hakkında iletim bilgisi ve geçmişi tutmadan non-deterministik ve dinamik bir şekilde bir sonraki sekme aktarımını seçmektedir. İletim alanının genişletilmesi ile daha fazla komşu düğümü dahil etmektedir. Bu durum komşuluklar içerisinde saldırıların seçilme ihtimalini azaltmaktadır.

TABLO I. YÖNLENDİRME SALDIRILARI VE SAVUNMA MEKANİZMALARI

SALDIRI TÜRLERİ	SAVUNMA MEKANİZMALARI
Aldatılmış, Değiştirilmiş veya Tekrar Edilmiş Yönlendirme Bilgisi	Çıkış filtreleme, kimlik doğrulama, gözetleme, mesaj doğrulama kodları
Seçici İletme	Artıklık kontrolü, çoklu yol kullanımı
Sinkhole	Kimlik doğrulama, gözetleme, artıklık, güvenlik protokolleri
Sybil Saldırıları	Kimlik doğrulama, deneme (probing)
Solucan Deliği	Kimlik doğrulama, coğrafi ve geçici bilgiler kullanılarak paketi bağlama
HELLO Taşkını	Kimlik doğrulama, çift yönlü bağlantıları doğrulama
Onay mesajını aldatma	Kimlik doğrulama



SIGF-0 IGF'ye göre acele ettirme saldırılarında karşı daha dayanıklıdır. Az miktarda verimsizlik olmasına rağmen, güvenliği önemli ölçüde artırmaktadır. SIGF-1 protokolü, SIGF-0 protokolündeki özelliklere ek olarak bir düğümün içeriden durumunu belirlemektedir. SIGF-1, SIGF-0 gibi çalışır ancak bir sonraki sekmenin seçimi her bir komşu düğüme atanan itibar değerine göredir. Bu değer düğüm tarafından depolanan ve sürdürülen durum bilgisinden türetilmektedir. SIGF-1 protokolü özellikle sybil saldırılarına karşı etkin bir koruma sağlamaktadır. SIGF-2 protokolü ise önceki protokollere ek olarak hizmet engelleme (DoS) saldırılarına karşı kriptografi kullanımını sağlamaktadır. Ayrıca komşu düğümler arasında gizlilik, kimlik doğrulama, bütünlük ve veri güncelliği kriterlerini sağlamaktadır. Yararlı yük şifreleme ile kulak misafiri olmayı engeller. Ağ planlayıcısı dağıtımdaki güvenlik ihtiyaçlarına göre gerekli SIGF protokolünü seçebilir ve ayarlayabilir. Sonuç olarak SIGF protokolü güvenlik, etkinlik ve performans arasında ayarlanabilir bir algoritma seçimi imkanı sağlar.

2) SDD

Doğrudan Difüzyon [25] protokolü KAA'lar için önemli bir veri merkezli yönlendirme protokolüdür. Güvenli Doğrudan Difüzyon (GDD/SDD) [24] protokolü ise Doğrudan Difüzyon algoritmasına bazı güvenlik parametreleri eklenmiş halidir. Doğrudan Difüzyon protokolü kimlik doğrulama ve bütünlük gereksinimlerinin eksikliği nedeniyle çeşitli saldırılara karşı oldukça kırılgan bir yapı göstermektedir. Saldırgan pozitif ya da negatif aldatmalarla veri akışının sırasının zorla değiştirilmesine sebep olabilir. Bu durum ise seçici iletme, kurcalama, DoS ya da kulak misafiri olma saldırıları gibi saldırılarla sonuçlanabilir. Ayrıca lap-top sınıfı saldırganlar solucan deliği saldırılarını sahte donatılar kullanarak sinkhole saldırıları yapabilir. SDD protokolü kimlik doğrulamalı yayın yapan immediate TESLA [26] kullanımına dayanmaktadır. Bu sayede yönlendirme ve veri mesajlarının kimlik doğrulaması ve bütünlüğü sağlanmaktadır. Ayrıca gizlilik ve saldırıların başarılarını engellemek için dayanıklılık ve hayatta kalma gereksinimleri de sağlanmaktadır. Sadece simetrik kriptografi kullanılır. Asimetri tek yönlü özet zincirleri ile sağlanmaktadır. Önerilen protokol değiştirilmiş LEAP'ın Doğrudan Difüzyon ile işbirliği ile ağın dışarısından gelen hemen hemen bilinen tüm saldırılara karşı koruma sağlamaktadır. Sadece düşük oranda veri yayılımı fazında problem oluşmaktadır. Saldırgan kulak misafiri olarak iletişimi dinleyebilir ve rastgele seçilen yol üzerinde bulunabilir.

3) SeRINS

Algılayıcı Ağlarda Güvenli Alternatif Yol Yönlendirme (AAGAYY/SeRINS) [27] protokolü çeşitli güvenlik mekanizmaları ve komşu raporlama sistemi ile güvenli yönlendirme sağlamaktadır. SeRINS protokolünün amacı ağ seçici iletme ya da sahte yönlendirme bilgisi tanıtımı saldırıları gibi içerden saldırılara karşı korumaktır. Bu çalışmada yazarlar saldırganların sadece az sayıda düğümü ele

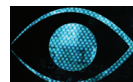
geçirdiğini kabul etmektedir. Ayrıca her bir düğüm baz istasyonu ile tek bir gizli anahtar paylaşarak bu anahtar üzerinden komşu düğümlerle iletişim kurduğunu kabul etmektedir. Son olarak ise tüm iletişim sekmeden sekmeye şifreleme ile korunduğu için dışarıdan saldırılara karşı ağa katılarak koruma sağladığını kabul etmektedirler. Üç farklı şema yapısı bulunmaktadır. Bunlar yönlendirme topolojisinin kurulduğu alternatif yol şeması, alt sekmelerin kimlik doğrulamasının yapıldığı komşu kimlik doğrulama şeması ve sahte tanıtım saldırıları gibi kötücül düğümleri belirleyen ve ortadan kaldıran komşu raporlama şemasıdır. SeRINS protokolünde her ikili komşu düğüm arasındaki güvenli kanallar sayesinde sybil saldırıları, sinkhole saldırıları, HELLO taşkını ve onay mesajını aldatma saldırıları gibi saldırılara karşı oldukça dayanıklıdır. Solucan deliği saldırılarına karşı ise paket bağlama gibi harici şemalarla savunma yapılmaktadır. Ayrıca seçici iletme saldırıları çoklu yol şeması ile önlenirken, sahte yönlendirme bilgisi problemi ise komşu raporlama sisteminin tespit ve reaksiyon mekanizmaları ile çözülmektedir.

4) Temiz Bir Sayfa Yaklaşımı

Temiz bir sayfa yaklaşımında [28] güvenliğin ve etkinliğin ana amaç olarak tanımlandığı bir yönlendirme protokolü sunulmaktadır. Aktif saldırganların olduğu ortamda bile herhangi bir özel donanım gerektirmemekte ve mesaj dağıtımını gerçekleştirebilmektedir. Yüksek dereceli güvenlik ve düğümden düğüme yüksek kullanılabilirlik sağlamak amaçlanmaktadır. Asimetrik kriptografi kullanılmaktadır. Bu protokol önleme, tespit/iyileştirme ve dayanıklılığın kombinasyonundan oluşmaktadır. Önleme yaklaşımı saldırılar karşısında kriptografi mekanizmaları ile protokolü daha dayanıklı hale getirmeyi amaçlamaktadır. Önleme yaklaşımı etkin bir yaklaşım olmasına karşın bilinen saldırılara karşı önceden önlem almaktadır. Tespit yaklaşımı protokol katılımcılarının davranışlarını gerçek zamanlı gözetleme işlemi yapmaktadır. Kötücül bir düğüm tespit edildiğinde kötücül katılımcıların yok edilmesi ve ağ sırası ve işlevselliğinin yeniden sağlanması için iyileştirme teknikleri kullanılmaktadır. Tespit yaklaşımı daha çok bilinmeyen saldırılara karşı koruma sağlamaktadır. Dayanıklılık yaklaşımı ise saldırı anında bile kullanılabilirlik oluşturmayı amaçlamaktadır. Bu yaklaşım ele geçirilmiş katılımcıların ağ içerisindeki varlıklarını azaltmada iyi bir performans sergilemektedir.

5) INSENS

Kablosuz Algılayıcı Ağlarda Sızma Toleranslı Yönlendirme Protokolü (STYP/INSENS) [29] KAA'larda güvenliği sağlayan yönlendirme tabanlı bir yaklaşımdır. INSENS algılayıcı düğümler ve baz istasyonu arasındaki iletişimin kolay olması için her bir düğümden iletim tabloları oluşturur. Bu protokolün amacı KAA'larda tek bir ele geçirilmiş düğümün ağ içerisinde sadece yerel bir bölgede bozulmalara sebep olacağı sızma toleranslı güvenlik sağlamaktır. Başka bir deyişle düğümlerdeki saldırılar tamamen engellenmeye



KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİ YÖNLENDİRME PROTOKOLLERİ ÜZERİNE BİR İNCELEME

çalışılmamaktadır. Sadece ağa verecekleri zararlar minimize edilmeye çalışılmaktadır. İki tip saldırı sınıfı için sızma toleransı sağlamak amaçlanmaktadır. Bunlar tüm ağı veri paketleri istilası yapan DoS-tipli saldırılar ve yanlış yönlendirme bilgisini de içeren hatalı kontrol paketleri yayılımına sebep olan yönlendirme saldırılarıdır. DoS saldırılarını önlemek için, bireysel düğümlerin tüm ağa yayın yapması engellenir. Yalnızca baz istasyonu yayın yapabilir. Ayrıca baz istasyonu herhangi bir kötücül düğüm tarafından kendini yetkili biri gibi gösterme saldırılarına karşı tek yönlü özet fonksiyonlarını kullanarak kimlik doğrulama yapar. Yanlış yönlendirme verilerinin sızmasını önlemek için yönlendirmeye ait olan kontrol bilgileri doğrulanır. İçeriden bir saldırgan bir düğümü ele geçirse ve paket iletimini engellese bile, INSENS artık çoklu-yol yönlendirme kullanarak kötücül düğüme uğramadan varış düğümüne iletim sağlayabilmektedir. Ayrıca her bir kaynak kısıtlı algılayıcı düğüm ile baz istasyonu arasında gizlilik ve kimlik doğrulama sağlamak için simetrik anahtar kriptografisini kullanmaktadır.

6) SPINS

SPINS [13] algılayıcı ağlarda güvenli iletişim sağlayan bir protokoldür. SPINS iki temel yapı içermektedir. Bunlar, güvenli ağ şifreleme protokolü SNEP [13] ve μ TESLA [13] protokolüdür. SNEP protokolü veri gizliliği, iki kısımlı veri kimlik doğrulama ve eş düzeyde iletişim (düğümünden baz istasyonuna) için veri güncelliği sağlamaktadır. SNEP, her bir mesaja sadece 8 baytlık ek yük ile düşük iletişim ek yükü sağlamaktadır. Ayrıca, anlamsal güvenlik ile şifreli mesajın içeriğine kulak misafiri olmayı önlemektedir. Veri kimlik doğrulama (MAC) ile verilerin yollayıcıdan gönderildiği durumlarda alıcı tarafından alındığını garanti eder. MAC'lerde bulunan sayaç değerleri ile tekrarlama mesajları engellenir. Böylece tekrarlama saldırılarına karşı da bir korunma sağlanmış olur. Ayrıca, eğer bir mesaj doğru bir şekilde doğrulanmışsa, kullanıcı bir önceki mesajı aldıktan sonra gönderici tarafından yollandığını bilmektedir. Bu da zayıf da olsa tazelik sağlamaktadır. Diğer bir güvenli yapı bloğu olan μ TESLA protokolünde ise, standart TESLA'nın [30] algılayıcı ağlar üzerindeki bazı zorluklarına çözümler üretilmiştir. Son zamanlarda önerilen TESLA kimlik doğrulamalı yayın yapmak için geliştirilen bir protokoldür. μ TESLA protokolü ile ilk olarak başlangıç paketindeki sayısal imzalamanın çok maliyetli olmasından dolayı simetrik anahtarlama kullanılmıştır. Her bir paket için bir anahtar bildirmek, alım ve gönderim için çok enerji gerektirdiği için her devirde bir kere anahtar bildirilmiştir. Son olarak ise, tek yönlü anahtar zinciri oluşturmak çok maliyetli olduğundan, μ TESLA ile doğrulanan yollayıcı sayısı kısıtlanmıştır.

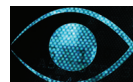
B. Enerji Etkin Güvenli Yönlendirme Protokolleri

1) KAA'lar için Güvenli ve Enerji Etkin bir Yönlendirme Protokolü

KAA'larda yönlendirmede güvenlik ve etkinlik problemlerinin adreslenmesinde Sen tarafından önerilen bu protokol [31] ile hatalı ya da ele geçirilmiş düğümler güvenilir bir şekilde tanımlanmakta ve yönlendirme yolu kullanılırken bu düğümlerden kaçınılmaktadır. Protokol tek bir yönlendirme yolu kullanmaktadır bu nedenle enerji etkindir. Önerilen protokol Lee tarafından önerilen yönlendirme şemasının [32] değiştirilmiş halidir. Bununla birlikte daha enerji etkindir ve daha az gecikmeye sebep olmaktadır. Protokol dayanıklı komşuluk gözetleme sistemine (NMS) dayanmaktadır. Bu sistem bir düğüm tarafından komşuluğun rastgele gözetlenmesine dayalı çalışır ve komşu liste kontrolü ile işbirliği yapan bir algoritma ile herhangi bir paket düşürme saldırısını tespit eder. Bu şema ile kötücül düğüm yönlendirme yolu içerisinde paket düşürme saldırısında bulunsu bile güvenilir sekmeden sekmeye paket dağıtımını yapılabilmektedir. Paket düşürme saldırısına karşı çoklu-yol yönlendirme ile savunma yapmaktadır. Her bir paket iletim düğümünün küme anahtarı ile şifrelenmektedir. Böylece iletim düğümünün tüm komşuları deşifreleyebilir ve kulak misafiri olabilir. Şifrelemenin küme anahtarı ile sağlanması düğüm ele geçirmelerine karşı dayanıklılık sağlar. Önerilen şema ayrıca yönlendirme bozma saldırılarına karşı da dayanıklıdır.

2) Kablosuz Algılayıcı Ağlar için Enerji Etkinliği ile Güvenli Bir Yönlendirme Protokolü

KAA'larda enerji etkin ve güvenli bir yönlendirme protokolü olan bu protokol [33] iyi bir veri dağıtım oranı, enerji dengelemesi ve yönlendirme etkinliği sağlamaktadır. Buna ek olarak önerdiği güvenlik mekanizmaları ile veri dağıtımında kimlik doğrulama ve gizlilik sağlamaktadır. Bu protokol ile daha iyi bir dağıtım oranı sağlamak için çıkış düğümüne yönelik grid yapısı kullanılmaktadır. İkinci olarak, en uzak ve en yüksek enerji yayılım düğümü araması ile kaynak düğümünden çıkış düğümüne etkin bir yol bulunmaya çalışılmıştır. Son olarak ise protokol tasarımı güvenlik gereksinimleri düşünülmüştür. Güvenlik mekanizması olarak tek yönlü özet zincirleri, mesaj doğrulama kodları (MAC), simetrik şifreleme ve çeşitli önceden depolanmış paylaşılmış gizli anahtarlar kullanılmaktadır. Bu protokolda, yanlış bir paket çıkış düğümüne ulaşmaması için yol üzerinde düşürülür. Böylece enerji tüketimi azaltılır. Ayrıca çıkış düğümü tarafından yeni eklenen düğümlerin kimlik doğrulaması yapılır ve komşu düğümlerin komşuluk bilgisi oluşturmaları sağlanır. Herhangi bir düzensizlik bulunduğu anda ise yönlendirme bilgisinin yeniden oluşturulması için çıkış düğümü görevlendirilir. Şüpheli düğümler raporlandıktan sonra bu düğümlerin kötücül oldukları ispatlanırsa çıkış düğümünün diğer düğümleri bilgilendirmesi sağlanır. Son olarak seçici iletim düğümleri yönlendirme protokollerine dahil olarak ağdaki düğüm sayısını kısıtlar ve böylece güvenliği sağlar.



TABLO II. GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

YÖNLENDİRME PROTOKOLLERİ	ETKİN OLDUKLARI SALDIRI TÜRÜ	GÜVENLİK GEREKSİNİMİ	ÖZELLİKLERİ
SIGF [22]	Sybil, DoS, Kulak misafiri olma	Gizlilik, Kimlik doğrulama, bütünlük, veri güncelleme	Güvenlik, etkinlik ve performans arasında ayarlanabilir bir algoritma seçimi sağlar.
SDD [24]	Ağın dışarısından gelen tüm saldırılar	Kimlik doğrulama, bütünlük, gizlilik, dayanıklılık, hayatta kalabilme	İmmediate Tesla kullanımına dayanmaktadır. Doğrudan Difüzyon protokolü LEAP ile güvenli hale getirilmiştir.
SeRINS [27]	Seçici iletme, Sahte yönlendirme bilgisi tanıtımı, Sybil, Sinkhole, Hello taşkını, Solucan deliği	Kimlik doğrulama, Paket bağlama, Çoklu yol kullanımı, Komşu raporlama	Yönlendirme topolojisinin kurulduğu alternatif yol şeması, alt sekmelerin kimlik doğrulamasının yapıldığı komşu kimlik doğrulama şeması ve sahte tanıtım saldırıları gibi kötücül düğümleri belirleyen ve ortadan kaldıran komşu raporlama şemasına sahiptir.
Temiz bir Sayfa Yaklaşımı [28]	İçeriden ve dışarıdan gelen tüm saldırılar	Kullanılabilirlik	Aktif saldırganların olduğu durumlarda özel bir donanım gerektirmez ve mesaj dağıtımını yapabilir.
INSENS [29]	DoS-tipli, yönlendirme saldırıları	Kimlik doğrulama, gizlilik	Sızma toleranslı güvenlik ile ele geçirilmiş düğüm ağ içerisinde sadece yerel bir bölgede bozulmalara sebep olabilir.
SPINS [13]	Tekrarlama, kulak misafiri olma	Kimlik doğrulama, gizlilik, veri güncelliği	SNEP ve µTESLA olan iki temel bloktan oluşur.

3) SERP

KAA'larda Güvenli Enerji Etkin Yönlendirme Protokolü (GEEYP/SERP) [34] kaynak düğümden baz istasyonuna limitli enerji tüketimi ile kimlik doğrulamalı ve dayanıklı iletimini sağlamaktadır. SERP'in tasarımında üç ana amaç düşünülmüştür. Bunlar; ağ ömrünü uzatmak ve enerji etkin iletim sağlamak için enerji farkında organizasyon, hatalı rapor enjektisinin tespitini sağlayan güvenli iletim ve düğümlerin başarısız olmasının ağın performansını çok etkilememesi için dayanıklı ve esnek bir iletimdir. Protokol iki aşamada çalışmaktadır. Öncelikle ağın omurgası oluşturulur. Sonrasında ise güvenli veri iletimi sağlanır. Ağaç yapısı enerji tüketimini dengelemek için ağın omurgası olarak oluşturulur. Minimum sayıda iletim düğümü ağ içerisinde seçilir ve ağ omurgası periyodik bir şekilde yeniden oluşturulur.

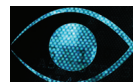
Güvenli veri iletimini sağlamak için tek yönlü özet zincirleri ve önceden depolanmış paylaşılmış gizli anahtarlar kullanılır. Veri güncelliği için ise uygulamaya bağlı olarak isteğe bağlı anahtar yeniden güncelleme mekanizması kullanılır.

4) EENC

Düğüm Ele Geçirme Drenci ile Enerji Etkin Yönlendirme (DEGDEEY/EENC) [35] protokolü ele geçirilmiş düğümleri yok sayarak enerji tüketimi ile paket doğruluğu arasında dengeleme sağlamaktadır. Yönlendirme tabloları için karınca kolonisi algoritmasına dayalı güçlendirilmiş öğrenme kullanılmaktadır. Öncelikle ağdaki tüm düğümlere güven değeri atanmaktadır. Bu güven değeri paket düşürme oranı, iletim gecikme oranı gibi değişkenlere dayalı olarak hesaplanmaktadır. Bu değerler kullanılarak kötücül düğümlerin tespiti yapılmaktadır. Ağdaki her bir düğüm bir sekme mesafedeki komşularının güven değerlerini hesaplar. EENC protokolündeki amaç minimum enerji tüketimiyle güvenlik sağlamaktır. Bunun içinde komşulara ait güven değerleri depolanır. Protokol iki farklı yönlendirme protokolü ile karşılaştırıldığında enerji etkinliğinde yüksek performans sağlanırken başarılı paket iletiminin yapıldığı görülmektedir.

TABLO III. ENERJİ ETKİN GÜVENLİ YÖNLENDİRME PROTOKOLLERİ

ENERJİ ETKİN GÜVENLİ YÖNLENDİRME PROTOKOLÜ	ETKİLİ OLDUĞU SALDIRI TÜRÜ	ÖZELLİKLER
Güvenli ve Enerji Etkin bir Yönlendirme Protokolü [31]	Paket düşürme ve yönlendirme bozma saldırıları	Hatalı ya da ele geçirilmiş düğümler tanımlanıp, yönlendirmede bu düğümlerden kaçınılmaktadır.
Enerji Etkinliği ile Güvenli bir Yönlendirme [33]	Yanlış paket enjektisi	İyi bir veri dağıtım oranı, enerji dengelemesi ve yönlendirme etkinliği sağlar. Ayrıca veri dağıtımında kimlik doğrulama ve gizlilik sağlar.
SERP [34]	Hatalı rapor enjektisi	Kimlik doğrulama ve gizlilik ile dayanıklı veri iletimi sağlar. Veri güncelliği uygulamaya bağlı olarak sağlanır.
EENC [35]	Ele geçirilmiş düğüm	Enerji tüketimi ile paket doğruluğu arasında dengeleme sağlar. Karınca kolonisi algoritmasına dayalı güçlendirilmiş öğrenme kullanılır. Başarılı paket iletim oranı sağlanır.



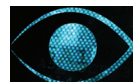
VI. SONUÇ

KAA'lar çeşitli tasarım kısıtlarına sahip açık alanlarda uygulanabilir bir yapı göstermektedir. Bu nedenle ağ içerisinde ya da dışarıdan çeşitli saldırılara maruz kalabilmektedir. Bu saldırılardan korunmak için güçlü güvenlik tedbirlerinin alınması gerekmektedir. Bu nedenle KAA'larda yönlendirme işlemi için çeşitli güvenlik ihtiyaçları oluşmaktadır. Özellikle yönlendirmeyi hedef alan saldırılar bulunmaktadır. Bu saldırılara karşı çeşitli güvenlik mekanizmaları geliştirilmiştir ve saldırılara karşı korunma sağlanmıştır. Bunun dışında ise bazı güvenli yönlendirme protokolleri ile yönlendirme işlemi güvenli hale getirilmeye çalışılmıştır. Bu makalede çeşitli yönlendirme saldırıları incelenip, bu saldırılara karşı geliştirilen savunma mekanizmaları üzerinde durulmaktadır. Tablo 1'de bu mekanizmalar özetlenmektedir. Ayrıca literatürdeki güvenli ve enerji etkin yönlendirme protokolleri incelenmiş ve özetlenmiştir. Geliştirilen protokollerin ne tür saldırılara karşı güvenlik sağladığı ve hangi güvenlik gereksinimlerini oluşturduğu Tablo 2'de gösterilmektedir. Buna göre bazı protokoller belirli saldırılara karşı güvenlik sağlarken, bazı protokoller ise tüm saldırılara karşı tam bir koruma sağlamaktadır. Ayrıca, gizlilik, bütünlük, kimlik doğrulama, kullanılabilirlik, veri güncelleme, dayanıklılık, hayatta kalma gibi güvenlik gereksinimleri tanımlanmaktadır. Bazı çalışmalarda ise güvenliğin sağlanmasının yanında enerji etkinliğinin de sağlanması ana amaçlar arasında gösterilmiştir. Böylece güvenli yönlendirme protokolleri ile güvenlik sağlanırken, gereksiz enerji tüketimi azaltılarak düğümlerin yaşam süreleri uzatılmıştır. Tablo 3'te ise bu protokoller sunulmaktadır. Enerji etkin güvenli bu protokoller paket düşürme, yönlendirme bozma, yanlış paket enjektisi, hatalı rapor enjektisi gibi saldırılara ve ele geçirilmiş düğümlere karşı etkinlik sağlamaktadır. Ayrıca kimlik doğrulama, gizlilik ve veri güncelliği gibi güvenliğin unsurları sağlanmaktadır. Enerjinin korunumu için 1) tekli-yol yönlendirme mekanizması, 2) yanlış bir düğümün çıkış düğümüne ulaşmaması için yol üzerinde düşürülmesi, 3) ağaç yapısının ağ omurgası olarak oluşturulmasını sağlayan enerji farkında organizasyonlar ve 4) kalan enerjinin bilgi ve yönetimi ile güven değerleri sayesinde etkin bir yönlendirmenin oluşturulması sağlanmaktadır.

Sonuç olarak, üzerinde durulan protokoller incelendiğinde her bir protokolün etkin olduğu saldırı türü, güvenlik gereksinimi ve özellikleri farklıdır. Uygulama alanının gereksinimine göre Tablo 2 ve Tablo 3'te özellikleri verilen protokollerden uygun olanı tercih edilmelidir.

KAYNAKLAR

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, Volume 38, Issue 4, 15 March 2002, pp. 393-422.
- [2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, 2008 pp. 2292-2330.
- [3] E. Sabbah, K. D. Kang, "Guide to Wireless Sensor Network: Security in Wireless Sensor Network," Chapter 19, pp. 489-490
- [4] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, 2003, pp. 293-315.
- [5] J. Kur, "Secure Routing Protocols for Wireless Sensor Networks," Yüksek Lisans Tezi, Masaryk University Faculty of Informatics, 2008.
- [6] E. Shi, A. Perrig, "Designing Secure Sensor Networks," *IEEE Wireless Communications*, 2004
- [7] J. P. Walters, Z. Liang, W. Shi, ve V. Chaudhary, "Wireless Sensor Network Security: A Survey," *Security in Distributed, Grid, and Pervasive Computing*, Chapter 17, 2006 Auerbach Publications, CRC Press.
- [8] A. Perrig, J. Stankovic ve D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.
- [9] X. Chen, K. Makki, K. Yen ve N. Pissinou, "Sensor Network Security: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, 52-73, 2009.
- [10] M. Megdadi, S. Özdemir, İ. Güler, "Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler," *Bilişim Teknolojileri Dergisi*, Cilt: 1, Sayı: 1, Ocak 2008.
- [11] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1, pp. 117-125, 2009.
- [12] E. B. Ceyhan, Ş. Sağiroğlu, "Kablosuz Algılayıcı Ağlarda Güvenlik Sorunları ve Alınabilecek Önlemler," *Politeknik Dergisi*, vol. 16, no.4, pp. 155-163, 2013.
- [13] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *ACM Journal of Wireless Networks*, vol. 8, no.5, 521-534, (2002).
- [14] S. Özdemir, Y. Xiao, "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview," *Computer Networks*, vol. 53, pp. 2022-2037, 2009.
- [15] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks," *IEEE Commun. Surveys Tutorials*, vol 8, pp. 2-23, 2006.
- [16] A. K. Pathan, H. W. Lee, C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," *ICACT*, pp. 1043-1048, 2006.
- [17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications*, May 2003, pp. 113-127.
- [18] M. Sadeghi, S. Alam, E. A. Gharb, "Security Analysis of Routing Protocols in Wireless Sensor Networks," *IJCSI International Journal of Computer Science Issues*, vol. 9, Issue 1, no 3, pp. 465-472, January 2012.
- [19] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks : analysis and defenses,". *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259-268, ACM Press., 2004.
- [20] Y.-C. Hu, A. Perrig, D.B. Johnson, "Packet leases: a defense against wormhole attacks in wireless Networks", in: *IEEE Infocom*, 2003.
- [21] V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks," *Wiley Inter Science*, 2006.
- [22] D. Anthony, L. F. Wood, J. A. Stankovic, T. He, "Sigf: a family of configurable, secure routing protocols for wireless sensor networks," *In SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pp 35-48, New York, NY, USA, 2006. ACM Press.
- [23] B. Blum, T. He, S. Son, and J. Stankovic. "Igf: A state-free robust communication protocol for wireless sensor Networks,". In *Technical Report, CS-2003-11. Department of Computer Science, University of Virginia, USA, 2003.*
- [24] X. Wang, L. Yang, ve K. Chen., "Sdd: Secure directed diffusion protocol for sensor Networks,". *In Security in Adhoc and Sensor Networks*, vol. 3313/2005 of Lecture Notes in Computer Science, pages 205-214, First European Workshop, ESAS 2004.
- [25] C. Intanagonwiwat, R. Govindan, ve D. Estrin. "Directed diffusion: a scalable and robust communication paradigm for sensor Networks,". *In MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 56-67, New York, NY, USA, 2000. ACM Press.
- [26] A.Perrig, R. Canetti, D. Song, ve D.Tygar. "Efficient and secure source authentication for multicast," *Proceedings of the Internet Society Network and Distributed System Security Symposium*, pp.35-46, 2001.

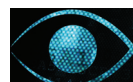


- [27] S.-B. Lee ve Y.-H. Choi., "A secure alternate path routing in sensor Networks,". *Computer Communications*, vol. 30, issue 1, pp 153–165, December 2006.
- [28] B. Parno, M. Luk, E. Gaustad, ve A. Perrig. Secure "Sensor Network Routing: A Clean-Slate Approach,". *In CoNEXT*, pp. 11-24, 2006.
- [29] J. Deng., R. Han, & S. Mishra., "INSENS: intrusion-tolerant routing in wireless sensor Networks,". Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado at Boulder.
- [30] A. Perrig, R. Canetti, J.D. Tygar, ve D. Song, "Efficient authentication and signing of multicast streams over lossy channels", *IEEE Symposium on Security and Privacy*, pp. 56-73, 2000.
- [31] J. Sen, & A. Ukil., "A secure routing protocol for wireless sensor Networks,". *Proceedings of the International Conference on Computational Sciences and its Applications (ICCSA'10)*, pp. 277 – 290, Fukuoka, Japan, 2010.
- [32] S.-B. Lee, & Y.-H. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor Networks,". *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 59-70, 2006.
- [33] H. W. Ferng, D. Rachmarini, "A Secure Routing Protocol for Wireless Sensor Networks with Consideration of Energy Efficiency," *IEEE Network Operations and Management Symposium (NOMS)*, pp. 105-112, 2012.
- [34] A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", *Annales des Telecomm.*, pp. 529–541, 2008.
- [35] K. Lin, Ch. F. Lai, X. Liu, X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks," *Mob. Netw. Appl.* vol. 17, pp. 75-89, 2012.

F. YILDIRIM OKAY 2010 yılında Çankaya Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. Aynı üniversitenin İşletme Bölümünden Çift Anadalı bulunmaktadır. 2013 yılında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünden yüksek lisans derecesini almıştır. Aynı bölümde Araştırma Görevlisi olarak çalışmakla birlikte Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora çalışmalarına devam etmektedir. Kablosuz algılayıcı ağlar, güvenlik, yapay zeka konularında çalışmaktadır.

S. ÖZDEMİR yüksek lisans derecesini 2001 yılında Syracuse Üniversitesinden almıştır. Doktora derecesini 2006 yılında Arizona State Üniversitesinden almıştır. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliğinde öğretim üyesi olarak çalışmaktadır. Algılayıcı ağlar, kablosuz ağlar, ağ güvenliği ve veri madenciliği konularında çalışmaları bulunmaktadır.

Ş. SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizli ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar; sosyal ağlar gibi konularda çalışmaktadır. 100'e yakın SCI tarafından taranan uluslararası dergilerde yayımlanmış makalesi, 100'ün üzerinde ulusal dergilerde yayımlanmış makalesi, 200'ün üzerinde uluslararası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş pek çok bildirisi bulunmaktadır. Ayrıca, bilgi güvenliği ve biyometrik alanında alınmış patentleri bulunmaktadır.



Attack Tree Visualization for Cyber Security Situational Awareness

M. Selvi, E. B. Aksu, M. H. Dilek, A. Erkan, and M. U. Demirezen

Abstract— Situational awareness in cyber domain is one of the key features for quick and accurate decision making and anomaly detection. In order to provide situational awareness, certain methods have been introduced so far and attack graph is one of them. Attack graphs help the security analyst to visualize the network topology and understand typical vulnerability and exploit behaviors in cyber domain (e.g., IT asset and the network). They provide more proactive view compared to other reactive views; hence risk management and evaluation can be done in an efficient and interactive fashion. Attack trees can be used for various purposes since they can map network assets, network attacks and possible vulnerabilities which may exist in the IT assets. This study introduces an integrated cyber security capability called, BSGS, which can help analysts to create attack trees, identify vulnerabilities and have effective risk assessment procedures. In this way, the cyber security specialists will have a more efficient and holistic way to assess their environments and take the most effective precautions to minimize cyber risks.

Index Terms—attack graph, attack tree, cyber security, risk assessment, situational awareness

I. INTRODUCTION

THROUGHOUT the 2000s, the term, cyber security, has become a household term. Cyber attacks became more frequent than ever. Serious and coordinated attacks had been experienced all over the world and the damages were quite non-ignorable. Thus, for the last ten years the nation states started to invest more in developing their own security and defense systems and make their preparations to fight with cyber threat. So, a new era was born as a fifth to modern warfare and the term, cyber security and defense, began to be heard more in nation states and military organizations such as NATO [1].

Cyber security can be defined as the information security for protection of cyber space and assets including tools, policies, security safeguards, guidelines, risk management approaches, assurance and technologies, etc... [2] In this cyber space, including users, networks and devices, the main objective is to secure and store data safely by means of comprising CIA (Confidentiality, Integrity and Availability) and enable uninterrupted and secure operation of business [2].

M. Selvi, E. B. Aksu, M. H. Dilek, A. Erkan, and M. U. Demirezen, STM Cyber Security Group

With increasing needs in cyber security platform, quick and accurate decision making become more and more important for being aware of the attacks and reacting as fast as possible [3]. For this reason, cyber situational awareness started to play a critical role and the need for systems having such capabilities has increased. Situational awareness provides the processes identifying both domain specific and cross domain activities [3]. These processes can be related to the system environment, the domains, the aims and the decisions of the users.

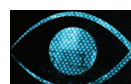
In order to provide situational awareness, attack visualization is a must to help decision makers to understand the baseline behaviors and detect anomalies in a network [4]. Several visualization methods have been introduced since the situational awareness against cyber attacks started to be a must-have capability. Among them, the most popular one is attack graphs. By using them, security specialists can detect critical security bottlenecks and identify vulnerabilities which are at the heart of particular system [5].

There are many ways to represent attacks. One of them is using attack trees. It is the best known way to categorize the attacks with different nature which target the defended networks [6]. Firstly introduced by Schneier [7], [8], it has become the most trustworthy and consistent way to detect vulnerabilities proactively [1]. This graphically structured tree notation is also selected as an easy and understandable way for implementing attack vector.

In this study, brief information about the terms - situation awareness, attack graphs and attack trees - will be given and Integrated Cyber Security System (Turkish: Bütünleşik Siber Güvenlik Sistemi, "BSGS") will be introduced as the answer to these needs. This system uses attack trees in order to evaluate risks based on vulnerabilities and calculate multi-step attacks. By using vulnerabilities and risks, the system maps the paths of attacks and gained privileges of attackers. The system provides an interactive method which helps the defenders to take necessary precautions before the attack occurs.

II. BACKGROUND

In this chapter, the background of situational awareness, attack graphs and attack trees has been explained briefly.



A. Situational Awareness

Cyber Situational Awareness (CSA) can be described as the traditional Situational Awareness (SA) which is applied to computer networks [9]. The main idea of situational awareness in cyber domain is to analyze the surroundings in cyber domain and creating certain events and visualizations for the purpose of efficient and fast decision making.

Another aim is to prioritize the attacks as all the attacks don't have the same impact over the defended network and system [9]. Hence, the analyst should prioritize the sub-systems and assets first since the impact of attack is determined by the importance of the asset. Then, based on the findings, the critical attacks should be taken into consideration for mitigation planning. It shouldn't be forgotten that the cyber situational awareness of an organization reflects the effectiveness of response to attacks.

According to [10], Situational Awareness for Cyber Defenses includes 7 basic aspects: "Being aware of a. current situation, b. impact of attack, c. how situations evolve, d. actor behavior, e. why and how the current situation is caused, f. quality and how plausible futures of the current situation." Based on this definition, it can be said that situational awareness provides the user the closer view and detailed inspection of network.

Providing the notion of 'situational awareness' will be challenging because of certain rigors in CSA [9]. Firstly, identifying missions will not be so easy that even some organizations don't know their cyber-missions. Moreover, they usually have neither any sufficient tracking mechanisms in their networks nor sensors which will warn them for attacks. Under these circumstances, it is really difficult to have an effective situational awareness. The best solution can be identifying the critical missions which the organization has; then implementing the tracking mechanisms and finally defining proactive solutions for the security of network.

Several studies have been made in this field. While some of the studies [3][10] generally describe the term of situational awareness and standard methods and applications which have been used in order to maintain it; others focus on more specific methods such as real time multistage attack awareness and mission-centric cyber situational awareness [11], [12].

B. Attack Graphs

Attack graphs are valuable analysis results for cyber defense and situational awareness that can map possible paths of attacker who aims to get access by means of infiltrating to a specific network [5]. Attack graphs have multiple capabilities such as [5]:

- network topology creation,
- understanding baseline behavior in network traffic,
- vulnerability and risk classification,
- more proactive perspective instead of reactive.

Topological Vulnerability Analysis (TVA) is one of the well-known methods that can provide user to monitor the current conditions of network assets and create the models of network vulnerabilities and actual risks [13], [14], [15]. It

produces a model by calculating both the individual and combined vulnerabilities. The main output of this security method is the attack graphs which show all the possible paths of an attacker that might infiltrate the network. One of the biggest advantages of TVA is that the raw asset and vulnerability related data gets transformed into meaningful information which shows the possible attacks. By using this information, one can proactively manage risks related to possible attacks and take precautions. If the analyst can do this analysis in real-time, then a just-in-time situational awareness can be achieved.

Recently, new techniques were introduced to visualize attack graphs [16]. The main aim of these attack graphs is to reduce complexity and portray the attack flows in a relatively simple and clear fashion. Attack graph views can be coordinated and the user can have a broader view of the network topology and attack vector [16]. These techniques can be used either independently or in a combined way based on the network complexity. This provides diversity that all has different uses having different properties and perspectives. A brief illustration of the techniques for attack graphs can be found in [16]:

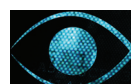
--*Attack Graph Adjacency Matrix Visualization* is used to understand the attack correlation, prediction and association in network attack graphs [17]. It is applied for showing gained access of attacker across the network and predicting all possible paths of the attacker. Based on the collected output, the impact of output is identified and it gives the ability to prioritize attacks according to the impact levels. Adjacency Matrix may be a standalone method as it requires network attack graphs for finding correlations and making predictions [17].

--*Interactive Attack Graph Filtering* is one of the useful methods if the user has larger network. It helps to filter the graph by using a selected schema [16]. Like attack trees, interactive attack graph filtering creates tree widgets to navigate through network. In this way, the user has the chance to focus on the network topology deeply and run through the network step-by-step with the help of penetration testing [16].

C. Attack Trees

Attack trees play a significant role in specifying system security and network in terms of vulnerability and risk identification [18]. They can be mapped in various forms. Mostly, while nodes represent attacks, the root node is the global goal of the attacker which can also described as an event [6]. Child nodes are the refinements of this goal and branches are the attacker's path which cannot be refined anymore. Each path in attack tree represents a unique attack. Moreover, attack trees can also be prepared textually instead of graphically. In textual form, the 'AND' and 'OR' decompositions are used and the consequences of achieve sub-goals were presented by them.

Attack patterns can be defined in order to increase the practicality of attack trees generation and reuse [19]. Attack pattern is the mapping of different types of attacks that



includes a. the goal of the specified attack, b. the preconditions for use, c. the steps for practicing attack, d. postconditions which are true if the attack is made successfully [19]. The preconditions contain assumptions which are related with the expected behaviors of attacker and the characteristics of the attack. The skills, resources, access and knowledge can be given as an example to preconditions [19]. On the other hand, postconditions cover the gained privileges when the attack was resulted successfully.

Attack trees have been used in many various ways and one of the previous studies is related to Supervisory Controls and Data Acquisition (SCADA) protocols [20]. These protocols are communication protocols which are used for exchange of control messages in industrial networks. The use of attack trees for SCADA is based on accessing vulnerabilities and the main purpose is analyzing the measurable goals and structured elaboration of events such as specific attack goals [20]. Like designing the attack patterns in textual way, the study focuses on 'AND' and 'OR' compositions in order to access vulnerabilities.

III. BSGS

In this part, the capabilities, architecture and operational scenario of BSGS and the attack trees generated by the system will be introduced.

A. Capabilities

BSGS integrates and centrally manages vulnerability, network topology and IT assets information collected from the organizational units and backbone network. The prototype calculates the most effective cyber attacks to be carried out by cyber-attackers and attack trees showing the possible attack vectors (vulnerability, topology, etc.) through which they can perform attacks. With the help of the attack tree, BSGS users can calculate the risks inherent in systems and analyse possible remediation.

In addition to the above-mentioned capabilities, BSGS can gather system and application logs and sensor alerts in real time all over the network through a central coordination unit. All collected data are correlated and users are informed by a "Common Operational Picture" that provides cyber situational awareness. It is composed of vulnerability, assets, risks and instant status information such a consolidated cyber security picture allows decision-makers to make integrated risk analysis and corrective action planning.

The developed prototype system has been evaluated in many cyber security scenarios. This evaluation is not only a classic software testing approach; but also the evaluation of effectiveness of the system from the perspective of cyber security experts. As a result of the scenario analysis, it has been evaluated that the competency of BSGS system is within the targeted scope of risk assessment, proactive defense planning, analysis of past cyber action and creation of consolidated cyber security situation picture.

BSGS also benefits from a distributed data processing infrastructure. As a prerequisite, the components, providing

the collection of static event and instant event logs, have to be deployed in the organizational unit. Each organizational unit has its own clients and servers and applications running on them and network devices such as IDS, IPS, firewall, etc... Then, this collected information is sent to a coordination center (cyber security operation center). Collected data is merged by using data fusion in order to create an integrated common picture.

BSGS project offers very important gains. With BSGS, foundations of a centre of excellence have been laid. This will be a center where new threats and methods of Cyber Attacks that may arise in the future can be tested and measures can be developed. Thanks to the flexible and scalable technical infrastructure of the BSGS, which has been developed under an R&D project, a long term, easily extendable system has been put into practice. Moreover, a Cyber Security Ontology and National Vulnerability Database have been provided and the infrastructure, which will lead to the formation of the inter-institutional and in-house Cyber Security processes and their coordination structure, has been prepared.

B. Architecture and Operational Scenario

In the following the main sub-systems of BSGS can be found:

- Vulnerability Analysis and Risk Management
- National Vulnerability Database (YZV)
- Attack tree creation infrastructure
- Organizational Cyber Security Application
- Integrated Cyber Security Application
- Central event logger and correlator (SIEM)

Figure 1 illustrates also the main tasks and componens of BSGS.



Fig. 1. BSGS main tasks and componens

ATTACK TREE VISUALIZATION FOR CYBER SECURITY SITUATIONAL AWARENESS

The operational scenario is as follows:

- Synchronization of vulnerabilities data in NVD (National Vulnerability Database) with local vulnerability database,
- Evaluation of vulnerabilities by analysts,
- Scanning the network topology, asset and vulnerability,
- Collection of static information (the results of scanning) in the coordination center,
- Identification of threat based on assumptions,
- Score and attack tree production based on threats,
- Collection of dynamic information and sending the coordination center,
- Correlation of event logs,
- Visualization of all information collected in the center and creation of integrated cyber security situational awareness common picture. In the following figure, the architecture of BSGS can be found.

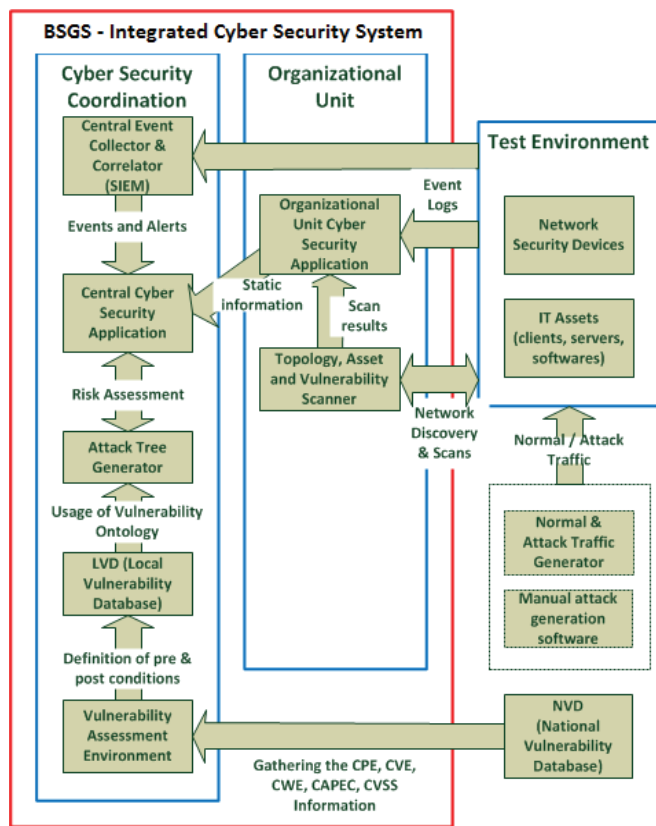


Fig. 2. BSGS is composed of three sub-systems which are cyber security coordination center, organizational unit and test environment

C. Attack Trees

The main aim of using attack trees is to find out which types of attacks may be experienced because of critical vulnerabilities and to identify ways of attacks by using assets in the network. Moreover, with the help of attack trees the risks will be calculated and the precautions against attacks will be analyzed and prioritized. In this way, possible risks are identified and arranged in an order based on their risk scores.

While creating attack trees, web ontology language (OWL) is used for discovering the steps (attack tree nodes) and transitions -by using vulnerability- between steps. OWL interpretation requires huge memory and processing power. To overcome this performance bottleneck, attack trees are distributed in parallel fashion. Moreover, instead of creating attack tree by adding the devices one-by-one, the devices which have the same level of accessibility are united and their vulnerabilities are integrated. It is also assumed that possible attacks can affect all clustered devices. In this way, attack trees for very large networks can be processed faster. In the figure 3 and 4, both network and logical topology of the sample system are illustrated. Also, in the figure 5 the illustration of attack tree is shown including the starting point and target system.

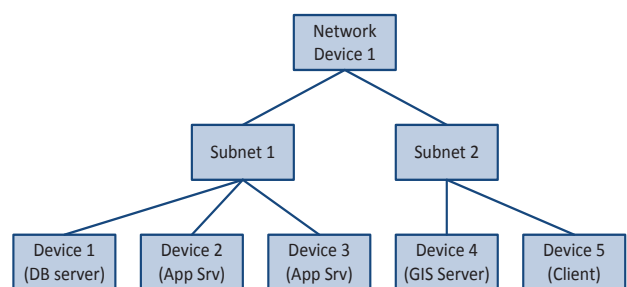


Fig. 3. The network topology of the sample system.

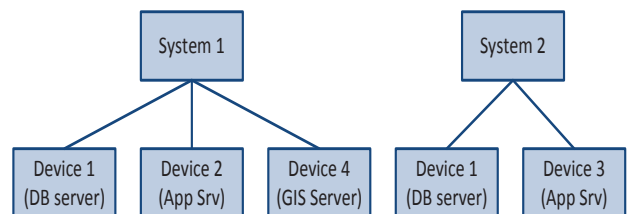


Fig. 4. The sample system's logical topology, showing the business structure of the organization, was illustrated.

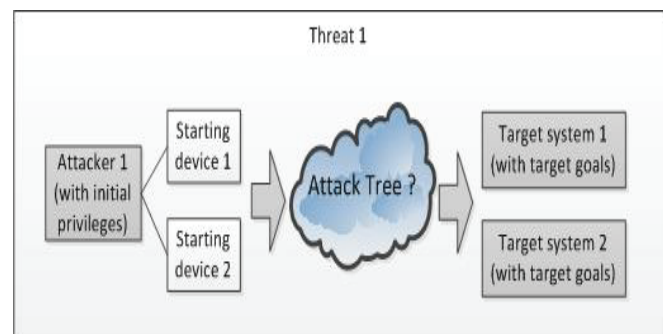


Fig. 5. The main idea of generating attack tree is to show the attacks on a target system where there is an attacker and a starting point (e.g. a compromised device)

The infrastructure of distributed simulation and attack tree gives the possibility of using vulnerabilities coming from local vulnerability database, vulnerability and attack ontology and ontology reasoning engine; then creates the attack tree which

shows the attack paths - which may give harm to system - by evaluating vulnerability preconditions and postconditions. In attack tree, the visualization is based on vulnerabilities. An attack tree node includes a. the device b. vulnerability which is the source of an attack to this device (including pre/post conditions), c. gained privilege as a result of this attack on this device. Afterwards, by using attack trees, impact scores of the vulnerabilities and criticality levels, risk analysis is made and risk scores are calculated for each path in an attack tree. In the appendix, the sample of attack tree can be seen. In figure 6 the necessary input for generating attack tree can be seen in a detailed way.

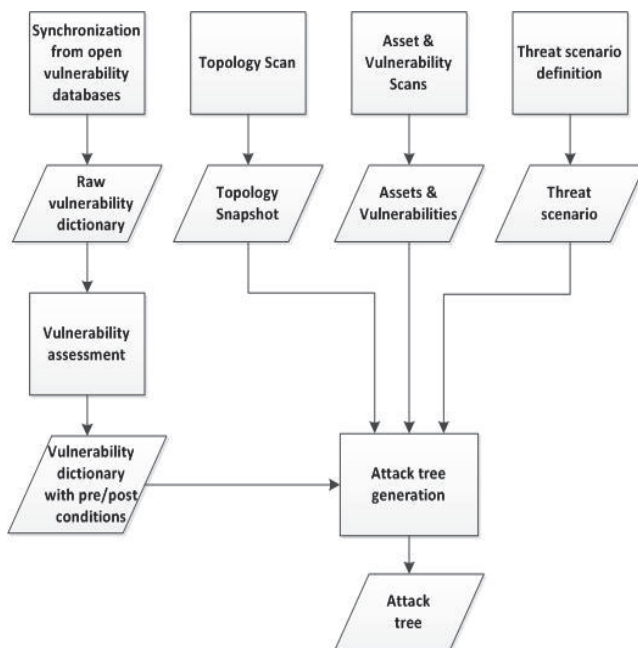


Fig. 6. The collection of vulnerabilities, assets and threats are processed in different ways and then they are all united in attack tree generation process.

IV. CONCLUSION

It is certain that the cyber security plays an important role in the protection of IT systems and critical infrastructures. Both proactive and reactive precautions are needed to provide a holistic security approach and situational awareness is essential for making the necessary decisions. Situational awareness is not only used for analyzing the networks and systems; but also needed for fast and accurate decision making. For providing situational awareness in the systems, attack graphs are mainly used to understand baseline behavior of an IT system and detect anomalies in real time. Attack graphs are effective tools which can map possible paths of the attacker through the target source. There are several methods to represent attack graphs as all have different functionalities.

One of them, tree structure, has been used in many ways in IT sector; attack trees provide an effective means of attack visualization in cyber security domain. In this study, an integrated cyber security system, BSGS, is explained as a combination of different cyber security capabilities including attack trees. Attack trees provide a considerable amount of

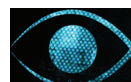
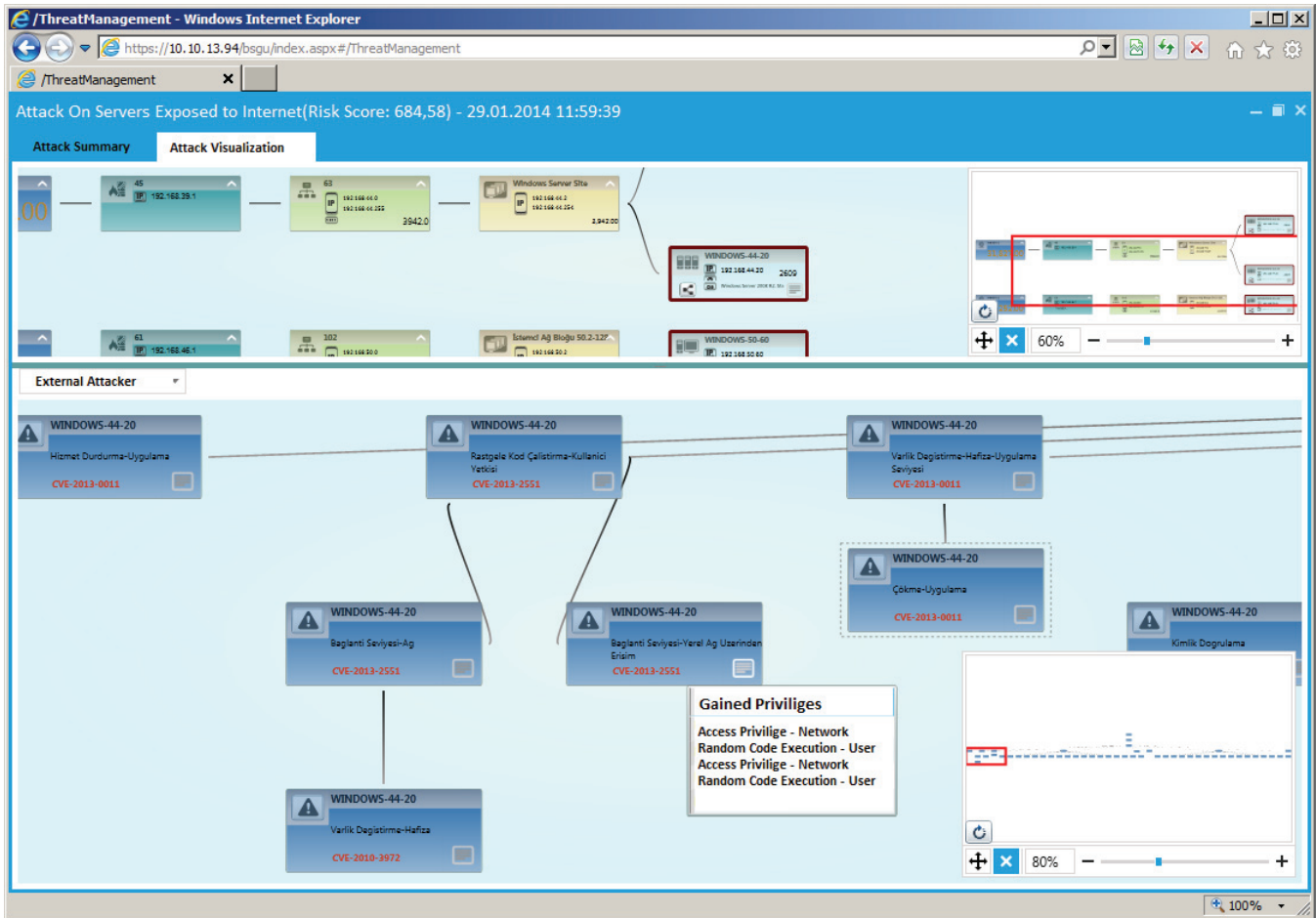
dynamism to the system as it helps users to make risk assessment and management by prioritization. Visualization of such information can help the decision makers to be more efficient and have a higher sense of governance from cyber security perspective.

REFERENCES

- [1] M. Yayla, "Cyber War As A Legal Term," USA, The City University of New York John Jay College, 2013.
- [2] *Overview of cybersecurity, ITU-T Telecommunication Standardization Sector Of ITU, Series X: Data Networks, Open System Communications and Security, Recommendation ITU-T X.1205, 2008 Available: https://www.itu.int/rec/T-REC-X.1205-200804-I.*
- [3] G. P. Tadda, J. S. Salerno, "Overview of Cyber Situation Awareness," in *Cyber Situational Awareness Issues and Research*, vol. 46, Springer, 2010, pp. 15-35.
- [4] D. M. Best, S. Bohn, D. Love, A. Wynne, and W. A. Pike, "Real-time visualization of network behaviors for situational awareness," in *Proc. Seventh International Symposium on Visualization for Cyber Security*, New York, 2010, pp. 79-90.
- [5] K. Ingols, R. Lippman, and K. Piwowarski, "Practical Attack Graph Generation for Network Defense," in *Proc. 22th Annual Computer Security Applications Conference(ACSAC'06)*, MIT Lincoln Laboratory 2006, pp. 121-130.
- [6] S. Mauw, M. Oostdijk, "Foundations of Attack trees," in *Proc. ISISC 2005 Information Security and Cryptology*, v. 3925, 2006, pp. 186-198.
- [7] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's journal, 1999.
- [8] B. Schneier, "Secrets & Lies: Digital Security in a Networked World," Wiley, 2000.
- [9] A. Doupe, M. Egele, B. Caillat, G. Stringhini, G. Yakın, A. Zand, L. Cavedon, and G. Vigna, "Hit'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness," in *Proc. 27th Annual Computer Security Applications Conference*, 2011, pp. 51-61.
- [10] L. D. Cumiford, "Situation Awareness for Cyber Defense," *Information for the Defense Community*, 2006.
- [11] S. Mathew, D. Britt, R. Giomundo, and S. Upadhyaya, "Real-Time Multistage Attack Awareness Through Enhanced Intrusion Alert Clustering," in *Proc. Military Communications Conference*, 2005, pp. 1801-1806.
- [12] S. Jajodia, S. Noel, P. Kalapa, and M. Albanese, "Cauldron mission-centric cyber situational awareness with defense in depth," in *Proc. Military Communications Conference*, 2011, pp. 1339-1344.
- [13] S. Jajodia and S. Noel, "Topological Vulnerability Analysis," in *Cyber Situational Awareness Advances in Information Security*, v. 46, Springer, 2010, pp. 139-154.
- [14] S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis of Network Attack Vulnerability," in *Managing Cyber Threats: Issues, Approaches and Challenges*, v. 46, Springer, 2005, pp.247-266.
- [15] S. Jajodia and S. Noel, "Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response," in *Proc. Algorithms, Architectures and Information System Security*, New Jersey, 2009, pp. 285-305.
- [16] S. Noel, M. Jacobs, P. Kalapa, and S. Japodia, "Multiple Coordinated Views for Network Attack Graphs," in *Proc. IEEE Workshop on Visualization for Computer Security*, 2005, pp. 99-106.
- [17] S. Noel, "Understanding complex network attack graphs through clustered adjacency matrices," in *Proc. 21st Annual Computer Security Applications Conference*, 2005, pp. 10-169.
- [18] I. Ray and N. Poolsapassit, "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders," in *Proc. Computer Security - ESORICS 2005 Lecture Notes in Computer Science*, v. 3679, 2005, pp. 231-246.
- [19] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack Modeling for Information Security and Survivability," Carnegie Mellon Software Engineering Institute, 2001.
- [20] E. J. Byres, M. Franz, and D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems," in *Proc. International Infrastructure Survivability Workshop (IISW'04)*, Institute of Electrical and Electronics Engineers, Lisbon, 2004.

ATTACK TREE VISUALIZATION FOR CYBER SECURITY SITUATIONAL AWARENESS

APPENDIX



Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörülleri

G. Şengül, F. K. Atsan, ve A. Bostan

Özet—Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesi süreçlerini kapsayan adli bilişim, bilişim hukuku alt alanına yardımcı bir disiplindir. Adli bilişim kapsamında sayısal sistemler üzerinde inceleme yapmak ve delil araştırmak oldukça karmaşık teknik bilgiye hâkim olmayı gerektirmekte ve aynı zamanda bu sistemlerdeki veri ve kayıtların çok büyük boyutlarda olması nedeni ile bu süreçler çok zahmetli ve zaman alıcı olabilmektedir. Hiç şüphesiz adli bilişim incelemesi kendine özel cihaz, sistem ve yazılımlara ihtiyaç duymaktadır. Bu alanda teknik inceleme yapan şahıslar da adli bilişim uzmanı/bilirkişisi olarak adlandırılmaktadır. Bu çalışmada ulusal ve uluslararası düzeyde adli bilişim ile ilgili durum tespiti yapılmış, alandaki problemler ve çözüm önerileri sunulmuş ve adli bilişimle ilgili gelecek öngörülleri vurgulanmıştır.

Anahtar Kelimeler—Adli bilişim, sertifikasyon, araçlar, adli bilişim uzmanı

I. GİRİŞ

SAYISAL ortamlar ve bilgi sistemleri kullanımı toplumsal hayat ve iş dünyasının vazgeçilmezi haline gelmiştir. İnsan yaşantısının ve etkileşimlerinin sayısallaşması ile sayısal ortamlardaki bir kısım olay ve etkileşimler de hukuki anlamda suç kabul edilmeye başlamıştır. Bu alanda ilk adli uygulamalara dünya genelinde 1970 sonlarında rastlanırken [1] ülkemizde bu kapsama girebilecek ilk uygulamalara 1990'lı yıllardan sonra rastlanmaktadır [2]. Sayısal ortamlarda gerçekleştirilen bazı eylemlerin suç kabul edilmesi ise, sayısal delil kavramını da beraberinde getirmiştir. Zira bu ortamlarda gerçekleştirilen eylemlerin iz ve kayıtları yine bu ortamlarda bulunmaktadır. Buna ek olarak, gelişen sayısal cihaz kullanımı ile daha önceden sayısal olmayan birçok bilgi ve kayıt sayısal hale gelmiş ve dolayısı ile bu bilgiler adli olay incelemelerinde kullanılmaya başlamıştır. Örneğin bir kişi veya aracın belirli zamanlarda nerede bulunduğu göstergesi olarak cep telefonu veya GPS cihazının sistem üzerindeki kayıtları kullanılabilir.

Gelişen teknoloji sayesinde, daha ekonomik ve daha yüksek performanslı sayısal sistemlerin izleme ve güvenlik amaçları

ile kullanılması da sürekli artış göstermektedir. Bu tür cihaz ve sistemlerde de delil araştırması ve olay incelemesi için sayısal teknik bilgiye ihtiyaç duyulmaktadır. Gönümüzde kayıt yapan sayısal güvenlik kamera sistemlerine hemen hemen her yerde rastlamak mümkündür.

Toplum yaşamını inkâr edilemez şekilde değiştiren sayısal sistemler, aynı zamanda suç işlenmesini ve delil yok edilmesi/karartılmasını da daha kolay hale getirmiştir. Artık başkalarına ait cihaz, sistem ve bilginin kullanılması, alınıp-satılması veya bozulması-kullanılmaz hale getirilmesi için çoğu kez aynı fiziki ortamda bulunmaya veya fiziki temasa gerek duyulmamaktadır. Coğrafi ve fiziki engeller suçun engellenmesinde etkisiz kalmaktadır. Ayrıca sayısal teknoloji ile sayısal sistemler üzerinde adli delil olarak kullanılabilir iz ve bilgileri de değiştirmek veya yok etmek daha kolay hale gelmiştir.

Sayısal sistemler üzerinde delil ve adli olay incelemesi yapabilmek özel bilgi ve tecrübe gerektirmektedir. Bu alanda adli süreçlere yardımcı olacak ve bilirkişilik yapacak personelin bilgisayar ve sayısal sistemler konusunda yeterli teknik bilgiye sahip olmasının yanında, temel hukuk ve adli olay araştırma prensiplerine de hâkim olması beklenmektedir.

Bu çalışmada, adli bilişim araştırmalarının Türkiye ve dünyadaki genel durumu hakkında özet bilgi verilmekte, sorun ve problemler ortaya konarak çözüm önerileri sunulmaktadır.

II. ADLI BİLİŞİMİN TANIMI VE MEVCUT DURUM

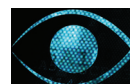
A. Adli Bilişimin Tanımı ve Adli Bilişim Uzmanlığı

Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesi süreçlerini kapsayan adli bilişim, bilişim hukuku alt alanına yardımcı bir disiplindir [3]. Zira hızla gelişen, teknolojisi değişen ve her geçen gün yaygınlaşan sayısal sistem ve cihazlar aracılığı ile gerçekleştirilen suçların ve olayların incelenmesi özel teknik bilgi ve altyapıya ihtiyaç duymaktadır. Dilimizde adli bilişim olarak yaygın olarak kullanılan, bu disiplinin farklı tanımları vardır. Bu tanımlardan örnek olabilecek üç tanesi şu şekildedir.

Gökhan Şengül, Atılım Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak çalışmaktadır; e-posta: gokhan.sengul@atilim.edu.tr).

F.K.Atan., TÜRKİSAT A.Ş. 40 km. Gölbaşı, Ankara da kıdemli güvenlik uzmanı olarak çalışmaktadır. (e-posta: fkatsan@turksat.com.tr).

Atıla Bostan, Atılım Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak çalışmaktadır; e-posta: atila.bostan@atilim.edu.tr).



- 1) *Adli olayların aydınlatılması amacıyla, olay yerinden, dijital veri saklama ve ileme özelliğine sahip cihazların toplanması, cihazların içerisindeki dijital delillerin tespit edilmesi ve adli otoritelere dijital delillerin raporlanması süreci içerisinde yapılan çalışmaların bütünü* [4]
- 2) *Elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci* [3]
- 3) *Bir olayın aydınlatılmasına yönelik olarak, olayla ilgili bilgi içerebilecek bilişim cihazlarının incelenmesi* [5].

Örnek tanımlarda da görülebileceği gibi, adli bilişim kavramının hukuki yönünden daha ziyade teknik yönü daha ön plandadır. Sayısal sistemler üzerinde inceleme yapmak ve delil araştırmak oldukça karmaşık teknik bilgiye hâkim olmayı gerektirmekte ve aynı zamanda bu sistemlerdeki veri ve kayıtların çok büyük boyutlarda olması nedeni ile bu süreçler çok zahmetli ve zaman alıcı olabilmektedir. Hiç şüphesiz adli bilişim incelemesi kendine özel cihaz, sistem ve yazılımlara ihtiyaç duymaktadır. Bu alanda teknik inceleme yapan şahıslar da adli bilişim uzmanı/bilirkişisi olarak adlandırılmaktadır. Ancak İngilizce “computer forensics”, “digital forensics” ve “network forensics” gibi tabirlerden tercüme ile dilimizde kullanılan adli bilişim terimi İngilizcede “forensics” kelimesinin tam karşılığını ifade etmemektedir. Zira “forensics” İngilizcede genellikle adli amaçlı olmakla birlikte, adli olsun veya olmasın, bir olayın nasıl gerçekleştiğine ilişkin tüm teknik incelemeleri kapsamaktadır [5]. Ancak Türkçede adli kelimesi doğrudan ve sadece adli işlemlerle ilgili kavramını çağırır. Bu açıdan değerlendirildiğinde adli bilişim olarak ifade edilen kavramın “sayısal sistem ve cihaz incelemesi” şeklinde ifadesi daha uygun olabilir.

Adli bilişim disiplininin çalışma alanları gelişen teknoloji ve kullanım yaygınlığına bağlı olarak sürekli olarak artmakta ve kapsamı gelişmektedir. Ancak çalışma konuları ana başlıklar halinde şunlardır;

- Sistem (işletim sistemi veya uygulama) kayıtlarının incelenmesi
- Farklı sistemler arasında kayıt ilişkilendirilmesi ve olay/işlem takibi
- Veri saklama
- Veri kurtarma
- Veri dönüştürme
- Veri imha etme
- Şifreleme
- Şifre çözme
- Gizlenmiş dosya bulma

Bu işlemleri yaparken incelenen veya delil olabilecek sayısal bulgu ana başlıkları ise şu şekilde listelenebilir.

- Sistem olay kayıtları
- Video görüntüleri
- Fotoğraflar
- Uygulama dosyaları (Word, Excell, Open Office vb.)
- Bilgisayar programları
- Sistem veya uygulama ayarları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb.)
- Gizli ve şifreli dosyalar / klasörler

- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son gerçekleştirilen işlem kayıtları
- İnternet ortamından indirilen dosyalar
- Silinmiş dosya/klasörler

Ana başlıkları verilen bu alanlar ve kayıtların incelenmesi becerileri sadece adli olayların incelenmesinde değil son zamanlarda bazı şirket ve şahıslar tarafından kendi iç iş süreçlerinde de yoğunlukla kullanılmaya başlamıştır. Günümüzde veri kurtarma, veri imha etme gibi hizmetler adli inceleme alanı dışındaki dünyadan da yüksek oranda talep almaktadır.

Adli bilişim inceleme süreci ise en geniş anlamda aşağıda belirtilen beş aşamada gerçekleştirilmektedir. Bu aşamalar sırası ile;

- Hazırlık
- Toplama
- İnceleme
- Çözümleme
- Raporlama

şeklinde listelenir. Ancak bazı yazarlar burada belirtilen ilk aşama olan hazırlık aşamasını bu süreç dışında tutarak bu listeyi dört aşama olarak kaleme almışlardır [6].

B. Mevzuat ve Mevcut Durum

Türkiye Cumhuriyeti hukuk mevzuatında adli bilişim ile ilgili hükümler Ceza Muhakemesi Kanun (CMK) madde. 134 ile Adli ve Önleme Aramaları Yönetmeliği'nin 17nci Maddesinde yer almaktadır. Bu iki düzenlemenin dışında adli bilişim konusunda başka bir hüküm bulunmamaktadır[3]. Ancak konu ile ilgili olarak Adalet Bakanlığı'na hazırlanan “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları” başlıklı bir kanun tasarısı halen kanunlaşma aşamasındadır [7].

Ceza Muhakemeleri Kanunundaki düzenlemeler doğrultusunda, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine inceleme yapılması amacı ile savcının talebi üzerine hâkim tarafından karar verilebilmektedir [8]. Kanun gerekli ve uygun durumlarda bu bilgilerin bir kopyasının alınarak bu kopya üzerinde inceleme yapılmasına da imkân tanımaktadır. Ancak kopya alınması durumunda alınan kopyanın bir suretinin şüpheliye veya vekiline teslimini de öngörmektedir.

Adli ve Önleme Aramaları Yönetmeliği'nin 17nci Maddesinde ise kanun tarafından düzenlenen el koyma ve kopya alma işlemlerinin kapsam ve usulleri belirlenmiştir [9]. Ayrıca yönetmelikte kanunda geçen bilgisayar, bilgisayar programları ve bilgisayar kütükleri ifadelerine ek olarak uzak bilgisayar kütükleri, bilgisayar ağları ve çıkartılabilir donanımlardan da bahsedilmektedir.

Adalet Bakanlığı tarafından düzenleme çalışmaları takip edilen “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı” özellikle adli bilişim uzmanını tanımlaması açısından önemlidir. Bu hususta kanun taslağı;

- adli bilişim uzmanı yetki belgesi olanların bilirkişilik yapabileceğini
- adli bilişim uzmanlığı ve yetki belgesine ilişkin esas ve

usullerin yönetmelikle belirleneceğini

- adli bilişim uzmanları hakkında CMK'nın bilirkişilikle ilgili hususlarının uygulanacağını

düzenlemektedir [7]. Ayrıca taslağın yürürlük maddesinde adli bilişim uzmanlığı konusundaki düzenlemelerin kanunun kabulünden iki yıl sonra yürürlüğe girmesi öngörülmektedir.

C. Uluslararası Mevcut Durum

Dünya genelinde ulusal sınırları aşan bir boyutta genişleyen İnternet ağı sayesinde, sayısal sistemler üzerinden işlenen bilişim suçları çok kolay uluslararası bir boyut kazanabilmektedir. Hatta uluslararası hukuki ve teknik işbirliği noksanlığından/zorluğundan faydalanan suçlular, bu tür suç oluşturan eylemlerini özellikle uluslararası bir tasarım üzerinden gerçekleştirmektedir. Suçlular kolay erişilebilir ve genellikle denetimden uzak iletişim ağından faydalanarak uluslararası katıllımlı suç çeteleri, terörist gruplar ve menfaat birliktelikleri oluşturabilmektedir. Son yıllarda sayısal sistemler ve özellikle İnternet üzerinden siyasi amaçlı güvenlik saldırıları gerçekleştiren gönüllü saldırgan gruplarının miktarında da artışlar gözlenmektedir [10]. Ayrıca bu tür uluslararası sayısal saldırıların siyasal ve ekonomik kaygılarla diğer devletler tarafından organize edildiği ve düzenlendiği konusunda da çok güçlü iddia ve örnekler mevcuttur.

Adli olay incelemelerinde sistem ve olayların uluslararası boyut kazanması, inceleme süreçlerini ve metotlarını genellikle olumsuz yönde etkilemektedir. Bu alanda diğer suç türlerinde olduğu gibi adli inceleme yapma, kontrol ve yaptırım uygulama konularında uluslararası düzeyde beraberlik ve eşgüdümü sağlayacak antlaşma ve prensiplere ihtiyaç duyulmaktadır. Bu amaçla uzun yıllardır çeşitli resmi kuruluş ve gönüllü birlikteliklerle çabalar sarf edilmiştir. Bu çabalardan önemli olanlar şunlardır;

Birleşmiş Milletler (BM)

Birleşmiş milletler örgütü sayısal suçlar alanının Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan düzenlemeler ile kontrol etmeye çalışmaktadır. Birleşmiş Milletler bünyesindeki Uyuşturucu ve Suçlarla Mücadele Bürosu (UNODC) da sayısal suçlarla ilgilenmektedir. Sayısal suçlar konusunda ilk ITR düzenlemesi 1988 yılında kabul edilmiştir [11]. Bilgisayar suçlarının kanunlaştırılması konusundaki karar ise 1990 yılında Havana-Küba'da yapılan Sekizinci BM Suçun Önlenmesi ve Suçlu Muamelesi kongresinde imzalanmıştır [12]. BM Genel Meclisi ise 2000 yılında 55/63 numaralı kararı ile;

- Üye ülkelerin bilgisayar teknolojilerinin suç işleyecek şekilde kullanılmasına imkân tanıyan ortamların azaltılması konusunda kanun ve uygulamalar geliştireceğini garanti etmesi
- Adli sistemlerin, bilgisayar sistemlerinin ve verinin gizliliği, bütünlüğü ve erişilebilirliğini yetkisiz erişimlerden koruyup, suça yönelik kullanımların cezalandırılması

hususları imza altına alınmıştır. 2010 yılında ise yine BM Genel Meclisi tarafından sayısal suçlarla mücadele konusunda

en iyi uygulamalar, ulusal kanunlar hakkında bilgi değişimi, teknik yardım ve uluslararası koordinasyon amaçları ile çok katıllımlı çalışma grupları oluşturulmasını 65/230 numarası ile karara bağlamıştır [13]. ITR düzenlemesinin son güncellemesi ise Dünya Telekomünikasyon Konferansı (WCIT-12) esnasında 2012 yılında Dubai'de 89 ülke tarafından imzalanmıştır [14-15].

Avrupa Konseyi (Budapeşte Sözleşmesi)

Avrupa konseyi 1997 yılında Siber Uzayda Suç Uzmanları komitesini kurdu ve 2001 yılında Budapeşte Sözleşmesi olarak anılan Siber Suçlar Sözleşmesini kabul etti. Bazı raporlara göre 100'den fazla ülke kendi iç hukuk düzenlemelerinde bu sözleşmenin belirlediği esaslardan faydalanmıştır [16]. Bu güne kadar 35 ülke sözleşmeyi imzalamıştır.

İktisadi İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development: OECD)

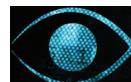
OECD bilgisayar suçları konusunda öngörülerde bulunan ilk uluslararası örgüttür [17]. Bu örgüt doğası gereği anlaşmalar imzalamamaktadır. Bunun yerine dünya çapında koordine edilmiş bir politika oluşturmaya çalışmaktadır. OECD bünyesinde kurduğu çeşitli çalışma grupları aracılığı ile 2002 yılında "Bilgi Sistemleri ve Ağ Güvenliği: Güvenlik Kültürüne Doğru"[18], 2008 yılında "Çevrimiçi Kimlik Hırsızlığı Raporu"[19] (bu dokümanda aynı zamanda kimlik hırsızlığının suçlar hukukunda bir suç olarak kabul edilmesini öngörmektedir), 2009 yılında da "Çevrimiçi Kimlik Hırsızlığı Konusunda OECD Politika Rehberi"[20] dokümanlarını yayımlamıştır.

Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization: NATO)

NATO örgütü kuruluş amacı doğrultusunda, daha çok üye ülkeleri hedef alan siber saldırılara odaklanmaktadır. NATO Kıdemli Sivil Acil Durum Planlama Komitesi (SCEPC) sivil halk ve kritik altyapının terörist saldırılara karşı korunması konusunda üye ülkelere yardımda bulunmaktadır. Ayrıca NATO Sivil İletişim Planlama Komitesi (CCPC) ise genel ve özel iletişim altyapılarından sorumludur. NATO Sivil Koruma Komitesi 2003 yılında Kritik Altyapı Koruma Konsept Dokümanını yayımlamıştır [21]. NATO Terörizmle Mücadele Mükemmeliyet Merkezi 2008 yılında Ankara'da kurulmuştur [22].

Asya Pasifik Ekonomik İşbirliği Kuruluşu (Asia-Pacific Economic Cooperation: APEC)

APEC süper güçler olarak bilinen ABD, Rusya ve Çin'i aynı çatı altında toplaması açısından önemli bir kuruluştur [23]. APEC 1990 yılında Bilgi ve İletişim Çalışma Grubunu kurmuştur. Bu çalışma grubu ise Liberalleşme Yönlendirme Grubu, Bilgi ve İletişim Teknolojileri Geliştirme Yönlendirme Grubu ve Güvenlik ve Geliştirme Çalışma Grubu olmak üzere üç alt çalışma grubu oluşturmuştur. Güvenlik ve Geliştirme Çalışma Grubu ağlar/altyapılar/servisler/teknolojiler/uygulamalar/e-ticaret konularında güvenlik ve karşılıklı güven oluşturma konusunda çalışmaktadır. Bu grup



spam e-postalar, casus yazılımlar ve siber suçların önlenmesinde Bilgisayar Acil Durum Müdahale Ekibi (Computer Emergency Response Team: CERT) ve Bilgisayar Güvenliği Olay Müdahale Ekibi (Computer Security Incident Response Team: CSIRT) yapılanmalarını desteklemektedir. Bu kuruluş bünyesinde yürütülen önemli çalışmalardan birisi de e-güvenlik Görev Grubu tarafından 2003 yılında başlatılan Siber Suçlar Mevzuatı ve Uygulama Kapasitesi Oluşturma Projesidir.

Şanghay İşbirliği Örgütü (Shanghai Cooperation Organization: SCO)

SCO örgütü üyelerini Rusya, Çin ve bazı eski Sovyet cumhuriyetleri oluşturmaktadır. Bu örgüt de 2009 yılında yayımladığı Yaketerinburg Açıklaması ile bilgi güvenliğini uluslararası müşterek sistemlerde öncelikli alanlardan biri olarak belirlemiştir. SCO ülke başkanlarının 2012 yılındaki Pekin toplantısında SCO'nun terörizm, aşırılık ve aynı zamanda siber suçlarla mücadelede sıkı işbirliği yapacağı duyurulmuştur [4,14].

Sanal Küresel Görev Gücü (Virtual Global Taskforce: VGT)

VGT Avustralya, İngiltere, Kanada, ABD, İtalya, Birleşik Arap Emirlikleri, Yeni Zelanda, Interpol ve Europol'ün üyesi olduğu bir kanun uygulama birimleri birlikteliğidir [24]. Bu örgüt özellikle çocuk cinsel istismarı konusunda sivil sektörle de beraber çalışmalar yapmaktadır.

Siber Suçlar Çalışma Grubu Stratejik İttifakı

Bu ittifak 2006 yılında Avustralya, ABD, Yeni Zelanda, Kanada ve İngiltere'den beş kanun uygulama biriminin katılımıyla siber suçlarla mücadele amacıyla kurulmuştur.

İlgilenen okuyucular uluslararası bilgi güvenliği, siber suçlar ve kanun uygulama birimleri ile bu konuda birliktelikler, organizasyonlar ve inisiyatifler hususunda detaylı bir çalışmayı "Institutions for Cyber Security" başlıklı araştırmada [25] bulabilirler.

Son yıllarda ülkeler sürekli olarak, ikili ve bölgesel işbirliklerinin siber suçlarla mücadele ve siber ortam güvenliği için yeterli olmadığına dikkat çekerek, uluslararası müşterek bir siber-uzay antlaşmasının gerekli olduğunu belirtmektedirler [10].

Bütün bu uluslararası çalışmaların ilk hedefi sayısal suçların önlenmesi olarak özetlenebilir. Ancak bu hedefe ulaşmak için suç araştırma, inceleme ve delillendirme süreçlerinde de eşgüdüm ve karşılıklı uygulanabilirliğin sağlanması kaçınılmaz bir ihtiyaçtır. Bu anlamda adli bilişim incelemesi konusunda uluslararası bir uygulama ve birliktelik bulunmamaktadır.

III. ADLI BİLİŞİM TRENDLERİ VE GELECEK ÖNGÖRÜLERİ

Adli bilişim sürekli değişen ve gelişen bir alandır. Bu ise adli bilişim ile ilgilenen kişi ve kurumların yeniliklere sürekli adapte olma zorunluluğunu gerektirmekte, aynı zamanda da bu kişi ve kurumlar için bazı problemlere neden olmaktadır. Bu problemler arasında; sürekli boyutları artan sabit disk gibi

depolama ortamları, sabit disk kullanımını gerektirmeyen bazı yöntemler geliştiren saldırganlar ve kötücül yazılımlar ve siber olaylara müdahale esnasında daha hızlı karar vermeye olan ihtiyaç sayılabilir.

Bilgisayarların ve mobil telefonların hızlı gelişimi hayatı kolaylaştırmasının yanı sıra bu cihazların suç teşkil eden faaliyetlerde de kullanılmasına yol açmıştır [26]. Bu cihazların karmaşıklığı ise hem güvenlik kontrollerinin uygulanmasını hem de bu cihazların kullanıldığı suç faaliyetlerinin araştırılmasını zorlaştırmaktadır.

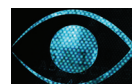
Bilgisayarlarla işlenen suçların üssel olarak artması ile adli bilişim, dolandırıcılık, siber taciz, öldürme ve çocuk istismarı gibi geniş bir yelpazedeki suç faaliyetlerinin araştırılmasında kullanılmaktadır. Burada adli bilişimin amacı, sayısal kanıtları, mahkemelerde kullanılmak üzere muhafaza etmek, araştırmak ve analiz etmektir. Analiz faaliyeti, basit olarak bilgilerin elde edilmesinden bir dizi olayın aydınlatılmaya çalışmasına kadar değişebilir.

Adli bilişim uzmanları, depolama ortamları, elektronik dosya türleri gibi teknolojilerin ve cihazların gelişimini sürekli takip edebiliyor olmalıdır. Bunların kullanımı ise sürekli gelişmekte ve değişmekte ve adaptasyonu zorlaştırmaktadır. Buna örnek olarak on yıl önce sürekli kullanılan CD/DVD ROM'ların, flash belleklerin çıkması ile birlikte kullanımlarının oldukça azalması, yine SSD disklerin yaygınlaşması ile birlikte mekanik disklerin kullanımlarının azalmaya başlaması gösterilebilir.

Adli bilişim alanında günümüzde yaşanan ve yakın gelecekte yaşanmaya devam edecek en belirgin değişikliklerden biri, depolama ortamları, bellek ve işlemcilerin türleri, boyutları ve hızlarında yaşanacak değişikliklerdir. Önümüzdeki 2-3 sene içinde standart bilgisayarlar 5TB depolama alanı veya daha düşük kapasitede fakat elektronik olan SSD diskler ile gelecek, flash bellekler ise 250 GB veriyi taşıyabilecektir. Bu nedenle, bugün olduğundan çok daha büyük boyutta verilerin analiz edilmesi ve ayrıştırılması söz konusu olacaktır. Bununla beraber bilgisayarlar da 7 veya 8 kat daha hızlı çalışacaktır. Geleneksel adli bilişimin zorluklarından biri, sabit disklerin boyut ve sayılarına göre veri toplamanın saatler hatta bazen günler almasıdır. Doğrulama yaptıktan sonra adli bilişim uzmanları, uzun zaman alan yüksek boyutlu veriler üzerinde çalışmaktadırlar.

Bu problemi aşmak ise "Canlı adli bilişim" 'in yaygınlaşması ile mümkün olabilecektir. Canlı adli bilişimden kasıt, çok yüksek miktarda veri ile karşılaşıldığında; geçici verinin toplanması, sabit diskin bazı alanlarının bazı soruların cevaplanması için analiz edilmesi ve tüm sabit diskten veri toplanmasının veya diğer sistemlerin analiz edilmesinin gerekip gerekmediğinin belirlenmesidir.

Diğer yaşanacak gelişmeleri ise; Uzmanlık olarak adli bilişim alanının genişlemesi ve adli bilişim araçlarının daha özel hale gelerek veri toplama ve işlemenin otomatikleşmesi olarak sıralamak mümkündür. Her ne kadar bu gelişme, daha az eğitilmiş insanların bu araçları kullanabileceği anlamına gelse de, donanım ve yazılımların daha karmaşık hale gelmesi ile geleceğin adli bilişim uzmanlarının, bunları yönetebilmek için daha detaylı teknik bilgilere sahip olmasını gerektirebilecektir.



Öte yandan, adli bilişim, suç araştırmalarının dışında güvenlik ve mahremiyet risk değerlendirmesinde veri eşleştirmesi, fikri mülkiyet haklarının otomatik olarak aranması gibi diğer alanlarda da kullanılmaya başlanmıştır. Bu kullanımların yakın gelecekte daha da yaygınlaşması söz konusu olabilecektir. Bu şekilde adli bilişimin sadece bir inceleme mekanizmasından çıkarak bir önleme ve uyumluluk sağlama mekanizmasına dönüşmesi de söz konusu olabilecektir.

Siber Suçlarla Mücadele

Adli bilişim alanındaki teknoloji ve araçların sürekli ve hızlı değişiminin diğer bir boyutu da siber suçlar ve suçlularla ilgilidir. Emniyet güçlerinin ve ulusal güvenlik kuruluşlarının, yeni teknolojileri farklı kanunsuz yollarla kullanma eğiliminde olan suçlular, organize suç örgütleri, devlet destekli veya desteksiz gruplara karşı mücadelede adli bilişim kapasitelerini teknik ve prosedürel olarak sürekli güncel tutmaları ve geliştirmeleri gerekmektedir. Emniyet güçleri tarafından bu kapasitenin sağlanabilmesi için ise, bu alanda ar-ge faaliyetlerine kaynak tahsis edilmesi gerekmektedir.

Fiziksel Bellek Adli Bilişimi

Siber suçlar ile ilgili olarak adli bilişimin en temel güçlükleri, fiziksel bellek (elektronik sabit diskler de dâhil olmak üzere) ve bulut bilişimdir.

Statik depolama ortamlarına kıyasla, fiziksel bellekler, aynı somut sayısal delilleri sağlamamakta, delillerin muhafazası, toplanması ve analiz edilmesi de daha zor olmaktadır [27]. Fiziksel bellek ortamlarında depolanan verilerin geçici nitelikte olması, genellikle belirli bir işleme yönelik olarak doğrudan bir kanıt oluşturmamasına yol açmaktadır.

Bunula birlikte, fiziksel belleklerde artık verilerin bulunması, geleneksel yöntemler ile toplanamayacak olan bilgilerin toplanması için fiziksel bellek adli bilişim tekniklerinin geliştirilmesi için fırsat oluşturmaktadır. İşletim sistemi veya uygulamalar tarafından kullanılan veriler fiziksel bellekte uzun süre kalabilmekte ve kullanıcının buna müdahale imkânı kısıtlı olmaktadır. Öte yandan, fiziksel bellek boyutları ve depoladıkları veri miktarları gitgide artmakta, elektronik sabit disklerin kullanımı da yaygınlaşmaktadır.

Bulut bilişim gibi günümüz teknolojik gelişmelerinin ışığında, fiziksel bellekten veri toplanması ve analizinin getirisi, risklerine göre daha ağır basar hale gelmiştir.

Bulut Bilişim Ortamında Adli Bilişim

Bulut bilişim ise artan bir şekilde yaygınlaşan ve adli bilişim uzmanları için zorluklar olduğu kadar fırsatlar da sunan bir alandır[2]. Bulut bilişim ortamları, siber suçlular tarafından sıklıkla saldırıya maruz kalan ortamlardır. Bu da siber suçların tespitinde daha yüksek hacimde analiz edilecek olan sayısal delil anlamına gelmektedir.

Bulut bilişimin suçlular tarafından kullanımı, kullandıkları cihazların sanallaşması, coğrafik olarak dağıtık olması ve kısa süreli olması anlamına gelmektedir. Bu ise bunların tespit edilmesi ve ele geçirilmesinde emniyet güçlerine teknik ve yasal olarak zorluklar getirmektedir.

Sanallaştırma ve buna istinaden mevcut adli bilişim analiz araçlarının kullanılamaması, sayısal kanıtların bulunduğu

ortamların net bir şekilde bilinmemesi, mahremiyet hususları ve yasal sınırlar adli bilişim alanında en çok zorluk yaşanacak konular olacaktır.

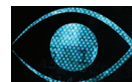
Bu noktada, sadece kısmi verinin, bir den fazla lokasyondan ve çeşitli formatlarda ve farklı kanuni düzenlemeler altında yasal olarak nasıl temin edilebileceği konusunda araştırmaların yapılması ve birlikte çalışmaya ihtiyaç vardır.

Yukarıda belirtilen adli bilişimin önündeki zorluklara istinaden, bu alanda yeni bazı yaklaşımların getirilmesinin kaçınılmaz olduğu değerlendirilmektedir [28]. Temel olarak adli bilişim alanındaki yönelimler özetlenecek olursa; Cihaz inceleme yaklaşımından, olayın incelenmesi yaklaşımına geçilmesi, veri merkezli analizden, inceleme merkezli analize geçilmesi ve araç tabanlı adli bilişimden, hizmet tabanlı adli bilişime geçiş yapılması şeklinde tanımlanabilir.

IV. BİLİRKİŞİLİK VE BİLİRKİŞİ ÇALIŞMA USULLERİ

Mahkemelerde yapılacak bilirkişilik ile düzenleme 01.10.2011 tarihli 6100 sayılı Hukuk Muhakemeleri Kanununda (HMK) düzenlenmiştir. Kanunun dördüncü kısmının beşinci bölümü mahkemelerde bilirkişinin nasıl görevlendirileceği ve bilirkişinin çalışma usullerini kapsamaktadır. Ancak kanunda tanımlanan ve çalışma usulleri belirlenen bilirkişi hizmetleri genel kapsamda olup, bilişim suçlarının incelenmesinde ihtiyaç duyulan detayları doğal olarak içermemektedir. Bilirkişi teriminin farklı tanımları bulunsa da en geniş yaklaşım ile “hâkim tarafından görüşüne başvurulacak kişidir” şeklinde ifade edilebilir. HMK’da bilirkişi görüşüne başvurulacak durumlar “çözümü hukuk dışında, özel veya teknik bilgiyi gerektiren hâller” olarak belirlenmiştir. Mahkemelerde bilirkişi görevlendirmesi ise mahkeme tarafından kendiliğinden veya tarafların birinin talebi üzerine yapılır. Mahkemelerde görevlendirilecek bilirkişiler ise bölge adliye mahkemesi adli yargı adalet komisyonları tarafından, her yıl düzenlenecek olan listelerle belirlenmektedir. Görüşüne başvurulacak bilirkişi miktarı için ise HMK 267/1 maddesinde mahkemelerin bilirkişi olarak yalnızca bir kişi görevlendirebileceği, ancak gerekçesi açıkça belirtilmek suretiyle tek sayıda birden fazla kişiden oluşturulacak bir kurulun görevlendirilmesine de imkân tanınmaktadır. Bilirkişilere görüşlerine başvurulacak konularda raporlarını hazırlamak üzere en çok üç ay süre verilebilir. Gerekli görülen durumlarda ise bu süre üç ay daha uzatılabilir. Bilirkişi raporlarının nasıl olması gerektiği konusunda ise kanunda sadece bilirkişilerin hukuki değerlendirmede bulunamayacağı belirtilmektedir. Bilirkişi raporun hazırlanma şekli ve örnek raporlar ile ilgili literatürde birçok yayın mevcuttur [26]. Ancak bu yayınların hiç birisi sayısal sistemler ve bilişim suçlarının incelemelerinde hazırlanacak raporlar için özelleşmiş bir yapıyı içermemektedir.

Bilirkişilik ve bilirkişi çalışma usulleri ile ilgili mevcut düzenleme ve uygulamalar incelendiğinde bu hizmetlerin adli bilişimin gerek ve ihtiyaçları doğrultusunda özelleşmediği görülmektedir. Mevcut genel bilirkişilik düzenlemelerinin de adli bilişim hizmetlerinin ihtiyaçlarını karşılamada yetersiz kaldığı görülmektedir [29].



V. ADLI BİLİŞİM HİZMETLERİ ALANINDA PROBLEMLER VE ÇÖZÜM ÖNERİLERİ

Adli bilişim kavramı görece olarak yeni bir kavramdır ve gelişen teknolojilere paralel olarak suç türlerinin değişmesi ve dolayısı ile kanıt toplama ve analiz etme yöntemlerinin değişmesi sonucu ortaya çıkmıştır. Bu açıdan bakıldığında adli bilişim ile ilgili en temel problem alanla ilgili yeterli sayıda ve yetkinlikte personel bulunmamasıdır. Bu husus hem adli bilişim alanında görev alan teknik personel anlamında hem de işin hukuki boyutunda görev alan hukukçular anlamında geçerlidir. Bu anlamda son yıllarda adli bilişim alanında yüksek öğrenim seviyesinde önemli gelişmeler yaşanmaktadır. Bazı üniversitelerde adli bilişim yüksek lisans programları açılmaktadır. Bunun yanında lisans seviyesinde de hem bilgisayar bilimleri alanındaki bölümlerde adli bilişim teknik altyapısı ile ilgili, hem de hukuk fakülteleri bünyesinde konunun hukuki yönleri ile ilgili dersler açılmaktadır. Teknolojik gelişmeler ışığında sayısal ortamlardaki suç miktarındaki artışa paralel olarak adli bilişim uzmanlarına duyulan ihtiyacın da artacağı göz önünde bulundurulursa, adli bilişim alanındaki eğitim-öğretim faaliyetlerinin artırılması gerektiği sonucuna varılabilir.

Adli bilişim alanındaki bir diğer problem ise adli bilişim alanında görev alacak bilirkişilerin belirlenmesi ve yetkinliklerinin ölçülmesi konusudur. Yukarıda da belirtildiği üzere adli bilişim konusunda görev alabilecek teknik personelin eğitimi konusunda ülkemizde çeşitli çabalar olmasına rağmen henüz adli bilişim uzmanının resmi bir tanımlaması yapılmış değildir. Bunun yanında hangi eğitimleri almış kişilerin adli bilişim uzmanı olabileceği, bir adli bilişim uzmanının taşıması gereken yetkinlik şartları, bu şartların karşılanıp karşılanmadığının nasıl belirleneceği konusunda ortaya konmuş gerek ulusal bazda gerekse de uluslararası düzeyde bir standart/kriter ya da benzeri bir uygulama bulunmamaktadır. Adli bilişim uzmanlarının yetkinliklerini belirleyen ve belgeleyen bir sertifikasyon programının bulunmaması, mahkemelerde görevlendirilecek bilirkişilerin hakimlerce belirlenmesi aşamasında ciddi sıkıntılar yaratmaktadır. Bu problemin çözümü için öncelikle Türk Standardları Enstitüsü bünyesinde ulusal düzeyde bir sertifikasyon programının başlatılması ve adli bilişim uzmanı olma yetkinliğine sahip kişilerin belgelendirilmesi, sonrasında da bu sertifikasyon programının uluslararası bir standarda dönüştürülmesi için çalışmaların başlatılması önerilmektedir.

Yukarıda bahsedilen yetkinlik problemine ilave olarak uzmanlık alt alanlarının da belirlenmesinin yapılacak çalışmalar için faydalı olacağı değerlendirilmektedir. Zira adli bilişim kapsamında inceleme yapılması gereken birçok sayısal ortam söz konusu olabilir ve bu ortamların her biri özel bir uzmanlık gerektirebilir. Bu kapsamda değerlendirildiğinde adli bilişim; veri kurtarma, işletim sistemi, veri tabanı incelemesi, bilgisayar ağları alanı, cep telefonu ve mobil cihazlar gibi alt alanlara ayrılabilir. Bu alt alanlardan birinde uzman olan bir kişinin diğer alanda bilgisi bulunmayabilir. Bu problemin çözümü için belki de yapılması gereken yukarıda önerilen sertifikasyon programının alt alanlara göre ayrıştırılması ve her bir alan için ayrı ayrı sertifikasyon

işleminin gerçekleştirilmesidir.

Buradaki hususlara ek olarak dikkat edilmesi gereken bir diğer husus da teknolojinin hızlı değişimine paralel olarak adli bilişim yetkinlik şartlarının da değişebilme gereksinimidir. Bu nedenle uygulanacak sertifikasyon programının belirli sürelerle yenilenmesi ve gelişen teknolojilere paralel olarak kişi yetkinliklerinin periyodik aralıklarla (örneğin 2 yıl gibi) yeniden gözden geçirilmesi, kontrol edilmesi ve gerekli şartları taşıyan kişilere sertifikasyonun yeniden verilmesinin uygun olacağı değerlendirilmektedir.

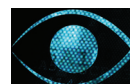
Adli bilişim alanındaki bir diğer problem ise kullanılan araçlarla ilgilidir. Adli bilişimde yapılan tüm incelemelerde bazı hazır yazılım ve/veya donanım araçları kullanılmaktadır. Bu araçlara örnek olarak SANS-SIFT, EnCase, FTK, Sleuth Kit, Wireshark, vb verilebilir. Bu araçların her biri adli bilişim alanında önemli bilgiler sağlamaktadır. Ancak bu araçların performanslarının ve işlevselliklerinin ölçülmesi anlamında bir değerlendirme bulunmamaktadır. Bu araçlardan elde edilen bilgilerin ne derece sağlıklı olduğu ve ne derecede güvenilir olduğu konularında bir değerlendirme yapılması ve belki de bu araçların performans ve güvenilirliği üzerine sertifikasyonlarının yapılması, adli bilişim alanında kullanılabilirliklerini artıracaktır. Ayrıca bu araçların kullanımı durumunda bilgi güvenliği riskleri oluşup oluşmadığı hususunun da ayrıca değerlendirilmesi gerekmektedir. Bu araçların hazırlanacak bir koruma profiline göre güvenlik sağladıklarının belgelendirilmesi için Ortak Kriterler Belgelendirme Programı kapsamında değerlendirilmeleri faydalı olacaktır.

Adli bilişim alanında bilirkişi olarak görevlendirilen kişilerin yetkinliklerinin tam olarak belli olmaması, bu kişilerin kullandıkları adli bilişim araçlarının güvenilirlikleri konusunda bir fikir birliği sağlanmamış olmasının yanında bilirkişilerce hazırlanan raporların içerik ve kapsamı konusunda da belirsizlikler söz konusudur. Her bilirkişi yaptığı çalışmalar ve elde ettiği bulgular ışığında bir rapor hazırlamaktadır. Oysaki hem bu raporların okunabilirliğinin ve anlaşılabilirliğinin sağlanması hem de bu raporlara güvenilirliğin sağlanması için, rapor kapsamında hangi hususların yer alması gerektiği, hangi araçların kullanıldığı, hangi analizlerin yapıldığı ve hangi bulguların elde edildiğinin belirli bir format kapsamında sunulması faydalı olabilir. Bunun için bir rapor formatının geliştirilmesi ve bu formata uyumun sağlanması faydalı olacaktır.

VI. SONUÇ VE ÖNERİLER

Bu çalışmada ulusal ve uluslararası düzeyde adli bilişim konusu ele alınmış, mevcut durum özetlenmiş, gelecek öngörüler yapılmış ve alandaki problemler ve çözüm önerileri sunulmuştur.

Adli bilişim göreceli olarak diğer bilgi teknolojileri alanları ile karşılaştırıldığında yeni bir alan olup teknolojinin gelişimine paralel olarak hızlı değişim gösteren bir alandır. Bu alandaki en temel problem konuya hakim uzman personel eksikliğidir. Bunun yanında adli bilişim alanında çalışacak ve özellikle de mahkemelerde bilirkişi olarak görevlendirilecek personelin taşıması gereken niteliklerin belirlenmemiş olması

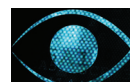


da bu konuda etkindir. Bu nedenle adli bilişim uzmanlarının yetkinlik şartlarının belirlenmesi ve bu yetkinlik şartlarının ölçülmesi kritik önem arz etmektedir. Bu probleminin çözümü için hem ulusal düzeyde hem de uluslararası düzeyde standartların hazırlanması ve belgelendirme programlarının başlatılması elzemdir.

Diğer bir problem ise, adli bilişim alanında yerli ürün ve teknoloji olmaması ve bu alandaki gelişmelerin yeterince takip ve adapte edilememesidir. Adli bilişim alanında önümüzdeki dönemde önemli gelişmelerin yaşanacağı ve hukuki süreçlerin sağlıklı yürütülmesi açısından bunların takip edilmesi gerektiği aşikardır. Bu alanda özellikle yerli ürünlerin geliştirilerek, kullanımlarının yaygınlaştırılması yakın gelecekte adli bilişim çalışmalarının yaygınlaşacağı düşünüldüğünde isabetli olacaktır.

KAYNAKLAR

- [1] WaveFront Consulting Group, A Brief history of Cybercrime, http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html, internet adresinden 11.07.2014 tarihinde erişilmiştir.
- [2] Mustafa Yücel, Bilişim Suçları, Ankara Barosu Dergisi, Y.49, Sy.4, 1992, Ankara, s.505
- [3] Edime Barosu, Adli Bilişim (Computer Forensic), <http://edimebarosu.org.tr/incelemler/adli-bilisim-computer-forensic> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [4] Adli Bilişim Derneği, Adli Bilişimin tanımı, <http://www.adlibilisim.org.tr/index.php/hakkimizda/2013-04-25-04-43-07/adli-bilisimin-tan-m> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [5] Yunus Ballı, Adli Bilişim Nedir?, http://www.dijitaldeliller.com/adli_bilisim_nedir.html internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [6] Ş. Sağroğlu, M. Karaman, Adli Bilişim, <http://www.telepati.com.tr/agustos12/konu8.htm> internet adresinden 10.07.2014 tarihinde erişilmiştir.
- [7] Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı, http://www.tbd.org.tr/index.php?dummy=1&sayfa=raporlar&mi=3&vkid=194&t=1290232819&jfr=true&keepThis=true&T_B_iframe=true&height=500&width=800 internet adresinden 10.07.2014 tarihinde erişilmiştir.
- [8] Caza Muhakemesi Kanunu, 04.12.2014 kanun numarası: 5271, <http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [9] Adli ve Önleme Aramaları Yönetmeliği, 01.06.2005 Resmi Gazete Sayısı: 25832, <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.8203&MevzuatIliski=0&sourceXmlSearch=> internet adresinden 12.07.2014 tarihinde erişilmiştir.
- [10] A. Levin, D. Ilkina, (2013), International Comparison of Cyber Crime, Privacy and Cyber Crime Institute, Ted Rogers School of Management, Ryerson University, March 2013. http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_March2013.pdf internet adresinden 10.07.2014 tarihinde erişilmiştir.
- [11] International Telecommunication Regulations (ITR), International Telecommunications Union (ITU), <http://www.itu.int/oth/T3F01000001> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [12] Guidelines on the Role of Prosecutors, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August to 7 September 1990, U.N. Doc. A/CONF.144/28/Rev.1 at 189 (1990). <http://www1.umn.edu/humanrts/instree/i4grp.htm> internet adresinden 12.07.2014 tarihinde erişilmiştir.
- [13] UN General Assembly resolution 65/230, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, https://www.unodc.org/documents/justice-and-prison-reform/AGMs/General_Assembly_resolution_65-230_E.pdf internet adresinden 13.07.2014 tarihinde erişilmiştir.
- [14] Signatories of the Final Acts: 89, World Conference on International Telecommunications, 3-14 December 2012, Dubai UAE, <http://www.itu.int/osg/wcit-12/highlights/signatories.html> internet adresinden 13.07.2014 tarihinde erişilmiştir.
- [15] Oliver Moore, Debate over Internet regulation's future rages at Dubai meeting, <http://www.theglobeandmail.com/technology/debate-over-internet-regulations-future-rages-at-dubai-meeting/article6016228> internet adresinden 14.07.2014 tarihinde erişilmiştir.
- [16] The Hon Nicola Roxon MP, (2012), New Laws in the Fight Against Cyber Crime, http://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/1867175/upload_binary/1867175.pdf;fileType=application%2Fpdf#search=%22cyber%20crime%22 internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [17] Schjolberg, S., Cybercrime Law. Global organizations: OECD, (2013), <http://www.cybercrimelaw.net/OECD.html> internet adresinden 14.07.2014 tarihinde erişilmiştir.
- [18] OECD Guidelines for The Security of Information Systems and Networks: Towards A Culture of Security, OECD, <http://www.oecd.org/sti/economy/2002-security-guidelines-review.htm> internet adresinden 13.07.2014 tarihinde erişilmiştir.
- [19] Scoping paper on online Identity theft, OECD, <http://www.oecd.org/internet/consumer/40644196.pdf> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [20] OECD Policy Guidance on Online Identity Theft, OECD, <http://www.oecd.org/sti/consumer/40879136.pdf> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [21] The Protection of Critical Infrastructures, NATO Parliamentary Assembly, <http://www.nato-pa.int/default.asp?SHORTCUT=1165> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [22] Centre of Excellence Defense Against Terrorism, NATO, <http://www.coedat.nato.int/index.htm> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [23] History of Asia-Pacific Economic Cooperation (APEC), <http://www.apec.org/About-Us/About-APEC/History.aspx> internet adresinden 10.07.2014 tarihinde erişilmiştir.
- [24] Virtual Global Task Force, Who we are, <http://www.virtualglobaltaskforce.com/who-we-are> internet adresinden 14.07.2014 tarihinde erişilmiştir.
- [25] Nazli Choucri, Stuart Madnick & Jeremy Ferwerda (2014) Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development, 20:2, 96-121, <http://dx.doi.org/10.1080/02681102.2013.836699> internet adresinden 15.07.2014 tarihinde erişilmiştir.
- [26] Digital Forensic Trends and Future, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76 <http://wp.vcu.edu/hsep/wp-content/uploads/sites/3338/2013/06/Digital-Forensic-Trends-and-Future-.pdf> adresinden 14.07.2014 tarihinde erişilmiştir.
- [27] Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future, Korean Institute of Criminology http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2421339 adresinden 16.07.2014 tarihinde erişilmiştir.
- [28] The future of digital forensics, SungKyong Un ETRI, RSA Conference Asiapacific 2013, https://www.rsaconference.com/writable/presentations/file_upload/cle-w04_final.pdf adresinden 13.07.2014 tarihinde erişilmiştir.
- [29] Erhan Bulut, Bilirkişi Seçimi ve Bilirkişi Raporlarının Bağlayıcılığı, Mevzuat Dergisi, yıl:4 sayı:47, Kasım 2001, <http://www.mevzuatdergisi.com/2001/11a/02.htm> internet adresinden 13.07.2014 tarihinde erişilmiştir.



Siber Saldırılarda İstismar Kitlerinin Kullanımı Üzerine Bir Analiz ve Savunma Önerileri

E. U. Küçüksille, M. A. Yalçinkaya, O. Uçar

Özet— İnternet üzerinde siber saldırganlar tarafından gerçekleştirilen saldırıların büyük bir kısmının, istismar kitleri aracılığı ile gerçekleştirildiği bilinmektedir. İstismar kitleri hedef sistemlere yönelik saldırıları otomatize etmek için oluşturulmuş, içerisinde hedef sistem üzerinde bulunan güvenlik açıklarından yararlanmaya yönelik olarak casus yazılımlar, istismar kodları ve diğer bileşenlerin bir arada bulunduğu bir platformdur. Bu çalışmada, saldırganlar tarafından istismar kitleri aracılığı ile gerçekleştirilen saldırı tipleri incelenerek, kullanıcılara istismar kitlerine karşı alınabilecek önlemler sunulmuştur. Ayrıca istismar kitlerinin kaynakları ve hedef aldıkları uygulamalar, araştırma raporlarından elde edilen istatistiki verilerden faydalanılarak incelenmiştir. Gerçekleştirilen çalışma, istismar kitlerinin neden olduğu zararlı yazılım yüklemeleri, sistem tahribatları ve veri hırsızlıkları gibi bilgi güvenliği alanında karşılaşılan önemli problemlere yönelik çözümler sunmaktadır.

Anahtar Kelimeler— Bilgi Güvenliği, İndirme Tabanlı Saldırıları, İstismar Kitleri, Veri Hırsızlığı

Abstract— A major part of the cyber-attacks that are performed by the hackers are carried out by means of the exploit kits. An exploit kit is a platform that is created automate the attacks against the vulnerabilities located on the target system and includes a combination of exploits, spywares and other components that attempt to exploit these vulnerabilities. In this study, we investigated the attack types which are performed by the cyber attackers through the exploit kits and we present different defense methods to prevent attacks of exploit kits. In addition, the source of the exploit kits and the applications they targeted are examined making use of the statistical data that obtained from research reports. Besides, performed study offers solutions against major problems encountered in the field of information security that caused by the exploit kits such as malware installations, destruction of the systems and data theft.

Index Terms— Data Theft, Drive-by Download Attacks, Exploit Kits, Information Security

I. GİRİŞ

Günümüzde internet siteleri üzerinden hedef sistemlere yönelik zararlı yazılımların indirilmesi ve çalıştırılmasında önemli bir artış gözlemlenmektedir.

E.U. Küçüksille, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye; (e-posta: ecirkucuksille@sdu.edu.tr)

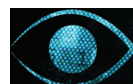
M.A. Yalçinkaya, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye (telefon: +90(246)2111381; e-posta: mehmetyalcinkaya@sdu.edu.tr)

O. Uçar, Bilgi Güvenliği Eğitim ve Danışmanlık Ltd.Şti., Kozyatağı, Kadıköy, İstanbul, Türkiye (e-posta:ozan.ucar@bga.com.tr)

Bilgisayar kullanıcılarının internete bağlanması ve dış dünya ile etkileşimde bulunmalarını sağlayan en önemli araçlar internet tarayıcılarıdır. Birçok internet tarayıcısı günümüzde işletim sistemi kurulumlarında otomatik olarak yüklenmektedir. İnternet tarayıcılarının oldukça sık kullanılması, onları saldırganların kurbanlarına erişmelerinde en önemli köprülerden biri haline getirmiştir. 2014 yılında yapılan bir araştırmaya göre, internet kaynaklı tehditlerin büyük bir çoğunluğunun, kullanıcıların ziyaret etmiş oldukları zararlı internet siteleri ve kullandıkları internet tarayıcılar ile tarayıcı eklentileri üzerinden gerçekleştirildiği tespit edilmiştir[1]. Kullanıcılarına indirme tabanlı saldırılar sunan istismar kitleri ile internet tarayıcıları üzerinde bulunan güvenlik açıkları hızlı bir şekilde keşfedebilmekte ve bu güvenlik açıklarından yararlanılarak zararlı yazılımlar hedef sistemlere yayılabilmektedir [2]. Ayrıca, tüm bu işlemler otomatize olarak gerçekleştirilmektedir. İstismar kitleri, kullanıcılara yönelik kimlik hırsızlığı ya da internet bankacılığı dolandırıcılığı gibi eylemlerden, bir kurumun güvenlik duvarı arkasındaki bir bilgisayara erişim sağlayarak son derece kritik sistemler üzerinde büyük hasarlara neden olmaya kadar varan birçok farklı saldırı senaryolarında başarılı olabilmektedir.

Siber suç piyasalarında istismar kitleri her geçen gün artan bir ivme ile işlem görmektedir. Dünya çapında ki internet kullanıcılarına yönelik saldırıların yaklaşık üçte ikisinden istismar kitleri sorumludur[3]. İstismar kitleri, şahsi bilgisayar kullanıcılarından, kurumsal ağlar içerisinde bulunan kullanıcılara kadar bütün bilgisayar kullanıcıları için ciddi bir tehdit oluşturmaktadır. Bir istismar kitinin en temel karakteristiklerinden biri, temel seviyede bilgisayar kullanma yeteneğine sahip herkes tarafından kullanılabilir basitlikte bir kullanıma sahip olmasıdır. Çoğunlukla yeraltı forumlarından temin edilebilen istismar kitleri, kullanıcı dostu bir web ara yüzüne sahip olmaları sayesinde kullanıcılarına, bir bilişim teknolojisi uzmanı ya da güvenlik uzmanı seviyesinde teknik bilgiye sahip olmadan, başarılı saldırılar gerçekleştirmelerine olanak sağlamaktadır. İstismar kitlerinin bir diğer avantajı da kullanıcının, hedefe yönelik saldırı işlemlerinde kullanılacak olan istismar kodlarının nasıl oluşturulduğunun bilmesine gerek olmamasıdır [4].

Uluslararası akademik dünyada istismar kitleri konusunda yapılmış çeşitli çalışmalar mevcuttur fakat ülkemizde henüz istismar kitleri konusunda bir çalışma yapılmamıştır. Bunun nedeni, istismar kiti geliştiricilerinin, piyasaya sürdükleri istismar kitlerinin kaynak kodlarının kopyalanmasına engel



olmak amacı ile ürünlerinde çeşitli şifreleme yöntemleri kullanılmaktadır.

Florian Malecki [2] çalışmasında, istismar kitlerinin şirket ağları üzerinde oluşturabileceği zararlara değinmiştir, kurumsal ağları istismar kitlerine karşı daha güvenli hale getirmek için bir takım önlemler ve tavsiyeler sunmuştur. Allodi ve arkadaşları [3] yeraltı forumlarından elde ettikleri 10 farklı istismar kitini, oluşturdukları MalwareLAB adındaki bir izole ortam içerisinde test etmişlerdir. Çalışmalarında zaman içerisinde farklı sistemler üzerindeki yazılım yapılandırmalarını değiştirerek, bu değişimlere karşı istismar kitlerinin esnekliklerini test etmişlerdir. Yazarlar gerçekleştirdikleri testler sonunda, yazılım güncelleme ve yapılandırmalarına karşı istismar kitlerinin iki farklı role büründüğünü belirtmişlerdir. Bazı istismar kitlerinin yazılım güncellemelerine karşı daha esnek olduklarını fakat bunun yanında daha düşük oranlarda enfeksiyon başarıları sağladıklarını, bazı istismar kitlerinin ise yazılım güncellemelerine karşı çok dirençsiz olduklarını fakat etkili oldukları zaman aralıklarında çok yüksek enfeksiyon oranlarına ulaştıklarını belirtmişlerdir. Kotov ve Massacci [5] çalışmalarında, indirme yolu ile gerçekleşen saldırıların arkasındaki temel araçlar olan 30 farklı istismar kitinin kaynak kodlarının ön analizini paylaşmışlardır. Gerçekleştirilen çalışmalar sonunda istismar kitlerinin karakteristik özellikleri çıkartılmış, istismar kitlerinin ip engelleme ve kod şaşırtma tekniklerini kullandıklarını, kullanıcılarına kitleri kişiselleştirme imkânı sağladıklarını ve gerçekleştirilen saldırıları takip edebilmek için istatistiki veriler sağladıklarını belirlemişlerdir. Moyatama ve arkadaşları [6] çalışmalarında, istismar kitleri gibi zararlı yazılımların temin edilebildiği altı farklı yer altı forumu üzerinde çalışmalar gerçekleştirmişlerdir. Gerçekleştirilen çalışmada forumların sosyal ağ yapısı karakterize edilmiş ve bireylerin bu ortamlarda diğer üyelerin güvenlerini kazanmaları veya kaybetmeleri için ne tür durumların oluşması gerektiğine değinilmiştir. Yazarlar ilgili çalışmanın, yeraltı forumlarının sosyal dinamiklerinin ve e-suç pazarının verimliliğinin inceleneceği daha geniş bir araştırma çalışmasının ilk adımı olduğuna değinmişlerdir.

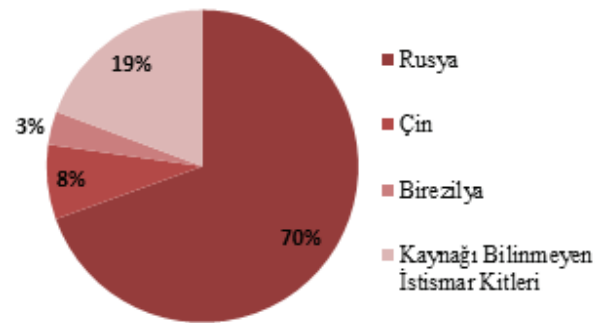
Bu çalışmada; gerçekleştirilmiş diğer çalışmalardan farklı olarak, istismar kitlerinin geliştirildikleri ülkeler, temin edilme süreçleri, kullanıldıkları saldırıların genel akışı ve bu saldırılarda hedef aldıkları uygulamalar çeşitli araştırma raporlarından elde edilen istatistiki veriler ışığında incelenmiş ve istismar kitlerine karşı savunma önerileri sunulmuştur. Çalışmada 2. Bölümde istismar kitleri, üretildikleri ülkeler bazında incelenmiş ve bir istismar kitinin hangi ortamlardan hangi şartlar ile temin edildiği araştırılmıştır. 3. Bölümde istismar kiti tabanlı saldırıların izledikleri genel metodoloji incelenmiş ve saldırılarda hedef alınan uygulamalar istatistiki veriler üzerinde tartışılmıştır. 4. Bölümde, önceki bölümlerde elde edilen verilere dayanarak istismar kitlerine karşı alınabilecek önlemler sunulmuş, 5. Bölümde gerçekleştirilen çalışmanın sonuçlarına değinilmiştir.

II. İSTİSMAR KİTLERİNİN EVRİMİ VE YERALTI PAZARLARDA İSTİSMAR KİTLERİ

Bir istismar kiti, siber suçlular tarafından kullanılan ve indirme tabanlı saldırılar gerçekleştiren yazılım aracıdır. Bir istismar kitinin asıl amacı, hedef sistemler üzerinde yer alan internet tarayıcılarda bulunan güvenlik açıklarından faydalanarak, hedef sistemlere gizlice zararlı yazılım indirmek ve çalıştırmaktır [5]. Siber saldırganların istismar kitlerini kullanarak izledikleri saldırı tekniklerine değinmeden önce, istismar kitlerinin geçmişine ve bir istismar kitinin bir saldırgan tarafından hangi ortamlardan temin edilebileceğine değinmek gerekmektedir.

Üretilen ilk istismar kitleri 2005 yılında piyasaya sürülmüştür. Bugün yayımlanan istismar kitlerinin büyük çoğunluğu, gelişen yer altı siber piyasalarına sahip olan Rusya ve Çin gibi ülkelerde geliştirilmektedir. 2012 yılında yayınlanan bir araştırma raporuna göre, üretilen istismar kitlerinin %69' unun Rusya kaynaklı olduğu belirtilmiştir. Rusya'yı ikinci sırada Çin ve üçüncü sırada da Brezilya'nın izlediği ifade edilmiştir. Araştırmaya mevcut istismar kitlerinin %20' sinin hangi ülke kaynaklı olduğu henüz belirlenememiştir [7]. İstismar kitlerinin üretildikleri ülke oranları Şekil 1' de gösterilmektedir.

Rusya, istismar kitlerini geliştirerek yüksek miktarda kazanç sağlayan siyah şapkalı geliştiriciler ile birlikte uzun bir siber suç geçmişine sahiptir. St. Petersburg merkezli Rusya İş Ağı (RBN) gibi kuruluşlar yıllar boyunca istismar kiti geliştiricilerine bir siber suç platformu sağlayarak istismar kitlerinin gelişmesinde önemli bir rol oynamıştır. RBN yıllar boyunca istismar kiti geliştiricilerine web sitesi hosting imkânı sağlamış, bunun yanı sıra uluslararası alıcılar ile işbirliği yapma ve ürünlerini pazarlamalarına izin vermiştir [4].



Şekil 1. Üretilen istismar kitlerinin ülkelere göre dağılımı[7]

Yasadışı olmanın doğası nedeni ile istismar kitlerinin elde edilmesi zor bir süreçtir. Farklı yetenek ve fonksiyonelliklere sahip istismar kitler yer altı forumlarda farklı fiyat aralıklarında satışa sunulmaktadır [3]. Bu forumlar Google gibi popüler arama motorlarında indekslenmemişlerdir. Bu yüzden söz konusu forumlara erişmek için daha detaylı bir arama işlemi gerçekleştirmek gerekmektedir. Yer altı forumlarına erişim sağlanabilmesi halinde dahi, bir istismar kitinin forumlardan temin edilmesi kolay bir süreç değildir.

Birçok organize suç grubu gibi, siyah şapkalı siber saldırganlar da kendi özel alanlarına (yeraltı forumları) dışarıdan erişim sağlanmasına kolay kolay izin vermemektedirler. Söz konusu forumların birçoğu için kayıt şartları çok ağırdır ve genellikle kayıt olabilmek için forum içerisinde bir kullanıcıdan referans gerekmektedir. Ayrıca kayıt olma başvurusunda bulunan kişiden, değerlendirme amacıyla geçmiş siber deneyimlerine yönelik bir takım kişisel bilgiler de istenmektedir[4].

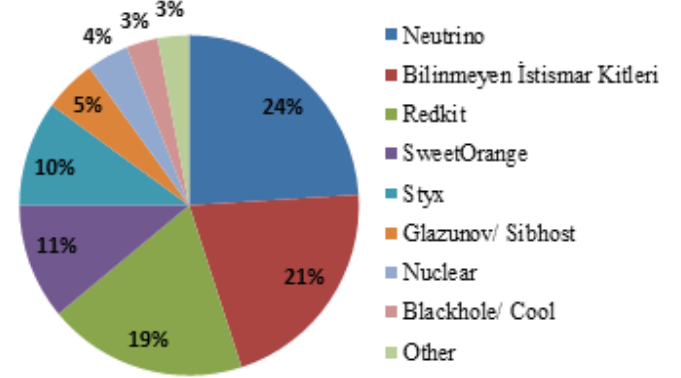
Birçok yasal ticari yazılımda olduğu gibi, istismar kitleri de belirli süre aralıklarında tanımlanmış lisanslara sahiptirler. İstismar kitleri için farklı fiyat aralıklarında üç aylık, altı aylık ya da yıllık lisans çeşitleri bulunmaktadır [2]. Kullanıcısına çok fazla fonksiyon olanağı sağlamayan ve bünyesinde, güncelliğini yitirmiş ve yaygın olarak kullanılan istismar kodlarını içeren tipik bir istismar kiti dahi çeşitli fiyat aralıklarında işlem görmektedir. Yeraltı piyasalarında işlem gören en pahalı istismar kitleri ise bünyelerinde çok gizli ve karmaşık istismar kodlarını bulundurmakta, hatta bazı çeşitleri sıfır gün güvenlik açıklarını hedef alan istismar kodlarını içermektedirler. İstismar kiti yazarları, geliştirdikleri ürünler üzerinden maddi kazanç sağladıkları için ürünlerini lisanslamaya önem vermekte, ücretsiz olarak dağıtılmasını ve yayılmasını engellemek için ürünlerinde kaynak kodu koruma, lisanslama, tek bir sunucuya bağlanma gibi teknikler kullanılmaktadır. Birçok istismar kiti, satıldığı müşterisine ait olan sunucudan farklı bir sunucu altında çalışmasına imkân tanımayan IonCube yazılımı ile korunmaktadır [5].

III. İSTİSMAR KİTİ TABANLI SALDIRILAR VE HEDEF ALDIKLARI UYGULAMALAR

İstismar kitleri, internet tarayıcıları ve tarayıcı eklentileri üzerinde yer alan güvenlik açıklarını hedef alan istismar kodlarını bünyesinde barındıran bir paket olarak tanımlanabilir. İstismar kitleri kurbanlara yönelik indirme tabanlı saldırılar gerçekleştirmektedir. Yapılan çalışmalarda en tehlikeli zararlı yazılım ailelerinin çoğunlukla indirme tabanlı saldırılar ile yayıldıkları tespit edilmiştir [8]. 2013 yılının aralık ayında yayınlanan bir araştırma raporuna göre dünya üzerinde istismar kiti tabanlı saldırılarda kullanılan istismar kitlerinin başında Neutrino istismar kiti gelmektedir. Neutrino istismar kitini ikinci sırada bulunan Redkit istismar kiti izlemektedir. 2012 yılı ve öncesinde Blackhole istismar kiti, dünya genelinde indirme tabanlı saldırılarda en çok kullanılan istismar kiti iken, gerek 2012 yılında piyasaya sürülen yeni istismar kitleri, gerekse geliştiricisinin 2013 yılı ekim ayında tutuklanmasından dolayı, sıralamada yerini kaybetmiştir [9]. 2013 yılında gerçekleşen indirme tabanlı saldırılarda istismar kitlerinin kullanım oranları Şekil 2' de gösterilmiştir.

Bir istismar kiti; işletim sistemi, tarayıcı ya da diğer uygulamaları hedef almak için oluşturulmuş istismar kodlarının bir listesi ile PHP ve HTML dosyalarının bir araya gelmesi sonunda oluşan bir paket olarak tanımlanabilir[8]. Saldırganlar tarafından yeraltı forumlardan temin edilen istismar kitleri, saldırıya ait bir sunucu üzerine bulunan bir web sitesi içerisine yerleştirilmektedirler. Saldırgan çeşitli

yöntemler kullanarak kurbanlarının istismar kiti barındıran web sitesini ziyaret etmesini sağlamaktadır. Kurbanın zararlı web sitesini ziyaret etmesi ve istismar kitinin hedef sisteme sızma işleminde başarılı olması durumunda; veri kaybı, fikri mülkiyet hırsızlığı, mali dolandırıcılık ve iş verimliliğinde düşüş gibi sonuçlar ortaya çıkabilmektedir [2].

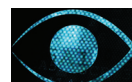


Şekil 2. 2013 yılında siber saldırılarda istismar kitlerinin kullanım oranları [9]

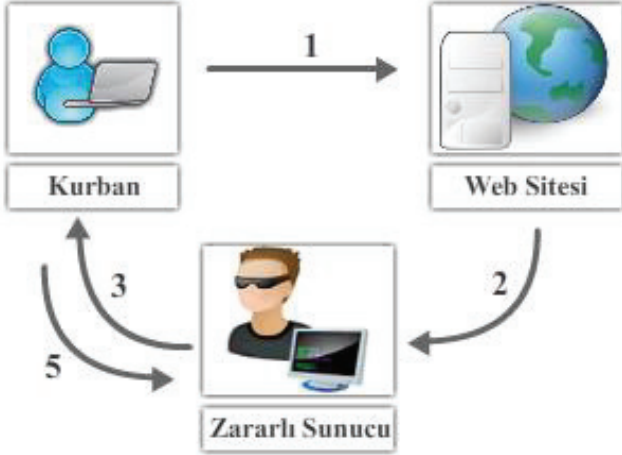
Hedef aldıkları kurbanlarının, istismar kitini bünyesinde barındıran web sitesini ziyaret etmelerini sağlamak için saldırganlar tarafından çeşitli yöntemler kullanılmaktadır. Bu yöntemlerden ilki, kurbanların dikkatlerini çekebilecek mesajlar ya da resimler ile birlikte istismar kitlerinin bulunduğu web sitesine yönlendiren bir web adresini içeren sosyal mühendislik mailleri göndermektir. Fakat günümüzde bilgisayar kullanıcılarının bu tarz maillere karşı nispeten daha bilinçli hale gelmeleri nedeni ile saldırganlar farklı yolları tercih etmektedirler. Saldırganların izlediği bir diğer strateji su kaynağı (watering hole) olarak adlandırılan saldırılardır. Bu tip saldırılarda, saldırganlar hedef aldıkları kullanıcılar ile doğrudan etkileşim kurmak yerine, hedef kullanıcıların ziyaret ettiklerini düşündükleri masum web sitelerini hedef almaktadır. Saldırganlar masum web sitelerini istismar ederek, bu web sitelerini ziyaret eden kullanıcıların istismar kiti barındıran zararlı web sitesine yönlendirilmelerini sağlamaktadırlar [10].

Saldırganlar tarafından yukarıda kullanılan teknikler göz önüne alındığında, istismar kitlerinin kullanıldığı saldırılarda Şekil 3' te gösterilen akış izlenmektedir.

Birinci adımda kurban, siber saldırganlar tarafından içerisine, ziyaretçileri istismar kiti barındıran bir web sunucusuna yönlendiren bir iframe' in enjekte edildiği istismar edilmiş bir web sitesini ziyaret etmektedir. İkinci adımda kurban, aracı sunucular üzerinden istismar kitinin bulunduğu sayfanın sunucusuna yönlendirilmektedir. Üçüncü adımda istismar kiti kurbanın bilgisayarına yönelik bilgi toplama işlemi gerçekleştirmekte ve hedef sistem üzerinde kullanılacak olan istismar kodlarını belirlemektedir. Saldırının dördüncü adımında belirlenen güvenlik açığına yönelik olarak kullanılacak olan istismar kodu temin edilmekte ve hedef sistemine gönderilmektedir. Eğer istismar kodu hedef sistem üzerinde başarılı olursa beşinci adımda saldırının hedef



sistem üzerinde çeşitli eylemlerde bulunmasına olanak sağlayan özel bir zararlı yazılım, hedef sisteme gizlice indirilmekte ve çalıştırılmaktadır [2,5].

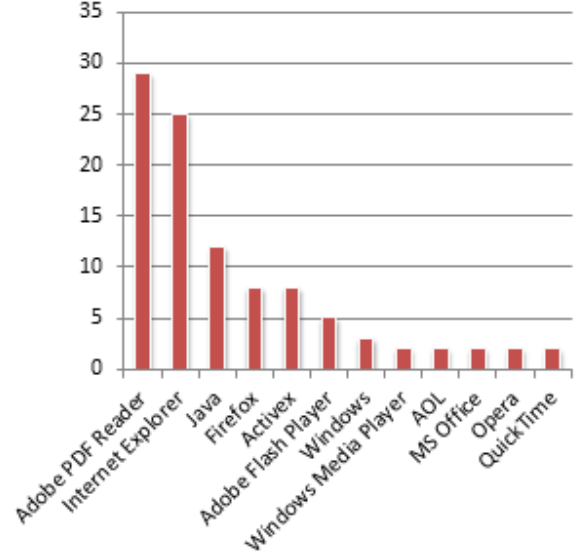


Şekil 3. İstismar kiti tabanlı saldırıların genel akışı

İstismar kitleri çoğunlukla Java, Flash, Adobe Acrobat, Internet Explorer yazılımları ve Windows işletim sistemleri üzerinde bulunan güvenlik açıklarını hedef almaktadır [2]. İstismar kit üreticileri, günümüz bilgisayar kullanıcıları arasında popüler olarak kullanılmakta olan uygulamaların bir listesini oluşturmakta ve bu listeye göre geliştirdikleri istismar kitlerini çeşitli istismar kodları ile donatarak saldırılarda başarı oranlarını arttırmaktadırlar. Örneğin, internetin yaygınlaşması bütün bilgisayar kullanıcıları internet üzerinde işlem yapmak için çeşitli internet tarayıcılarını kullanmaktadırlar. İnternet tarayıcılar ile birlikte gelen çeşitli tarayıcı eklentileri ise saldırganların hedef aralıklarını genişletmektedirler.

2011 yılında KasperskyLAB araştırmacıları tarafından gerçekleştirilen bir araştırmaya göre günümüzde istismar kitlerinin hedef aldıkları uygulamaların %35' ini Internet Explorer, Firefox ve Opera tarayıcıları oluşturmaktadır. Bu da saldırganların hedef aralığında internet tarayıcıların ne kadar önemli bir yer kapladığını göstermektedir. Araştırma verileri incelendiğinde, bilgisayar kullanıcıları arasında popüler olarak kullanılmakta olan Adobe Reader, Oracle Java, Windows Media Player, Adobe Flash, Microsoft Office gibi uygulamalar ise toplam hedef alınan uygulamaların %50' sini oluşturmaktadır [11]. Şekil 4' te istismar kitleri ile gerçekleştirilen saldırılarda hedef alınan uygulamalar ve hedef alınma oranları gösterilmektedir.

İstismar kitleri kullanılarak gerçekleştirilmiş saldırılardan başlıcalarına örnek olarak Hindistan devlet sitelerinden biri olan Küçük ve Orta Ölçekli İşletmeler Bakanlığı web sitesinin 2013 yılının mayıs ayında istismar edilmesi örnek gösterilebilir. Söz konusu web sitesi kullanıcılarını Black Hole istismar kiti barındıran bir sunucuya yönlendirmek üzere istismar edilmiştir[12].



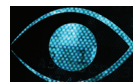
Şekil 4. İstismar kitleri tarafından hedef alınan uygulamalar[11]

2013 yılının ekim ayında ise, günümüzde alexa.com sıralamasına göre dünya üzerinde en çok ziyaret edilen 241. web sitesi olan php.net sitesi, ziyaretçilerini Magnitude adında bir istismar kitini barındıran bir sunucuya yönlendirmek üzere saldırganlar tarafından istismar edilmiştir [13]. İstismar kiti kullanılarak gerçekleştirilen en etkili saldırılardan bir tanesi, 28 Nisan 2014 tarihinde, alexa.com verilerine göre dünya üzerinde en çok ziyaret edilen 89. web sitesi konumunda olan dünyanın en popüler video paylaşım sitelerinden Dailymotion' ın istismar edilmesi ile gerçekleştirilmiştir. Saldırganlar ziyaretçileri, üzerinde Sweet Orange adında bir istismar kiti barındıran bir web sitesine yönlendiren bir iframe'i Dailymotion web sitesine enjekte etmişlerdir. Böylelikle Internet Explorer, Adobe Flash Player ve Oracle Java üzerindeki güvenlik açıklarını hedef alan Sweet Orange istismar kiti, kullanıcıların Bilgisayarlarındaki olası güvenlik açıklarını tespit etmekte ve istismar kodlarını (exploitler) kullanıcıların bırakmaktadır [14]. İstismar kitleri kullanılarak Türkiye' de gerçekleştirilmiş saldırılara örnek olarak 2013 yılında Sağlık Bakanlığı' na ait web sitelerinden birinin istismar edilmesi örnek gösterilebilir. İstismar edilen web sitesi ziyaretçilerini, otomatik olarak istismar kiti barındıran bir sunucuya yönlendirmektedir.

Şekil 5'te sağlık bakanlığına ait istismar edilmiş web sayfasının, malware domain list adresinden elde edilen bilgileri gösterilmektedir.

IV. İSTİSMAR KİTLERİNE KARŞI SAVUNMA ÖNERİLERİ

İstismar kitleri, çeşitli saldırı teknikleri ile kurbanın izni olmadan hedef sistemlere istismar kodları indirilebilmekte ve çalıştırılabilmektedir. Birçok istismar kiti, yıllar önce deşifre olmalarına rağmen hala hedef aldıkları sistemler üzerinde göz ardı edilemeyecek düzeyde başarı oranı yakalamaktadırlar.



Date (UTC)	Domain	IP		
↑ ↓	↑ ↓	↑ ↓		
2013/06/05_20:17	www.tdms.saglik.gov. [REDACTED] [REDACTED].htm	[REDACTED]		
Reverse Lookup	Description	Registrant	ASN	
↑ ↓	↑ ↓	↑ ↓	↑ ↓	
-	compromised sites lead to exploit kit	Salk Bakanl / netsistem@saglik.gov.tr	9121	

Şekil 5. Sağlık bakanlığına ait istismar edilmiş bir web sitesine ait bilgiler

Günümüzde istismar kitleri tarafından istismar edilen güvenlik açıklarının %60'ı iki yıldan fazla süredir istismar edilmektedir. İstismar kitlerinin, söz konusu güvenlik açıklarını istismar etmede hala bu denli başarılı olmalarının nedeni bilinçsiz kullanıcıların sistemlerini güncel tutmamalarıdır [4]. İstismar kitlerinden korunmak için, kullanıcı bilgisayarları üzerinde yer alan işletim sistemi, internet tarayıcı gibi istismar kitlerinin hedef aldıkları uygulamaların son güncel sürümlerine sahip olduklarından emin olunmalıdır. Kullanıcıların söz konusu uygulamaları güncellemeyi unutmama ihtimaline karşı, uygulamaların güncelleştirmeleri otomatize bir şekilde gerçekleştirilmelidir. Ayrıca mümkün olduğunca sistemler üzerinde korsan yazılım kullanımından kaçınılmalı ve lisanslı yazılımlar kullanılmalıdır. Güvenli bir tarayıcı kullanmak ve yazılımları güncel tutmak, istismar kitlerinin başarılı olduğu güvenlik açıklarının büyük çoğunluğunun kapatılmasını sağlayacak ve istismar kitlerinin etkinliğinde büyük bir azalmaya neden olacaktır. Unutulmamalıdır ki, piyasada bulunan birçok eski istismar kiti, hedef alınan sistemler üzerinde yer alan güncellenmemiş yazılımlar nedeni ile hala etkili bir saldırı aracı durumdadır.

Bir kurum bünyesinde hangi sayıda bilgisayar kullanıcısına sahip olursa olsun, istismar kitlerine karşı alabileceği en etkili önlemlerden biri, bünyesindeki çalışanlarına olası tehlikeler ve saldırılara karşı farkındalık sağlamaktır. Çünkü çalışanlar, siber saldırganlar tarafından gerçekleştirilen saldırılar hakkında bilgi sahibi olmaları durumunda olası bir saldırıyı ve gelebilecek zararlı yazılımları tanıyacak, dolayısı ile bu zararlı yazılımların kurumsal ağ içerisine girmesine neden olabilecek bir eylemde bulunmayacaktır. Bunun sağlanması için kurumların bilgi işlem departmanları, kurum yönetimi ile işbirliğinde olmalı, ağ güvenliği ve çalışanların eğitimi gibi kurum ağını daha güvenli hale getirilecek işlemler beraber planlanmalıdır. Periyodik aralıklarla kurum içerisinde ki çalışanlara bilinçlendirme ve farkındalık eğitimleri sağlanmalıdır. Böylelikle kullanıcılar bilinmeyen kişiler aracılığı ile gelen elektronik postalara tıklamama ve güvenliğinden şüphe duyulan web adreslerine yönlendirici linkleri açmama gibi farkındalıklara sahip olacaktır.

Ayrıca günümüzde birçok işletme varolan güvenlik duvarlarının, onları saldırılardan koruyacağına inanmaktadırlar. Gerçekte ise, eski güvenlik duvarları bugün

kuruluşlar için ciddi bir güvenlik riski oluşturmaktadırlar. Birinci nesil güvenlik duvarı teknolojisi bugünün internet suçluları tarafından gönderilen zararlı yazılım içeren ağ paketlerini denetlemek ve olası saldırılardan korumak için yetersiz hale gelmiştir [2]. Bu nedenle; işletim sistemlerinde “beyaz liste” mantığı kapsamında yalnızca belirli uygulamaların çalışmasına olanak sağlayan Bit9 gibi uygulamaların kullanımı ile istismar kitlerinin neden olduğu tehditlerden büyük oranda korunabilmektedir. Ayrıca kurumlar, kullanıcılarını sıfırcı gün (zero day) güvenlik açıklıklarına karşı etkili bir şekilde koruyabilmek için, sezgisel çalışma ve analiz yeteneklerine sahip olan aktif ağ cihazları kullanmalıdırlar. Bu sistemler, exe, bat, swf, pdf gibi uzantılara sahip olan çalıştırılabilir tüm uygulamaları, kendi içlerinde barındırdıkları sanal sistemler üzerinde davranışsal olarak analiz edebilmekte ve istismar kitlerinin neden olduğu tehditleri tespit edebilmektedirler. Eğer bir kurum, siber saldırılara karşı ciddi tehdit altında ise, istismar kitleri ve diğer çeşitli saldırı türlerine karşı önceden haber alma ve etkili korunma sağlamak amacıyla “siber istihbarat” hizmeti veren çeşitli kurumlar ile ortaklaşa bir çalışma yürütebilmektedirler.

Kurumlar içerisinde kullanılan ağ ve güvenlik cihazlarından çok fazla miktarda log üretilmektedir. Üretilen logların kurum bilgi işlem personelleri tarafından düzenli aralıklarla kontrol ve analiz edilmesi, kurum güvenliği açısından büyük önem taşımaktadır. Bu nedenle kurum içerisinde yer alan tüm sistemlerin log kayıtları merkezi bir sunucuda eş zamanlı olarak toplanmalı ve log kolerasyonu işlemine tabi tutulmalıdır. Bu işlem sonunda elde edilen verilere göre istismar kiti tabanlı saldırılar alarm durumu olarak kaydedilebilmektedir. Böylelikle tanımlanan alarm durumunun gerçekleşmesi anında uygulanmak üzere koruyucu işlemler tanımlanabilmektedir. Çünkü her başarılı ya da başarısız saldırı girişimi mutlaka sistemler üzerinde bir kayıt oluşturmaktadır. Bu kayıtlar uygun kurallar ile kolerasyon işlemine tabi tutularak, saldırı aşamasında ya da başarılı olmuş bir saldırı sonrasında, sistemler üzerinde bıraktıkları izler büyük oranda bulunabilmekte, elde edilen veriler gerekli güvenlik önlemlerinin alınması amacıyla kullanılabilir.

V. SONUÇ

Yapılan araştırmalar göstermektedir ki, istismar kitleri günümüz siber suç dünyasında saldırganlar tarafından kullanılan silahların en başında gelmektedir. İstismar kitlerinin bu denli popüler olmasının başlıca nedenleri; içerisinde düzenlerce istismar kodlarını barındırmak suretiyle saldırganlara çok büyük boyutlarda bir saldırı kütüphanesi sağlaması ve bir sisteme yönelik gerçekleştirilecek sızma denemelerini saldırgandan bağımsız olarak otomatize etmesidir.

Yapılan araştırmalar sonunda sıfır gün istismar kodları da dâhil olmak üzere en güncel istismar kodlarını bünyesinde barındıran istismar kitleri kadar, iki yıldan fazla bir süredir saldırganların kullanımında olan istismar kitleri de saldırılarda başarılı olmaktadır. Bunu en temel nedeni ise günümüz bilgisayar kullanıcılarının sistemlerini güncel tutmak konusunda gösterdikleri dikkatsizliktir.

Bu çalışma da istismar kitleri geliştirildikleri ülke bazında incelenmiş, istismar kitlerinin satışa sunulduğu yer altı piyasalarının sosyal karakteristiklerine değinilmiştir. Ayrıca istismar kitleri kullanılarak saldırganlar tarafından gerçekleştirilen saldırı tipleri araştırılmış ve gerçekleştirilen saldırıların genel bir akışı sunulmuştur. Çalışmada istismar kitlerine karşı alınabilecek en temel önlemin kullanıcı bilinçlendirilmesi ve kullanılan sistemlerin güncel tutulması olduğuna değinilmiş ve istismar kitlerine karşı savunma önerileri maddelenmiştir.

KAYNAKLAR

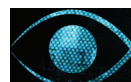
- [1] Symantec Corporation. (2014 April). Symantec Internet Security Threat Report 2014 [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
- [2] F. Malecki, "Defending Your Business From Exploit Kits", *Computer Fraud & Security*, pp. 19-20, 2013.
- [3] L. Allodi, V. Kotov and F. Massacci, "MalwareLab: Experimentation with Cybercrime Attack Tools", presented at the 6th Workshop on Cyber Security Experimentation and Test, Berkeley, CA, 2013.
- [4] J. Cannell. (2013, February 11). Tools of the Trade: Exploit Kits [Online]. Available: <http://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/>
- [5] V. Kotov, F. Massacci, "Anatomy of Exploit Kits", *Engineering Secure Software and Systems*, Springer Berlin Heidelberg, 2013, pp. 181-196.
- [6] M. Motoyama, D. McCoy, K. Levchenko, S. Savage and G. M. Voelker, "An analysis of Underground Forums", in *Proceedings of the ACM Internet Measurement Conference*, Berlin, 2011, pp. 71-80.
- [7] Solutionary Incorporated. (2013 January). SERT Quarterly Threat Report-Q4 2012 [Online]. Available: http://www.solutionary.com/_assets/pdf/research/solutionary-sert_q42012_research.pdf
- [8] C. Grier, et al., "Manufacturing compromise: the emergence of exploit-as-a-service", in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, North Carolina, 2012, pp. 821-832.
- [9] Sophos Limited Company. (2014 January). Sophos Security Threat Report 2014 [Online]. Available: <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf>
- [10] M. Sarica, (2013, August 1), İstismar Kiti Nedir [Online]. Available: <http://www.mertsarica.com/istismar-kiti-nedir/>
- [11] V. Diaz, M. Preuss. (2011, February 10). Exploit Kits- A Different View [Online]. Available: http://www.securelist.com/en/analysis/204792160/Exploit_Kits_A_Different_View, Şubat 2011

- [12] P. Paganini. (2013, May 27). Watering Hole Attacks And Exploit Kits-Indian Gov Site Case [Online]. Available: <http://securityaffairs.co/wordpress/14725/hacking/watering-hole-attacks-exploit-kits-indian-gov-site-case.html>
- [13] P. Paganini. (2013, October 26). Php.net Compromised And Redirecting to Magnitude Exploit Kit [Online]. Available: <http://securityaffairs.co/wordpress/19070/cyber-crime/php-net-compromised.html>
- [14] A. Singh. (2014, July 03). Dailymotion Compromised to Send Users to Exploit Kit [Online]. Available: <http://www.symantec.com/connect/blogs/dailymotion-compromised-send-users-exploit-kit>

Doç. Dr. Ecir Uğur Küçüksille- 1976 yılında Isparta'da doğdu. Lisans eğitimini Gazi Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği Bölümü'nde tamamladı. Yüksek Lisans Eğitimini Süleyman Demirel Üniversitesi Makine Eğitimi Ana Bilim Dalında yaptı. Doktora Eğitimini Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü İşletme/Sayısal Yöntemler Ana Bilim Dalında tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.

Mehmet Ali Yalçınkaya- 1990 yılında Isparta'da doğdu. Lisans eğitimini Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği'nde tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisi olarak görev yapmakla birlikte, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında, bilgi güvenliği ve sızma testleri yer almaktadır.

Ozan Uçar- 2006 yılından itibaren profesyonel iş hayatında sızma testleri, Linux sistemlerin güvenliği ve bilişim güvenliği eğitimleri vermektedir. 2010 yılı itibarıyla BGA Bilgi Güvenliği Eğitim ve Danışmanlık firmasında bilişim güvenliği üzerine eğitimler vermekte ve sızma test ekibi liderliği yürütmektedir. Çalışma alanları içerisinde sızma testleri, ağ sistemlerinde adli bilişim analizi ve bilişim güvenliği yer almaktadır.



Siber Güvenlik ve Savunma için BM Bilim Dalı Kuruluş Çalışmasının Amacı, Yapısı, Anlamı, Kullanımı, Yüksek Teknoloji Üretme Gücü Üzerinde Açıklamalar

F. Ünlü

Abstract— Author studied the Knowledge-Based Object (BTN) which has Communicating Tic of Tics Cloud Storage Herd (TTBBS) formatted Q memory designs or Communicating Spiral Clouds Memory Herd (BBSS) formatted Q memory designs. The axioms of the communication exist on the same $k \in \text{Kip}[n] = \{0, 1, 2, n-1\}$, $n \in \mathbb{N}$, coded $\langle \text{tamra}, \text{ramta} \rangle$ antennae pairs which are able to conduct information perception and secretion were searched and found. Grammar's rules appearing in some Formal Grammar (BG) in a given Grammar Closure (BG*) have been identified and used for this purpose. Formal language TASIM was designed. In TASIM, Knowledge Based Object (BTN) with TTBBS formatted Q memory or BBSS formatted Q memory structures are generated. They are programmable by some special algorithms to generate $\text{Kip}[n]$ based FÜ-Algebras. Obtained results are loaded into Q memories of Communicating Mathematics which has been under study since 1968 by FÜ. Therefore, for cyber security and defense; the structure, meaning, usage and some important disclosures of Communicating Mathematics (BM) are introduced concisely in this paper for helping to produce new high-technologies. The meanings of the new words and brief vocabularies are given at the beginning of the first section.

Key words: Boolean algebra, $\text{Kip}[n]$ algebra, CITALOG, FÜ algebra.

Özet — Yazar tarafından bildirisi yapmaya muktedir olan Tiklerin Tiki Bulut Bellek Sürüsü (TTBBS) veya Bildirisi Bulut Bellek Sürüsü Sarmalı (BBSS) formatında Q bellekli Bilgi Tabanlı Nesne (BTN) tasarımları çalışıldı. Tamra ve ramta adlı anten sistemlerinde aynı $k \in \text{Kip}[n] = \{0, 1, 2, \dots, n-1\}$, $n \in \mathbb{N}$, kodlu $\langle \text{tamra}, \text{ramta} \rangle$ çiftlerinde yürütülmekte olan bilgi algısı ve salgısının bildirisi belitleri kümesi arandı ve bulundu. Verilen bir Biçimsel Gramer (BG) yıldız kapanış kümesi (BG*) içinde yer alan BG kuralları bu amaç için tespit edildi ve kullanıldı. BD olan TASIM dilini üreten BG kuralları bulundu. BD olan TASIM dilinin tasarımı yapıldı. İçeriğinde kendi içinde bildirisi yapabilen TTBBS formatlı veya BBSS formatlı Q bellek ihtiva eden BTN tasarımlarının üretilebileceği algılandı. Bildirisi yapan yazılım yongası olarak TTBBS veya BBSS Q bellekli BTN tasarımları, BD TASIM dili içeriğinde, TASIM BG kuralları ile üretildi. FÜ-cebir üretmek için özel olarak tasarlanmış farklı algoritmalarla programlanabileceği bulundu. FÜ tarafından 1968 yılından beri üzerinde çalışmakta olunan ve bildirisi BTN tasarımlama bilim dalı diye adlandırılan BM içeriğine konuldu. Bu nedenle, siber güvenlik ve

savunma için BM Bilim Dalının amacı, yapısı, anlamı, kullanımı ve yüksek teknoloji üretme gücü üzerinde önemli olan açıklamalar bu bildiride özlü biçimde yapılacaktır. Özet içeriğinde geçen kısaltma ve yeni sözcüklerin anlamları giriş kesiminin başında verilmiştir.

Açar Sözcükler — Boole cebir, $\text{Kip}[n]$ cebir, CITALOG, FÜ cebir.

1. GİRİŞ

BM üzerinde yapılacak açıklamalar içeriğinde kullanılacak kısaltma ve sözcüklerin anlamları:

BB: Bulut Bellek. Her elamanı tiklerin tiki olarak oluşturulmuş olan bir Q bellekli BTN tasarımı kümesi göz önüne alalım. Burada her Q bellek, tiklerin tiki olan alt tik Q belleklerden oluşmuştur. Bir BD imdizisidir. BG kurallarını yenidenlikli biçimde kullanan algoritmalarla birbirleri ile bildirisi yapabilmek yeteneğine sahip olarak üretilmiştir. Bu özelliklere sahip olan her tiklerin tiki Q bellek sürüsü yapısına bu nedenle bu bildiride bir BB denmiştir.

BD: Biçimsel Dil. BM içinde yapısı, anlamı ve kullanımı kesin olarak, yani %100 kesinlikle, algılanabilen diller. ALGOL, C, TASIM dilleri gibi. Her BD içeriğini üreten en az bir BG vardır.

Biçimsel Düşünme: %100 yapısı, anlamı ve kullanımı bilinen ham mantık bilgilerinden %100 yapısı, anlamı ve kullanımı bilinen sonuç mantık bilgileri çıkarımı yapan akıl erkinin zihinde kurgusunu yaptığı algoritma yapısında bir fonksiyon.

BG: Biçimsel Gramer.

BG*: BG kümesi.

Bellek: Hafıza. İyi organize olmuş BTN oluşumlarını içeriğinde konaklayabilen biçimsel düşünme erkine sahip beyin yapısı.

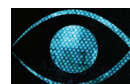
Biçimsel: %100 kesin yapı, anlam ve kullanıma sahip olan.

Bildirisi: Çok katmanlı biçimsel iletişim. Çok katmanlı biçimsel haberleşme.

BBS: Bulut Bellek Sürüsü. Birden çok BB ihtiva eden BB yapısına verilen isim.

BBSS: Bildirisi Bulut Bellek Sürüsü Sarmalı. Bir BBS içeriğinde yer alan her Q belleğine bir BBS yüklemekle elde edilen yeni BBS yapısına verilen isim.

BÇK: Bildirisi Çekimi Kanunu.



BM: Bildirişimli Matematik. Çok katmanlı ortamlarda güvenli biçimsel iletişim yaparak, güvenli SM bilgilerinden güvenli SM bilgileri üretebilen matematik.

BMD: Biçimsel Mantık Değeri.

BMT: Biçimsel Mantık Tasarımı.

BMD kuantumları: N doğal sayılar kümesi verildiğinde, $Kip[n] = \{ 0, 1, 2, \dots, n-1 \}$, $n \in \mathbb{N}$, kümesinin elemanlarına verilen isim.

BMF: Biçimsel Mantık Fonksiyonu.

BMT: Biçimsel Mantık Tasarımı.

BTN: Bilgi Tabanlı Nesne. Bir BG ile bir BD içeriğinde tiklerin tiki olarak üretilen imdizi, bir biçimsel sistemi temsil ediyor ise ona bir BTN denir. BTN yapısı, anlamı ve kullanımı %100 kesin biçimde algılanarak yapılandırılabilir, anlamlandırılabilir ve kullanılabilir. Alt bileşenlerinden bazıları veya hepsi tiklerin tiki BTN biçiminde oluşturulmuş olabilir.

Bulut: Gözlenebilen, sayılabilir çokluktaki tik BTN tasarımları değişik çözünürlüklü teknolojiler altında değişik yönlerde değişik hızlarla hareket ederken veya ettirilirken, YÇK ve BÇK ilkeleri altında bildirişim yapma erki kazanır ise; bu BTN kümesine bulut denir.

BBSS: Bildirişimli Bulut Bellek Sürüsü Sarmalı. Bir F formatlı TTBBS Q bellek içeriğinde görülen en az bir S formatlı alt TTBBS Q rand belleklerine aynı veya farklı formatlı tiklerin tiki Q bellek yüklenerek elde edilen Q bellek türüdür. Bir algoritma ile programlanabilir. En az bir X formatlı TTBBS Q bellek ve çok sayıda S formatlı Q bellek içerir.

CITALOG: Compact and Integrated TAsim LOGic.

DSSTM: Döngülü Sayı Sistemi Tasarım Modeli.

F: Fonksiyon yutan, içeriğinde yuttuğu fonksiyonu tutan ve işleyen TTBBS veya BBSS Q belleği. İşini iyi yapabilmesi için özel biçimde F-formatı ile formatlanmıştır.

FÜ-cebir: $Kip[n]$, $n \in \mathbb{N}$, değerli CITALOG. Her $Kip[n]$, $n \in \mathbb{N}$, değerli Boole cebir. $Kip[n]$ tabanlı cebir.

FÜ-BMT fonksiyonu: CITALOG formatlı $Kip[n]$, $n \in \mathbb{N}$, değerli Boole fonksiyonu.

İmdizi: Harf, hece, kelime, cümle, paragraf, metin, resim, çoklu resim ve müzik ile süslenmiş metin kompozisyonu, medya tasarımı, I@I tasarımı, BTN tasarımı, vb.

I@I: İnternet içinde İnternet.

$Kip[n]$ = $\{ 0, 1, 2, \dots, n-1 \}$, $n \in \mathbb{N}$. Tam n farklı BMD kuantumu içeren BM kümesi.

$Kip[n]$ -cebir: FÜ-cebir.

N = $\{ 0, 1, 2, \dots, n-1, n, n+1, \dots, \infty \}$ doğal sayılar kümesi.

Ramta: İki farklı durumun birinde bilgi alabilen ve diğerinde bilgi salabilen rand anteni.

Rand: Verilen bir frekans veya dalga-boyunda bilgi almayı ve salmayı sahip olduğu ramta antenini kullanarak yapmayı biçimsel olarak iyi bilen ve yapan Q bellekli BTN tasarımı. Operand.

Rator: Verilen sonlu sayıda frekans veya dalga-boyunda bilgi almayı ve salmayı sahip olduğu bir tamra anten bulutu aracılığıyla iyi bilen ve yapan BTN tasarımı. Operator.

RCR: Rator-Cab-Rand. RCR bir sistem tasarım formatıdır.

Q: S, X ve F gibi üç farklı biçimde formatlanabilen BBS. Bir BBS kümesinden oluşmuş veya oluşturulmuş BBS.

S: Sabit formatlı TTBBS veya BBSS Q bellekli BTN yutan, içeriğinde tutan ve işleyen bir Q belleği. İşini iyi yapabilmesi için özel biçimde S-formatı ile formatlanmıştır.

SM: Standart Matematik.

Tamra: İki farklı durumun birinde bilgi salabilen ve diğerinde bilgi alabilen rator anten bulutu.

TASIM: Tidy Automatic Sequential Information-processing Mechanism.

Tik: Alt bileşenlerine kolay ayrılmayan tiklerin tiki bir BTN oluşumdur. Alt tik BTN bileşenlerine kolay ayrılmayı engelleyen, şeffaf veya şeffaf olmayan, bir giysi giyinmiş olabilir. **Örnekler:** 1. Tanrı parçacığı, foton, proton, nötron ve elektron benzeri fiziksel parçacıklar. 2. Atom, molekül ve madde gibi kimyasal oluşumlar. 3. Hücre, yumurta ve beyin gibi biyolojik oluşumlar. 4. Tohum, çekirdek ve meyve gibi tarımsal ürünler. 5. Harf, kelime ve cümle gibi dil veya dilbilim yapıları. 6. Kum tanesi, toz parçası ve plaj kumu gibi doğal oluşumlar. 7. Fert, aile, köy, kasaba, şehir, millet ve ülke gibi sosyal veya kitlesel oluşumlar. **Tok:** Tik olmayan BTN oluşumu.

TTBBS: Tiklerin Tiki Bulut Bellek Sürüsü. **Örnek**

Açıklama: 1. Her kuş bir BTN oluşumdur. Başı içinde, üzerine elastik şeffaf veya şeffaf olmayan zar torba giysisi giydirilmiş, bir Q bellekli BTN oluşumu örneğidir. Doğada mevcuttur. Bir kuş sürüsü gökyüzünde uçarken gözlenebilir. Çok geniş bir elastik şeffaf torba anlamında atmosfer giysi içinde dolaşırken bir TTBBS Q bellek oluşumu olarak algılanır. Onu bir BTN olarak oluşturan bir doğal BG vardır. Sürüye yeni kuş veya yeni kuşlar katılırsa BTN oluşumunun Q belleği büyür. Sürüden bir kuş veya birden çok kuş ayrılırsa BTN oluşumunun Q belleği küçülür.

TTBBS BTN: Tiklerin Tiki Bulut Bellek Sürüsü BTN. Rator ve rand olarak kümelenip bildirişim yaparak bilgi işleme yeteneği kazanmış olan bir tik Q bulut bellekli BTN oluşumdur.

TTTBBBS: Tikler ve Tokların oluşturduğu Tok Bulut Bellek Sürüsü.

X: Değişken BTN oluşumu yutan, içeriğinde tutan ve işleyen Q bulut belleği. İşini iyi yapabilmesi için özel biçimde bir X-formatı ile formatlanmıştır.

Yenidenlikli: Kendi geleceğini kendi geçmişi ile tanımlayan.

YÇK: Yer Çekimi Kanunu.

Yonga: Programlanabilir Q bellekli BTN.

Günümüzde, SM uygulaması olarak üretilen değişik teknolojilere bağımlı yazılım ve donanım yongalarının ustalıklı tasarımı, gerçekleştirilmesi ve kullanımı yeryüzü yaşamını her yönü ile etkileyip değiştirmektedir. Bulunan yeni algoritmalar farklı TTBBS veya BBSS yapısında Q belleği olan BTN üretimlerini tetiklemektedir. Bu tetiklemelerin sonucunda BM bilimi; genişleme büzülme özelliğine sahip olan TTBBS veya BBSS Q bellekli BTN tasarımı, gerçekleştirilmesi ve kullanımı bilimi dalı olarak doğdu. Onu üreten BG küme kapanışları bulundu. Alt bileşenleri ile bildirişim yaparak biçimsel bilgidan biçimsel bilgi üretme, yorumlama ve yayma

yolunda hızla gelişti ve gelişiyor. $Kip[n]$, $n \in \mathbb{N}$, BMD kuantumları kümesini N doğal sayılar kümesinin bir alt kümesi olarak tanımladı. Bulutsu tamra ve ramta antenleri ile bildirişim yapmaya muktedir olan m rator denetim değişkeni ile denetlenebilir n^m rand sabitinden oluşan, $Kip[n]$, $n \in \mathbb{N}$, BMD kuantumları ile programlanabilir $ü[m, n]$ sayıda F formatlı BMF BTN tasarımı üretildi. Üretilen bu F formatlı BMF BTN fonksiyon tasarımlarını kullanarak her $n \geq 2$, $n \in \mathbb{N}$, değerli mantıkta; yeni çıkarımlar yapmak mümkün olmuştur. Bir $Kip[n]$ -cebir bulunmuştur. Duyurulur.

Yazar, özgün biçimde hayal ettiği **BM bilim dalının amacını, yapısını, anlamını, kullanımını, yüksek teknoloji üretme gücünü ve diğer içeriklerini**, 1968 yılından beri bilinçli ve özverili olarak çalışmaktadır. Artık m değişkenli ve n farklı BMD tanımını kullanan BMT içeriğinde çıkarım yapabilmenin yolu, bilim dünyasının kullanımına açılmıştır. Önemli olan bulgular aşağıda özetlenmiştir.

1. BG kurallarına sahip olan $T = \text{TASIM}$, bir BD olarak tasarlanmıştır. Bildirişim yapan TTBBS veya BBBSS Q bellekli BTN tasarımı yapmada kullanılmıştır.

2. $T = \text{TASIM}$ BD BTN tasarımı içeriğinde $Kip[n]$, $n \in \mathbb{N}$, kuantum değerlerine duyarlı olan; genişleme-büzülme özelliğine sahip programlanabilir S , X ve F formatlı TTBBS veya BBBSS Q bellekli BTN dağılımları ile donatılmış yenidenlikli tasarım teknolojileri kullanılarak; yeni TTBBS veya BBBSS Q bellekli BTN model tasarımları elde edilmiştir. Genişleme-büzülme özelliğine sahip olan TTBBS veya BBBSS Q belleklerini kullanan, özel programlama algoritmaları ile F , X ve S formatlı BMT fonksiyonları üreten, BTN model tasarımları bulunmuştur. Böylelikle F , X ve S formatlı TTBBS veya BBBSS Q bellekli BTN tasarımı içeriğinde biçimsel bildirişim kurma, sürdürme ve kullanıma sunma yöntemleri çalışılmıştır, yapılandırılmıştır, anlamlandırılmıştır ve kullanımdadır.

3. Özel “@” sembolünü bildirişim merkezi anlamında kullanarak; F , X ve S formatlı TTBBS veya BBBSS $Q = Q@Q$ belleği tasarımının temel ilkeleri çalışılmıştır. Her $ü[m, n]$ sayısında, m değişkenli ve n değerli F , X ve S formatlı BMT fonksiyonu üreten TTBBS veya BBBSS Q bellekli BTN tasarımı bulunmuştur. Bir özel programlama tekniği kullanılarak F fonksiyonlarının programlandığı Q belleklerinin her biri, n farklı bildirişim pin kodu(veya e-kimliği) olan tamra ve ramta antenlerini kullanarak; kendi iç dinamik yapısı içinde bildirişim yapıp, kendi mantık fonksiyonu değerini bulabilmektedir. Sonsuz sayıda $Kip[n]$, $n \in \mathbb{N}$, tabanlı e-kimliklerini kullanan TTBBS veya BBBSS Q bellekli BTN model tasarımları bulunmuştur ve yayınlanmıştır. Bunların %99'dan daha çoğu bu gün bilim dünyasında akıllı yaşam tarafından bilinmemektedir.

4. TTBBS veya BBBSS Q bellekli BTN tasarımları ve onların imdizi olarak üretilen benzetim modelleri en az bir BD içeriğinde bir BG ile üretilmiştir.

5. Basit ve karmaşık yapıda yenidenlikli alt TASIM algoritmalarını kullanılarak TTBBS veya BBBSS Q bellekli BTN tasarımları, değişik formatlı TTBBS veya BBBSS Q bellekli BTN oluşumlarını yutabilmektedir. Bunun sonucu olarak genişleyip büzülebilen yeni TTBBS veya BBBSS Q bellekli BTN tasarımları oluşmaktadır. Böylece her TTBBS veya BBBSS Q bellekli BTN tasarımı kendi kendine evrimleşmektedir. TTBBS veya BBBSS Q bellekli BTN tasarımlarından yeni TTBBS veya BBBSS Q bellekli BTN oluşturan TASIM algoritmaları bulunmuştur.

6. Her $k \in Kip[n]$, $n \in \mathbb{N} - \{0, 1\}$, BMD kuantumunu kullanan m değişkenli F ve X formatlı BMF tasarımının nasıl yapılacağı sorunu yazar tarafından kesinlikle çözülmüştür. Özellikleri çalışılmıştır. Değişik tür $Q = Q@Q$ ve $I = I@I$ modelleri geliştirilmiştir. Duyurulur.

7. Evrenin her zerresinde yer alan her TTBBS veya BBBSS Q bellekli BTN bileşeninin, her an çok katımlı biçimsel bildirişim yaparak, sürekli değişebilen ve evrimleşebilen, bir bildirişimli TTBBS veya BBBSS Q bellekli BTN modeli tasarımı olduğu görülmüştür.

8. Evrende tıpkı YÇK gibi mevcut olan bir BÇK vardır. Bulunmuştur. YÇK ve BÇK gereğince her TTBBS veya BBBSS Q bellekli BTN tasarımı, iç ve dış biçimsel bildirişimini yapma yeteneğine sahip olmaktadır. Duyurulur.

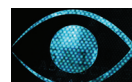
II. BM BİLİM DALININ AMACI, YAPISI, ANLAMI, KULLANIMI, YÜKSEK TEKNOLOJİ ÜRETME GÜCÜ VE İÇERİĞİ ÜZERİNDE AÇIKLAMALAR

Bu kesimde 16 farklı BM açıklaması sıra ile kısa ve özlü biçimde yapılacaktır.

1. BM, N doğal sayılar kümesini ve onun özelliklerini doğal olarak algılar ve öğretir. N doğal sayılar kümesinden özel yapılı alt küme olarak üretilen her sonlu $Kip[n]$, $n \in \mathbb{N}$, kümesi içinde yer alan kuantumu(rakamı veya sayıyı) bir BMD olarak algılar. Onun için gerekli olan yeterli sayıda belitleri ifade eder ve kullanır.

2. BM, evren veya doğa varlıklarını bir konik ortamında kendi aralarında bildirişim yapamaya zorlayan bir BÇK olduğunu bilir. Onu anlatabilmek için tanımsal belitleri bulur, yapılandırır, anlamlandırır ve kullanır. Bilim dünyasına duyurur.

3. BM, çıplak gözle görünen veya görünmeyen, her evren veya doğa varlığını biçimsel düşünme yolu ile algılar. $Kip[n]$, $n \in \mathbb{N}$, BMD kuantumlarını tamra ve ramta anten sistemlerinde yer alan ve bildirişim kurup yapan $\langle \text{tamra, ramta} \rangle$ anten çiftlerinin frekansı veya dalga boyu kodu olarak kullanır. Evrende ve doğada üretilen, değişik $Kip[n]$, $n \in \mathbb{N}$, alfabeli biçimsel dillerde bildirişim kuran ve yürüten, TTBBS



veya BBBSS Q bellekli BTN kodlarının olduğunu bilir. Bu kodlar, bir BG ile üretilmiş bir BD imdizileridir. Bilim insanı, çok gizemli görünen evrenin veya doğanın, TTBBS veya BBBSS Q bellekli BTN kodlarını algılayıp çözebilmek için biçimsel olarak düşünmek ve düşündüklerini bir BD ile anlatmak zorundadır. Yönlendirici rol oynayan akıllı yaşamın geleneğinde ve göreneğinde bu vardır. Biçimsel düşünmenin sonucu olarak, akıllı yaşam bir BD içinde birbirleri ile bildirişim kuran, yapan ve etkileşen TTBBS veya BBBSS Q bellekli BTN tasarımlarını üretmiştir. BM içeriğinde biçimsel düşünme erki, gerektiğinde “tik BTN, TTBBS BTN, TTBBS veya BBBSS Q bellekli BTN” ve “tok BTN, TTBBS BTN veya TTBBS Q bellekli BTN” deyimlerini eş anlamlı deyimler olarak kullanır. Başında tik ve tok vurgusu olmayan her BTN deyimini bir tik veya bir tok BTN oluşumu anlamında algılanır. Tik BTN tasarımları belirlenen belli amaçlar doğrultusunda yazılım veya donanım olarak yorumlanmıştır ve tasarımları gerçekleştirilmiştir.

4. BM, değişik $Kip[n]$, $n \in N$, kümesi üzerinde sonsuz sayıda birbirinden farklı DSSTM yapısının varlığını bilir. Onların bir tik BTN tasarımını yapılandırılırken, anlamlandırılırken, kullanılırken arka planda bir gizemli SM kavramı biçiminde var olduğunu algılar, gereğinde yeniden yapılandırır, anlamlandırır ve kullanır.

5. BM, günümüz SM tasarımını bir BD olarak algılar. SM içeriğini BM içeriğindeki m değişkenli ve n değerli biçimsel bildirişim yapmaya muktedir olan biçimsel mantık tik BTN modellerinin yapılandırılmasında, anlamlandırılmasında, kullanılmasında ve gerçekleştirilmesinde anlatım dili olarak kullanır.

6. BM, çok güçlü bildirişim yapmaya muktedir olan TTBBS veya BBBSS Q bellekli BTN oluşumu modellerini, bir BG tarafından oluşturulup kontrol edilen kapanış kümesinde imdizi tasarımları olarak üretir. Farklı BG altında üretilen farklı BD içinde tanımlı TTBBS veya BBBSS Q bellekli BTN küme kapanışları vardır. Onların farklı özelliklerini algılar, çalışır, geliştirir ve kullanıma sunar.

7. BM, her BTN tasarımının TTBBS veya BBBSS Q belleğindeki alt tik belleklerin sayısını bilir. Onların S formatlı olanlarını programlayarak F ve X formatlı BMT türü veya diğer bilinen türlerde yeni fonksiyonları üretir.

8. BM, evrende ve doğada var olan her sonlu TTBBS veya BBBSS Q bellek tasarımını çalışır. Sonlu sayıda S formatlı Q bellekli BTN olarak tasarlanmış **rand** BTN tasarımlarını sonlu sayıda X formatlı Q bellekli BTN **rator** BTN tasarımları ile kontrol eden, yeni F ve X formatlı Q bellekli BTN tasarımlarını algılar, tasarımlar, değişik teknolojiler kullanarak yapılandırır, anlamlandırır ve kullanır. Bildirişim yaparak S formatlı Q bellekli rand BTN tasarımlarını kontrol eden X formatlı TTBBS veya BBBSS Q

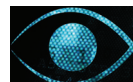
bellekli rotor BTN tasarımları BM içeriğinin en önemli bileşenleridir. F ve X formatlı TTBBS veya BBBSS Q bellekli BTN tasarımları TASIM programları biçiminde bulunmuştur. Bu gün bir TTBBS veya BBBSS Q bellek içinde gözlenen S biçimli Q bellek kümeleri, uygun $Kip[n]$, $n \in N$, kuantumları kullanarak oluşturulan sayma sistemlerinin sayıları ile programlanabilmektedir. Yani her $Kip[n]$, $n \in N$, BMD kuantumu tanım bölgesinde tanımlı biçimsel mantık tasarımı fonksiyonları üretilmektedir. Bu her $Kip[n]$, $n \in N$, kuantumları mantığında biçimsel çıkarım yapmayı mümkün kılmaktadır. Duyurulur.

9. Biçimsel bildirişim yapmaya muktedir olan m değişkeni, $Kip[n]$, $n \geq 2$, $n \in N$, BMD tanım bölgesinden tanımlı olan; $ü[m, n]$ sayıda F ve X formatlı BMT fonksiyonlarının küme kapanışları bulunmuştur. Bu küme kapanışları içeriğinde yer alan, sonsuz sayıda biçimsel mantık fonksiyonun çoğunun, yaklaşık %99'unun, anlamı ve kullanımı bugün henüz bilinmemektedir. BM bu fonksiyonları algılar, ifade eder, yeniden yapılandırır, anlamını bulduklarını duyurur ve doğru mantık çıkarımı yapan algoritmalarda kullanır.

10. BM, bir amaca en uygun bildirişim yaparak bilgiden bilgi üreten doğal algoritmaları algılar. Bildirişim yapmaya muktedir yeni TTBBS veya BBBSS Q bellekli BTN tasarımlarını yine TTBBS veya BBBSS Q bellekli BTN tasarımlarından yenidenlikli ifadeler kullanarak üretir, yeniden yapılandırır, anlamlandırır ve kullanır. Bu yenidenlikli tasarım süreci içinde elde edilen TTBBS veya BBBSS Q bellekli BTN tasarımlarına kısaca Q-FÜ bellek tasarımları denir. TASIM algoritması kavramını çok durumlu ve çok sayıda tik bellekli soyut makine tasarımlarını gerçekleştiren yazılım veya donanım üreten Q bellekli BTN oluşumları olarak kabul eder. Onları kolayca kodlayan $T = TASIM$ dili benzeri BD tasarımlar, programlar ve çok durumlu makine oluşumları olarak kullanır.

11. BM, en iyi biçimde bildirişim yaparak bilgi işleyen TTBBS veya BBBSS Q bellekli BTN üreten TASIM algoritmalarını iyi algılar. Yaşantımıza girerek bildirişim yapmaya muktedir olan her sonlu sayıda TTBBS veya BBBSS Q bellekli BTN tasarımını akıllı davranış gösterebilen yeni TTBBS veya BBBSS Q bellekli BTN tasarımlarına yenidenlikli algoritmalar kullanarak dönüştürür, yeniden yapılandırır, anlamlandırır ve kullanır.

12. BM, TASIM algoritmalarının çok durumlu bildirişim yaparak bilgi işleyen soyut makine tasarımlarını gerçekleştiren yazılım veya donanım türünde RCR formatlı TTBBS veya BBBSS Q bellekli BTN tasarımları olduğunu bilir. Bu tasarımları farklı görünümde oluşturmak için $T = TASIM$ benzeri biçimsel dilleri bulur, tasarımlar, gerçekleştirir ve kullanır.



13. Pratik kullanıma sahip olan iyi örgütlenmiş TASIM algoritmaları ile üretilen m değişkenli $Kip[n]$, $n \in N - \{0, 1\}$, değerli F ve X formatlı MTF tasarımları BM içeriğinin çok önemli konusudur. Genelde m değişkenli farklı $Kip[n]$, $n \in N$, mantık değeri kullanan BMT çıkarımlarının kısa sürede yapılmasına izin verir. Bulunan Q bellekli BTN tasarımları F , X ve S formatlaması ile çok önemli yeni özelliklere sahip fonksiyonlar üretmiştir. Çünkü özel biçimde programlanmış bildirişim yapmaya muktedir olan m -değişkenli ve çok farklı $Kip[n]$, $n \in N$, değerli Q bellekli BTN tasarımları içeriğinde yer alan her F , X ve S formatlı tik Q belleği bir doğal bulut gibi genişleme-büzülme özelliğine sahiptir. Çok değişik biçimde programlanabilmektedir. Böylelikle, bildirişim yapmaya muktedir olan m -değişkenli n -değerli F , X ve S formatlı BMF oluşumlarının F^+ formatlı küme kapanışları kolayca gerçekleştirilebilmektedir. Bu nedenle, çok değişik $Q = Q@Q$ bellekli $I = I@I$ formatlı BTN modelini algılar, ifade eder, tasarımlar, gerçekleştirir ve kullanır. Çok farklı F^+ formatlı $I@I$ internet modeli geliştirilmiştir.

14. BM, tam olarak $u[m, n]$ sayısı ile belirlenen bir sayıda m değişkenli $Kip[n]$, $n \in N$, değerli biçimsel bildirişim yaparak değer üreten; F formatlı Q belleğine programlanmış olan biçimsel mantık fonksiyonlarının var olduğunu bilir. Onları $Kip[n]$, $n \in N$, kuantumları ile m değişkenli n değerli Q bellekli BTN tasarımlarına programlamayı anında hemen yapar. İleri teknoloji üretme yeteneği olan yeni kuşağa öğretir.

15. BM dünyada, güneş sisteminde, yıldızlarda, galaksilerde ve evrende bulunan bildirişimli TTBBS veya BBBSS Q bellekli BTN tasarımlarının; yapısını, anlamını ve kullanımını iyi algılar. Onların kolay biçimde biçimsel anlatımını gündeme getirir, çalışır, araştırır, bulur, öğrenir ve öğretir.

16. BM matematiksel evrende, m -değişkenli ve $Kip[n]$, $n \in N$, değerli bildirişim yaparak bilgi işleyen F ve X formatlı Q belleği üretmeyi iyi bilir. Onların oluşturduğu her F^+ formatlı BMF küme kapanışını iyi algılar. Oluşturulan $F \in F^+$ ışığında en iyi biçimde bildirişim yapabilen; cebirsel, topolojik ve geometrik yapıların çalışmasını destekler. Ayırık matematikte kolay algılamayı mümkün kılan yeni yöntemleri algılar, çalışır, ifade eder, tasarımlar, gerçekleştirir ve kullanır.

III. ÖNEMLİ YAZAR BULGULARI

1. Çok basit biçimsel dilbilimi olan, $T = TASIM$ biçimsel dilini tasarlamış ve bildirişim yapan TTBBS veya BBBSS Q bellekli BTN tasarımında kullanmıştır.

2. $T = TASIM$ BD içeriğini kullanarak, $Kip[n]$, $n \in N$, kuantum değerlerine duyarlı olan genişleme-büzülme özelliğine sahip programlanabilir F , X ve S formatlı TTBBS

veya BBBSS Q bellek dağılımı ile donatılmış BTN tasarımları yapmıştır.

3. T dilini kullanarak F , X ve S formatlı genişleme-büzülme özelliğine sahip olan TTBBS veya BBBSS formatlı Q belleklerini kullanan; F formatlı TTBBS veya BBBSS Q belleği olan BTN tasarımlarını üretmiştir. F formatlı TTBBS veya BBBSS Q bellek içeriğinde biçimsel bildirişim kurma, sürdürme ve kullanıma sunma yöntemlerini çalışmıştır, yapılandırmıştır, anlamlandırmıştır ve kullanıma sunmuştur.

4. Her $u[m, n]$ sayısında, m değişkenli ve $Kip[n]$, $n \in N$, değerli mantık fonksiyonunun nasıl tasarımlanacağını göstermiştir. Bu fonksiyonlardan her biri n farklı bildirişim pin kodu(veya e-kimliği) kullanmaya muktedir tamra ve ramta antenlerini kullanarak, kendi iç dinamik yapısı içinde bildirişim yaparak, kendi sonuç mantık fonksiyonu değerlerini bulmaktadır. Sözü edilen $Kip[n]$ tabanlı e-kimliklerini kullanan TTBBS veya BBBSS Q bellekli BTN tasarımları bulunmuştur ve yayınlanmıştır.

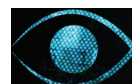
5. Gündüzleri güneş, geceleri ay ve yıldız ışınları doğayı aydınlatırken, görünmeyen BTN oluşumlarını insan gözüne görünür kılmaktadırlar. Ay ışığının olmadığı gecelerde evrenin değişik katmanlarından biri olan, Saman Yolu gök adasında yer alan yıldızlarından dünyanın bu coğrafyasına mevcut olan YÇK ve BÇK kuralları altında yoğun olarak bilgi taşındığı düşünülmüştür, gözlenmiştir ve görülmüştür. Yani TTBBS veya BBBSS Q bellekli BTN tasarımlarının olduğu gerçektir.

6. Gökyüzünde gördüğümüz her yıldız sonlu sayıda TTBBS veya BBBSS Q bellekli BTN tasarımıdır. Yani açık ve net olarak bir BD içeriğinde bir BG ile üretilen bir kelimedir. Işık yayarak bizimle bildirişim kurma çabasıdır. Bildirişim kurarken hangi $Kip[n]$, $n \in N$, BMD kuantumlarına bağımlı FÜ-mantığını kullandıkları ve bu mantığı üreten hangi bellek yapısına sahip oldukları biçimsel olarak bir en üst kimlik tarafından kesinlikle bilinmektedir. Yaratıcı olan odur.

7. YÇK ve BÇK kanunun algılanmasında geçerli olan aksiyomlar vardır. Bu aksiyomlar çalışılmıştır. Bulunmuştur. Yayınlanacaktır.

8. Basit ve karmaşık yapıda tasarlanmış yenidenlikli alt TASIM algoritmalarını kullanarak TTBBS veya BBBSS Q bellekli BTN formatlı Q bellekli algoritmaları yutan ve yeni TTBBS veya BBBSS Q bellekli BTN yapısında yeni TASIM algoritmaları bulunmuştur. $Kip[n]$, $n \in N$, kuantumları ile programlanmıştır. Düşünülmesi mümkün olan her m değişkenli ve her $Kip[n]$, $n \in N$, değerli mantık fonksiyonun tasarımı CITALOG içeriğinde en iyi biçimde gerçekleştirilmiştir. Bu, içinde bulunduğumuz yüzyılda, bulunan çok yeni ve oldukça önemli olan bir yeni buluş haberidir. Duyurulur.

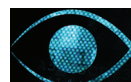
9. Her m değişkenli ve n değerli mantık fonksiyonu tasarımının nasıl yapılacağı sorunu yazar tarafından kesin



olarak çözülmüştür. Özellikleri çalışılmıştır. BM içeriğine konulmuştur. Duyurulur.

KAYNAKLAR

- [1] F. Ünlü: Kuramsal λ -Tasımlaması, *Atatürk Üniversitesi Basımevi*, Erzurum, 1976.
- [2] F. Ünlü: A TASIM Logic Realization of Boolean Algebra, *DIRASAT: A Research Journal, the University of Jordan, VIII (7): pp67-76, Amman, 1986.*
- [3] F. Ünlü: CITALOG: Compact and Integrated Tasim Logic Closure, *Journal of King Abdulaziz University, Science, Vol. 2, pp 117-136, Jeddah, KSA, 1990.*
- [4] F. Ünlü: A Remote Programming Technology on a Remote VDM Clustering in λ -Calculus, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 - 685, 2006 .*
- [5] F. Ünlü: Plemvanel: A Communicating Commuting Mathematics Generator Type, *International Mathematical Form, Vol. 1, No. 13-16, pp 671 – 685, 2006 .*
- [6] F. Ünlü: T-genetic RCR-U Form, *INISTA 2010, ID 16, pp 1-5, Kayseri, Turkey, 2010.*
- [7] F. Ünlü: Biçimsel TASIM Dilbilimi, *AYSU 2010, ID 5, pp 1-5, Kayseri, 2010.*
- [8] F. Ünlü: Q ve Q^+ Sürü Bellekli I@I İnternet Modeli Tasarımında Kullanılan T Genetik Altyapı Elamanları, *XVI. Türkiye'de İnternet Konferansı. Bildiri No. 3, 30 Kasım-2 Aralık 2011, E. Üniversitesi, İzmir.*
- [9] F. Ünlü: Bildirişimli Matematğin $\langle T \langle x \rangle, 1, n \rangle$ Q Sürü Bellekli 3D I@I İnternet Sürüsü. *XVI. Türkiye'de İnternet Konferansı. Bildiri No. 4, 30 Kasım -2 Aralık 2011, Ege Üniversitesi, İzmir.*
- [10] F. Ünlü: Güvenli Q Sürü Bellek Yazılım Yongası Üreten Dilbilim Örneği, 5. Uluslar arası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18 Mayıs 2012, ODTÜ Kültür ve Kongre Merkezi, Ankara.
- [11] F. Ünlü: Cycle Counting For Information Security in I@I Swarm İnternet Generating Q Swarm Memory, 5th International Conference on Information Security & Cryptology, MRTU Culture and Congress Center, Ankara, Turkey.
- [12] P. Linz, *Introduction to Formal Languages and Automata*, Fourth Edition, Jones and Bartlett Publishers, London, 2006.



Ulusal ve Uluslararası Yönetmeliklerde Kişisel Sağlık Verisi Mahremiyetinin Korunması

E. Olca ve Ö. Can

Özet— Bilgisayar ve internet kullanımı; hayatı kolaylaştırma, verimliliği artırma ve maliyetleri düşürme gibi katma değerlerle birlikte günlük hayatın en önemli parçalarından biri olmuştur. Ancak, bilgi sistemlerinde yer alan verilerin hangi amaçlarla, hangi durumlarda ve nasıl kullanılacakları konusunda yeterli kontrollerin ve yaptırımların bulunmaması, kişinin kendi verisi üzerindeki erişimleri kontrol edebilmesini zorlaştırmakta ve kişisel mahremiyetini korumasına yönelik endişelerin ortaya çıkmasına neden olmaktadır. Teknolojinin hızla gelişmesi ve bunun sonucunda meydana gelen elektronik dönüşümler çerçevesinde, kişisel sağlık bilgilerinin dijital ortama geçirilmesi kişisel haklar yönünden ciddi riskler ortaya çıkarmaktadır. Bu dönüşümle birlikte, e-sağlık alanında oluşan riskleri yönetmek, kişisel verilerin gizliliğini ve güvenliğini sağlamak için ulusal ve uluslararası alanlarda standartlar belirlenmesine ve yasal düzenlemeler yapılmasına başlanmıştır. Bu çalışmada; mahremiyeti korunması gereken bir e-varlık şeklini alan kişisel veri, kişisel sağlık verisi ve dijital ortamda tutulan Elektronik Sağlık Kaydı (ESK) olarak incelenmekte, bu e-varlıkların mahremiyetinin korunması için oluşturulan yönetmelikler ve standartlar bazında yapılan çalışmalar anlatılmaktadır.

Anahtar Kelimeler—Elektronik sağlık kaydı, kişisel veri, mahremiyet, veri güvenliği.

Abstract— Computers and internet usage have become one of the most important parts of daily life with the added values such as making life easier, increasing productivity and reducing costs. However, the absence of sufficient control and sanctions over the purposes, situations and ways of data usage in the information systems makes it difficult for a person to control access on her/his own data, and causes concerns to emerge about personal privacy. As a result of the rapid technological development and the electronic transformation it brings with, transition of personal health information to the digital environment poses serious risks in terms of personal rights. In order to manage risks in e-health domain and to secure privacy and security of personal data, new attempts have emerged to set standards and legal regulations both in national and international fields. In this study; personal data which has become an e-entity whose privacy needs to be protected, is analyzed as personal health data and Electronic Health Record (EHR) in digital platform, and the study also reviews studies carried out in the form of regulations and standards to protect the privacy e-entity.

Manuscript received July 19, 2004.

Emre Olca, İzmir Üniversitesi Mühendislik Fakültesi Yazılım Mühendisliği Bölümü, 35350, Üçkuyular, İzmir, Türkiye (İlgili yazar telefon: +90-232-4464949; faks: +90-232-2240909; e-posta: emre.olca@izmir.edu.tr).

Özgü Can, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (e-posta: ozgu.can@ege.edu.tr).

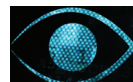
Index Terms—Electronic health record, personal data, privacy, data security.

I. GİRİŞ

Teknolojinin hızla gelişmesi sonucunda, e-sağlık sistemlerinde yer alan hasta ve tedavi verileri, kayıtların elektronikleşme süreci içerisinde dijital ortama taşınmıştır. Bu taşınma öncesinde, hasta ve tedavi verilerinin saklanması için o dönemin teknolojik imkânları kullanılırken, sağlık verilerinin düzgün alınması, düzenli saklanması, gerektiğinde hızlı bir şekilde erişilmesi, paylaşılması ve arşivlenmesi konularında ciddi sıkıntılar yaşanmıştır. Elektronik ortama geçiş ile bu sıkıntılar aşılmış, istenildiği zaman ve yerden ulaşılabilir bir hale gelmiştir. Fakat bu erişim kolaylığının yanında veri güvenliği riskleri, veri istismarları ve ekonomik tehditler ortaya çıkmıştır. Bu tehditlerin en önemlilerinden birisi, kişiler üzerinde maddi ve manevi büyük zararlara yol açabilecek kişisel sağlık veri mahremiyetinin ihlal edilmesidir. Elektronik sağlık kayıtları, sağlık alanında yer alan bütün kullanıcılar için önemli avantajlar sağlamış olmasına rağmen, teknolojinin kötü amaçlı kullanımı sonucu verilerin gizliliği ve güvenliği konusunda ciddi sıkıntıların ortaya çıkmasına neden olmaktadır.

Sağlık verisi üzerinde oluşan risklerin sonucu olarak, yasal düzenlemeler yapılmaktadır. Ulusal bilgi güvenliği açısından tehlike yaratabilecek bu riskler için, kanunlarla ve uluslararası yönetmeliklerle yapılan düzenlemeler uygulanmalıdır. Yapılan tüm düzenlemelere rağmen, kişinin kendi haklarının farkında olması ve mahremiyetinin korunması için yasal mevzuatlar doğrultusunda işlem yapıldığından emin olması gerekmektedir. Çünkü bilgi güvenliğinin en zayıf halkası tehdide doğrudan veya dolaylı olarak maruz kalan eğitimsiz ya da bilinç eksikliği olan bireylerdir. Bu nedenle kişi, sağlık sistemindeki bir aktör olarak, kişisel verisinin mahremiyetini ve güvenlik önlemlerini tamamen diğer paydaşlara bırakmamalı ve sürecin yönetmelikler doğrultusunda ilerlediğinin takibini yapabilmelidir.

Bu çalışmada; kişisel veriler, kişisel sağlık verileri ve bunların kanunlarla ve uluslararası yönetmeliklerle yapılan düzenlemelerinden bahsedilmekte, e-sağlık dâhilinde kişisel sağlık verileri için gizlilik ve güvenlik kavramlarının önemine değinilmektedir. Sağlık etki alanında, potansiyel mahremiyet riskleri ve mahremiyetin hasta hakları açısından önemi anlatılmaktadır. Bu çalışmanın organizasyonu aşağıdaki şekilde düzenlenmiştir: İkinci bölümde kişisel veri ve kişisel sağlık verisi kavramları açıklanmakta ve hukuki zeminleri



ULUSAL VE ULUSLARARASI YÖNETMELİKLERDE KİŞİSEL SAĞLIK VERİSİ MAHREMİYETİNİN KORUNMASI

aktarılmaktadır. Üçüncü bölümde, genel bir değerlendirme yapılmakta ve dördüncü bölümde sonuç yer almaktadır.

II. KİŞİSEL VERİ VE YÖNETMELİKLER

Veriden ya da bu verinin ilgili olduğu diğer veriler ile birleştirilmesi sonucunda oluşan veri kümesinden, veri sahibinin kimliği elde edilebiliyorsa bu veri kişisel veridir. Örneğin, bir veri tabanında yer alan kullanıcı isimleri ve adresleri kişisel verilerdir. 1995 yılında yayınlanmış olan 95/46/EC numaralı Avrupa Birliği direktifi [1], kişisel veri tanımını, kim olduğu belli veya belirlenebilen bir gerçek kişiye ait tüm bilgilerdir şeklinde ifade etmektedir. Bu direktife göre, kimliği belirlenebilir gerçek kişi; “Özellikle bir kimlik numarası referans alınarak doğrudan ya da dolaylı belirlenebilen ya da fiziksel, psikolojik, akli, ekonomik, kültürel veya sosyal kimliğine özgü bir veya birden çok faktörle tanımlanabilen kişidir”. Bu tek bir bilgi olabileceği gibi, birbiriyle ilişkili çok sayıda bilgi de olabilmektedir. Kişinin adı, adresi, kimlik numarası, doğum tarihi, banka hesap numarası, kredi kartı numarası, parmak izi, IP adresi, sağlık raporları, kişisel veri örnekleridir. Anayasanın 20. Maddesi “Özel Hayatın Gizliliği” [2] başlığı altında yer alan “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz” ifadesiyle kişisel veriler bir hak olarak tanımlanmakta ve koruma altına alınmaktadır. Avrupa İnsan Hakları Sözleşmesinde, kişisel veri tanımı için açık bir ifade bulunmamaktadır. Ancak, “özel ve aile hayatına saygı hakkı” başlıklı 8. maddesinin 1. fıkrasına göre; “Herkes, özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir” hükmünde geçen “özel hayata saygı hakkı” kişisel verileri de kapsamaktadır [3]. Kişisel Verilerin Korunması Kanun Tasarısı’nda [4], kişisel veri tanımının içine tüzel kişiler de dâhil edilmekte ve kişisel veri “Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bilgilerin tamamı” olarak tanımlanmaktadır. 108 Numaralı Avrupa Konseyi Sözleşmesinde [5] ise; “Kişisel veri, kimliği belirtilen ya da belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder” şeklinde bir tanım yer almaktadır. Ekonomik Kalkınma ve İşbirliği Örgütü (The Organisation for Economic Co-operation and Development, OECD)’nin Rehber İlkelerinde [6] ise “Belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler” olarak bir tanım bulunmaktadır.

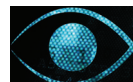
A. Kişisel Veri, Erişimi, Kullanımı ve Korunması

Amerika ve birçok gelişmiş Avrupa ülkesinde, elektronik ortama ve bilgisayar kullanımına ülkemizden daha önce geçilmiş olması nedeniyle, son çeyrek yüzyılda kişisel verilerin güvenliğine ilişkin tehlikelerin farkına varılmış ve bu alanda ülke mevzuatlarında çeşitli düzenlemeler yapılmıştır. Katı yaptırımları olan gizlilik düzenlemeleri nedeniyle, kişisel bilgiler kritik kurumsal veriler arasında en önemli bilgiler olarak kabul edilir bir duruma gelmiştir. Bu nedenle, kişisel verilere sahip olan kurumlar, bu verilerin erişimi ve kullanımı için kritik kurumsal verilerinin güvenliğine ilişkin bir program yürütmektedirler [7].

Yine kişisel verinin erişimi ve kullanımı için, Türkiye Cumhuriyeti Anayasasının 20. Maddesinde [2] özel hayatın

gizliliğinin dokunulamaz olduğu belirtilmekte ve kişisel veriye erişim için “Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar” tanımı yapılmaktadır. Sonradan eklenen ek fıkra ile de “kişinin açık rızası” terimi kullanılmakta, kişisel verinin ancak kanunda öngörülen durumlarda ve/veya kişinin açık izniyle erişilip işlenebileceği vurgulanmaktadır. Kişisel verinin korunması kapsamında, 2010 yılında yapılan bir düzenleme ile 20. Maddeye ek bir fıkra eklenmiştir. Bu ek fıkra [2], “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” ifadesi yer almaktadır. Bu fıkra, hüküm açık bir şekilde ifade edilmekte, kişisel verilerin ancak kanunla öngörülen durumlar ve kanuna dayalı düzenlemelerle işlenebileceği vurgulanmakta ve kişisel verilerin korunması öngörülmektedir. Ayrıca, bu maddede, kişisel verilerin ancak kişinin açık izni ile işlenebileceği, kişisel verilerin nasıl korunacağına dair esas ve usullerin kanunla düzenleneceği ifade edilmekte [8] ve kişisel verilerin mahremiyeti ve korunması hakkının varlığı tanınmaktadır.

Avrupa İnsan Hakları Sözleşmesinin 8. maddesinin 2. fıkrasında, kişisel veriye erişim hakkı için “Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlâkın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir” tanımı yapılmakta, ayrıca kişisel veri gizliliğinin ve güvenliğinin nasıl uygulanabileceği ifade edilmektedir [3]. 8. maddenin ihlal edilmesi ve yasal yaptırımlar ile ilgili de çeşitli adli örnekler mevcuttur. Avrupa İnsan Hakları Mahkemesi’nin 02.12.2008 tarih ve 2872/02 başvuru numaralı K.U. v. FİNLANDİYA davasında [9], 12 yaşında bir erkek çocuğu adına yayınlanan bir ilanda; çocuğun yaşı ve fiziksel özellikleri belirtilerek “kendisine yol gösterecek” kendi yaşında veya daha büyük bir erkekle yakın ilişki kurmak istediği ifadelerine yer verilmiştir. İnternet servisi sağlayıcısının bu reklamı veren kişinin kimliğini gizlilik kurallarını ihlal edeceği gerekçesiyle açıklamayı reddetmiştir. Finlandiya mahkemeleri de servisi sağlayıcının yasal olarak söz konusu bilgiyi açıklamaya mecbur olmadığı hükmüne varmışlardır. Bunun üzerine, Avrupa İnsan Hakları Mahkemesi bunun ceza gerektiren bir eylem olduğuna ve



ULUSAL VE ULUSLARARASI YÖNETMELİKLERDE KİŞİSEL SAĞLIK VERİSİ MAHREMİYETİNİN KORUNMASI

Avrupa İnsan Hakları Sözleşmesinin 8. maddesinin ihlal edildiğine karar vermiştir [10]. 25.02.1997 tarih ve 22009/93 başvuru numaralı Z v. FİNLANDIYA davasında [11], bir ceza davası kapsamında kişinin HIV durumunu da içeren tıbbî bilgilerin açıklanmasından dolayı özel hayatına saygı gösterilmesi hakkının ihlal edildiği gerekçesiyle açılan davada, mahkeme ilgili kişinin tıbbî kayıtlarının ifşasının, Avrupa İnsan Hakları Sözleşmesi 8. madde 2. fıkra kapsamında gerekli olduğuna karar vermiştir. Ancak mahkeme, temyiz mahkemesi kararında kişinin adının ve HIV statüsünün açıklanmasının herhangi bir meşru amaç için gerekli olmadığına ve özel hayata saygı hakkının ihlal edildiğine karar vermiştir. Çünkü kişinin yaşadığı sağlık problemleri, doktoru ile arasındaki ilişkisi, teşhis, tedavi ve tetkik bilgileri, verilen ilaçlar ve görüntüleme sonuçları tümüyle özel hayatının gizliliği ve korunması hakkı kapsamına girmektedir. 27.08.1997 tarihli M.S. v. İSVEÇ davasında ise [12], başvurana ait kürtaj hakkında bilgileri de içeren tıbbî verilerin, tedavi gördüğü sağlık kurumu tarafından sosyal güvenlik kurumuna verilmesinin Avrupa İnsan Hakları Sözleşmesinin 8. maddesini ihlal ettiği iddiası değerlendirilmiştir. Bu davada, diğer dava sonuçlarının aksine, sosyal güvenlik kurumunun ilgili sağlık kurumundan bilgileri isteme yükümlülüğünün kanun dâhilinde olduğuna ve Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edilmediğine karar vermiştir. Avrupa Birliği Direktifi 2b maddesinde ise [13], verinin işlenmesi çok geniş bir şekilde tanımlanmaktadır. Buna göre verinin işlenmesi; verinin toplanması, kaydedilmesi, organizasyonu, depolanması, değiştirilmesi, geri alınması, kullanımı, iletimi, yayma veya yayını ve hatta engellenmesi, silinmesi veya imhası dâhil olmak üzere kişisel veriler üzerinde manüel veya otomatik müdahaleyi kapsamaktadır.

Kişisel verilerin korunması konusu, gerçek anlamda ilk defa 1980 yılında Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından ele alınmaktadır. Burada kabul edilen ilkeler diğer çalışmalara da rehber niteliğinde olmuştur. Bu çalışmaya göre, kişisel veri toplanması ve işlenmesi ilkesinde, kişisel veri kullanımının sınırları olması gerektiği belirtilmekte ve yine kişisel verilerin yasal mevzuatlara uygun, meşru yollarla ve mümkün olduğunca bireyin bilgisi veya izni dâhilinde elde edilmesi gerektiği vurgulanmaktadır [14]. 5237 sayılı Türk Ceza Kanunu, kişisel verilerin korunmasına yönelik suçları düzenleyen 134., 135., 136., 137. ve 138. maddelerinde manüel olarak yapılan veri işleme faaliyetleri de suç kapsamına alınmaktadır [15]. Türk Ceza Kanunu 138. maddesinde, kişisel verilerin korunmasında temel ilkeler arasında bulunan “süre sınırı” karşılanmaktadır [15]. Bununla birlikte, Türk Medeni Kanunu’nda “Kişilik Haklarının Korunması”nı düzenleyen 23. ve 24. maddeleri uyarınca da, kişisel veriler koruma altına alınmaktadır [16]. Avrupa Birliği Temel Haklar Şartı’nın 8. maddesinde kişisel verilerin korunması başlığı altında “Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzeltirme hakkına sahiptir. Bu kurallara uyulması,

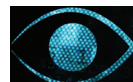
bağımsız bir makam tarafından denetlenir” ifadesi bulunmaktadır [17].

Kişisel verilerin korunmasına yönelik dünyada yapılan çalışmaların tarihsel sürecine bakıldığında, 1970 yılında Almanya’da *Verilerin Korunması Kanunu* çıkarılmış [18], 1970 yılının sonunda Lüksemburg’da kişisel verilerin korunmasına yönelik bir düzenleme yapılmıştır. 1973 yılında İsveç’te verilerin korunmasına ilişkin kanun çıkartılmış, 1974’te Amerika’da özel alanın korunmasına ilişkin kanun kabul edilmiştir. Bu kanunlara ek olarak, 1977 yılında Kanada’da *İnsan Hakları Kanunu* ve 1978 yılında Fransa’da *Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına* ilişkin kanun çıkarılmıştır. Aynı süreçte; İsviçre, Danimarka ve Norveç’te de verilerin korunmasına ilişkin yasal düzenlemeler yapılmıştır [19]. 1980 yılında OECD tarafından kişisel veri toplanması ve işlenmesi [6] ile ilgili sözleşme kabul edilmiş, 1981 yılında da Avrupa Konseyi, verilerin korunmasına yönelik olan 108 numaralı sözleşmeyi [20] kabul etmiştir. Bu sözleşmeler birçok sözleşmeye rehber olmuş, birçok yeniden gözden geçirilmiştir. Avrupa Birliği; AB 95/46/EC numaralı direktifi, 108 Numaralı Sözleşme, OECD Rehber ilkeleri gibi çalışmalar ile kişisel verilerin mahremiyetinin korunması alanında temel alınacak çeşitli çalışmalar ortaya çıkarmıştır [21].

B. Kişisel Sağlık Verisi, Erişimi, Kullanımı ve Korunması

Kişisel sağlık verisi kavramı, kişisel veri kavramı içinde yer almaktadır. Tedavinin sürekliliğinin sağlanmasında önemli bir payı olan kişisel sağlık verisi, toplum sağlığına da önemli katkılarda bulunmaktadır. Ayrıca, bilimsel araştırmalara kaynak olmakta ve hukuki durumlar için belge niteliği taşımaktadır. Kabul edilen kanunlar, mevzuatlar, sözleşmeler dâhilinde kişinin, kişisel sağlık verileri ile ilgili hakları; özel yaşama ve aile yaşamına saygı hakkı, sağlık hizmetinden faydalanma hakkı, yaşam hakkı, ifade özgürlüğü, düşünce vicdan ve din özgürlüğü, adil yargılanma hakkı, hakların kötüye kullanılmasının yasaklanması hakkı, hakların kısıtlanmasının sınırlandırılması hakkı, özgürlük ve güvenlik hakkı ile doğrudan bağlantılıdır [22].

Kişisel sağlık verisinin sahibi durumundaki hastanın hakları, uluslararası alanda ilk olarak 1981 yılında Lizbon’da imzalanan Dünya Hekimler Birliği (DHB) Hasta Hakları Bildirgesinde ele alınmıştır. Bu bildiğe, 1995’te Bali’de yenilenmiş, son olarak ta 2005 Santiago Bildirgesi’yle geliştirilmiştir. Washington’da 2002 yılında yapılan Dünya Hekimler Birliği (DHB) [23] Genel Kurulu’nda kabul edilen bildirgede kişisel sağlık bilgileri; “*Kişinin bedensel ya da zihinsel sağlığına ilişkin kayıt edilmiş tüm bilgilerdir*” olarak tanımlanmaktadır. Kişisel veri olarak, kişinin kimlik ve sağlık bilgileri yanı sıra hücre, uzuv, kan ve DNA gibi bilgileri de önemlidir. Kasım 2002 tarihli Avrupa Birliği Hasta Haklarına İlişkin Avrupa Statüsü Ana Sözleşmesi Temel Dokümanı 6. Maddesinde [24] “*Özel ve Gizlilik Hakkı*” başlığı altında; “*Her birey kişisel bilgilerinin; sağlık durumu, yapılan teşhis ve tedavi konularında bilginin yanı sıra teşhis ve tedavi yapılırken veya özel ziyaretlerinin gizliliğinin muhafazası hususunda, gizli tutulmasını talep etme hakkına sahiptir*” tanımı yer almaktadır.



ULUSAL VE ULUSLARARASI YÖNETMELİKLERDE KİŞİSEL SAĞLIK VERİSİ MAHREMİYETİNİN KORUNMASI

Türkiye Cumhuriyeti Sağlık Bakanlığı Hasta Hakları Yönetmeliği “Mahremiyete Saygı Gösterilmesi” başlıklı Madde 21’e bakıldığında [25], kişisel sağlık bilgileri ile ilgili olarak: “Hastanın, mahremiyetine saygı gösterilmesi esastır. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir. Mahremiyete saygı gösterilmesi ve bunu isteme hakkı;

- 1) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,
- 2) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini kapsar” tanımı yer almaktadır.

Sağlık Bakanlığı tarafından hazırlanan, kamuoyunun bilgisine ve görüşüne sunulan “Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı [26]”nın amacı; kişisel sağlık verilerinin kayıt altına alınabilmesi, veri mahremiyetinin sağlanması, işlenmesi ve işleyecek gerçek ve tüzel kişilerin uyacakları esas ve usulleri belirlemektir. Ancak, Sağlık Bakanlığı’nın kişisel sağlık verilerini hangi şartlarda tutacağı belirtilmemiştir. Bu taslak kapsamında, Sağlık Bakanlığı en büyük veri toplayan kurum olarak görülmektedir. Bu durumda, kişisel sağlık verilerinin gereğinden uzun saklanması önüne geçmek ve suiistimalleri önlemek için gerekli düzenlemelerin yapılması ve sınırların belirlenmesi gerekmektedir.

Bilgi güvenliği konusunda ki diğer bir önemli çalışma olan ISO 27000 ailesi, oldukça kapsamlı süreçleri içermektedir [27]. ISO/IEC 27001:2005, *Bilgi Güvenliği Yönetim Sistemi* için özellikleri belirlerken ISO/IEC 27002:2005 *Bilgi Güvenliği Yönetimi* için uygulama kodu niteliğindedir. ISO 27799:2008 standardı ise, sağlık bilişimi için bir standarttır. Sağlık sektöründe bilgi güvenliği yönetiminin gerçekleştirilmesinde ISO/IEC 27002 kullanılarak düzenlenmeler gerçekleştirilmektedir [28].

Amerika Birleşik Devletleri’nde sağlık sektöründeki bilgi ve bilgi akışının güvenliğini oluşturmak ve devamlılığını sağlamak için 1996 yılında kabul edilen ve uygulanmaya başlanan HIPAA’ya (Health Insurance Portability and Accountability Act) göre sağlık bilgisi, sağlık hizmeti servisleri, halk sağlığı otoriteleri, sigorta firmaları, sağlık hizmetinde bulunan profesyoneller tarafından üretilen ya da elde edilen ve hayatın tüm dönemi için fiziksel veya ruhsal sağlık ile ilişkili olan herhangi bir bilgidir [29]. Özetle; kişisel sağlık bilgileri, kişinin doğumundan ölümüne kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür.

Kişisel veriler açısından sağlık sektöründe uygulanan prensipler genel prensiplere paraleldir. Sağlık uzmanları için Sağlık Hizmetlerinde Mahremiyet ve Gizlilik Üzerine Avrupa Rehberi’nde (European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare) kişisel sağlık verileriyle ilgili olarak hastanın bilgilendirilmesi, rıza/onam alınması, seçim hakkı, hasta kimliğinin gizlenmesi ve anonimleştirme, bilgi açıklamasını gerektiren durumlar, güvenlik, erişim ve düzeltme maddeleri tanımlanmaktadır [30].

Kişisel sağlık verisi, kişinin tedavisinin sürekliliği için ne kadar gerekli ise, istatistiksel ve bilimsel amaçlar için de aynı derecede gereklidir. Bu doğrultuda sağlık verisine, veri

örneklerine ve laboratuvar sonuçlarına erişim isteği gerekliliği ve bu veriler üzerinde araştırma yapma ihtiyacı da her geçen gün artmaktadır. Kaynaklara erişim denetiminin gerçekleştirimi, kişisel hakların korunmasının sağlanmasında önemli ve gerekli bir denetimdir. Araştırma ve geliştirme için kullanılan veri kümeleri ne kadar fazla veri içerirse, elde edilen sonuçların geçerliliği ve genelleştirilmesi de etkili olacaktır. Bu nedenle, hasta verilerinde kişisel mahremiyetin korunması ve veri güvenliğinin sağlanması hakkı dâhilinde araştırmalar için kullanılacak sağlık verisinin kullanımının maksimizasyonu ile gizlilik ve güvenlik dengesinin kurulması önemlidir.

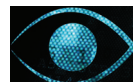
Türkiye’de tüm sağlık kurumları, tek bir çatı altında toplanmış olup, 2006 yılından itibaren Sosyal Güvenlik Kurumu (SGK) güvencesiyle hizmet alan kişilerin bilgileri elektronik ortamda (MEDULA) [31] tutulmaya başlanmıştır. 2012 yılı itibarıyla, e-reçete sistemine geçilmiş ve kişilerin ilaç bilgileri de saklanmaya başlanmıştır. SGK, anlaşmasız kurumlar/muayenehanelerden hasta verilerini almak için, ayrı bir sistem tasarlamıştır (Sağlık2NET) [32]. Bu sistem 2013 Ağustos’ta yasalaşmış ve uygulamaya alınmayı beklemektedir.

Türkiye’de sağlık hizmetinin özelleştirilmesine bağlı olarak Sosyal Güvenlik Kurumu’na MEDULA sistemi kapsamında gönderilen veriler incelendiğinde, özel sağlık sektörü de kişisel sağlık verilerine en az %35 oranında sahip bulunmaktadır [33]. Ulusal özel sağlık sektörünün uluslararası sermaye ile ortaklıklarının artması ve yönetimlerinin uluslararası sermaye lehine değişmesi sonucu, bu bilgiler tümü ile uluslararası sermayenin de kontrol ve kullanımına geçmiş bulunmaktadır.

Türkiye’de, kişilerin sağlık hakkıyla ilgili pek çok dava Avrupa İnsan Hakları Mahkemesine taşınmış ve Türkiye, kişinin yaşam hakkını korumak için gerekli sistemi oluşturamadığı gerekçesiyle mahkûm olmuştur [34]. Hasta haklarının korunması kapsamında kişisel sağlık verilerinin gizliliği ve güvenliğinin sağlanması ile hasta güveni ve memnuniyeti ile başlayan ve sonrasında sağlık kurumuna ulaşacak olan olumlu etki, ülke çıkarları bağlamında zaman tasarrufu ve ekonomik kazanımlar sağlayacaktır.

Kişisel sağlık verileri kapsamında olan kişinin sağlık durumuna ilişkin genel veriler, kişiye uygulanan tedaviye ilişkin veriler ve tedavi sonrasında kapsayan süreç için öngörülen durumlar gizli olmalı ve korunmalıdır. Sağlık Bakanlığının 2005 yılında yayınladığı “Veri Güvenliği Genelgesi” adlı genelgede [35] verilerin kullanımıyla ilgili “verilerin hastanın izni olmadan başka kurumlara/shahıslara verilmemesi” gibi esaslar getirilmiş ve bu esasların uygulanmasına yönelik olarak da “Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol tabanlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.” maddesiyle açıklama yapılmıştır. HIPAA güvenlik kurallarına göre [36]; kişisel sağlık bilgilerinin gizliliği, bütünlüğü ve erişilebilirliği garanti altına alınmalıdır. Bu nedenle, kişisel sağlık bilgilerinin bütünlüğünü tehdit edici ve/veya mahremiyetini tehlikeye sokacak her türlü izinsiz erişime karşı önlemler alınmalıdır.

Kişisel sağlık verileri açısından evrensel ilke her zaman kişinin hak ve özgürlüklerinin korunmasının ön planda



ULUSAL VE ULUSLARARASI YÖNETMELİKLERDE KİŞİSEL SAĞLIK VERİSİ MAHREMİYETİNİN KORUNMASI

olmasının gerektiğidir. Dünya standartlarında kişisel sağlık verileri, kişisel veri kategorisi içinde kritik ve özel niteliği olan veriler kategorisinde yer bulmaktadır.

III. DEĞERLENDİRME

E-dönüşüm sürecinde kritik önem taşıyan sağlık verilerinin dijital ortama taşınması ile hasta ve tedavi bilgileri kağıt tabanlı formattan çıkarak dünyanın her noktasından kolayca ulaşılabilir olmuş, elektronik sağlık kayıtları da tıp bilişimi alanında ön plana çıkan önemli konular arasına girmiştir. Dijital ortama geçiş ile birlikte kalite ve verimin artması, iş akışının otomatize olması, hasta tedavi ve bakımının iyileştirilmesi, acil durumlarda hasta bilgilerine hızlı ulaşım, daha iyi bir dokümantasyon, yasal bilgi ve belge oluşturmada kolaylık, sağlık hizmetinin daha iyi planlanabilmesini gibi birçok kazanım sağlanmıştır. Ancak, bu kazanımların karşısında da hasta mahremiyetinin ihlali ve kişilerin maddi, manevi ve sosyal yönden zarar görmesi, kişisel bilgilerin kişilerin haberi olmaksızın çeşitli ortamlarda ifşa edilebilmesi, sisteme güven duygusunda ki azalmaya bağlı hastanın bilgilerini saklaması ve tedavinin bu durumdan etkilenmesi, toplanan verilerin metalaştırılarak alınıp, satılabilir bir duruma gelmesi ve verilerin amaç dışı kullanımı gibi çok kritik riskler ortaya çıkmaktadır. Temel hak ve hürriyetlerin öneminin giderek arttığı ve kişilerin bilinçlendiği günümüzde de, kişisel bilgilerin gizliliği dâhilinde bu riskleri minimize etmek için ülke ve sağlık kurumları bazında ve uluslararası çapta tanımlar yapılmakta, standartlar belirlenmekte, çözümler önerilmektedir.

Bu tanımlamaların en başında, Sağlık Bilgi ve Yönetim Sistemleri Topluluğu (Healthcare Information and Management Systems Society, HIMSS) Elektronik Sağlık Kaydı (ESK) tanımını [37]: *“Hasta sağlık bilgilerinin herhangi bir sağlık kuruluşunda bir veya birden çok kuruluş tarafından oluşturulmuş boylamsal (dikey) elektronik kayıtlardır. Bu bilgiler kapsamında hastanın cinsiyeti, ilerleme notları, sorunları, tedavileri, yaşam belirtileri, geçmiş tıbbi bilgileri, bağışıklıkları, laboratuvar verileri ve radyoloji raporları girmektedir”* olarak vermektedir. Sağlık Bakanlığı tarafından duyurulan bir sertifikada [38], ESK’ nın dijital çağ ile birlikte yaşamımıza giren kavramlardan biri ve de en önemlisi olduğundan bahsedilmektedir.

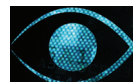
Her türlü kayıta olduğu gibi, elektronik sağlık kaydında da kişisel sağlık verilerinin gerçek sahibi kişidir. Kişinin sağlık hizmeti aldığı kurumlar açısından sağlık hizmetini veren kurum ya da kişi (hekim) olma durumu kişisel sağlık verilerinin üzerinde “sahip olma” hakkını oluşturmamaktadır. Sağlık hizmeti gerek kişinin doğrudan kendi ödemesi sonucu, gerekse de vergilendirme yöntemi ile almış olduğu bir hizmettir. Her iki durumda da kurumsal haklar kişisel hakların önüne geçmemelidir. Tüm sağlık kurumlarının ve ilgili personellerin kişisel hakları tanıma ve destekleme ve hatta kişilerin mahremiyetini sağlama konusunda sorumlulukları bulunmaktadır. Santiago’da 2005 yılında yapılan Dünya Hekimler Birliğinde ortaya çıkan Hasta Hakları Bildirgesinin

gizlilikle ilgili 8. Maddesi [39] “Hastanın sağlık durumu, tıbbi durumu, tanısı, hastalığın seyri ile ilgili tahmini, tedavisi ve kişiye özel diğer tüm bilgiler ölümünden sonra bile gizli olarak korunmalıdır” ifadesine yer vermektedir. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununa [40] göre, Sosyal Güvenlik Kurumu (SGK) MEDULA [31] sistemi ile hizmet alımı sonucu ödeme kapsamı dâhilindeki kişilerin kişisel sağlık bilgilerini elektronik ortamda kayıt altına almaktadır. Sağlık Bakanlığı kendine bağlı ya da denetiminde bulunan sağlık kurumlarından GEBLİZ, AşıNet, 15-49 Yaş Kadın İzlem gibi formlar ile hastaların sağlık verilerine ek olarak kişisel bilgileri de toplamaktadır. Kamu ve özel sağlık kuruluşlarından da SağlıkNET [32] kapsamında bilgiler bakanlığa gönderilmektedir. Tutulan tüm kişisel sağlık verileri, Sağlık Bakanlığı, SGK, hekimler, eczaneler, laboratuvarlar ve çalışanları, adli süreç kapsamında adli makamlar tarafından da kolaylıkla izlenebilmektedir. Veri miktarı hızlı bir şekilde artarken, veriye erişim imkânı da yoğun ve kolay bir şekilde gerçekleşmektedir. *Kişisel Verilerin Korunması Kanun Tasarısı* [4], halen kanunlaşmayı beklemektedir. Türkiye Cumhuriyeti hukuk sisteminde tek genel düzenleme Türkiye Cumhuriyeti Anayasası olup, Türk Ceza Kanunu ve Medeni Kanun ile de kişisel verilerin korunmasına aykırı davranışlara ilişkin genel hükümler belirtilmektedir. Günümüzde, genel olarak düzenlenen bir “Kişisel Verilerin Korunması Hakkında Kanun” mevcut değildir ve AB mevzuatına uyum içinde genel bir kanuni düzenlemeye acil olarak ihtiyaç duyulmaktadır.

IV. SONUÇ

Verilerin elektronikleşmesi sürecinin olumlu yanlarının yanında, olumsuzlukları da aynı derecede önem taşımaktadır. Sürecin hukuki bağlamda kurallara bağlanması, gizliliğinin ve güvenliğinin sağlanması ve kontrol edilebilmesi konusunda yönetmeliklerin oluşturulması ve teknolojik düzenlemelerin gerçekleştirilmesi ihtiyacı doğmaktadır. Ancak, yaşanan bazı olaylara ve alınan tüm tedbirlere rağmen olumsuzlukların tümüyle ortadan kalkmasının mümkün olmadığı tartışmaları da sürmektedir. Hukuk alanındaki gelişmeler ve düzenlemeler, bilim ve teknolojiye kadar hızlı olamamaktadır. Bu durum, elektronik ortamda tutulan kişisel sağlık verilerinin gizliliği, güvenliği, güvenilirliği, işlenmesi ve saklanması konularında çeşitli aksaklıkları beraberinde getirmektedir.

Türkiye Cumhuriyeti Sağlık Bakanlığı, hasta mahremiyeti konusunda MEDULA sistemi ile sağlık verisi toplayan diğer birçok sağlık kurumuna göre daha hassas davranmaktadır. Sağlık Bakanlığı tarafından, 2005 yılında yayınlanan Veri Güvenliği Genelgesi [41] son yıllarda detaylandırılarak güncellenmiştir. Hukuk ve tıp bilişimi alanlarında yürürlükte olan kanunlar ve Avrupa Birliği kriterleri ile birlikte yapılan çalışmalar sınırları belirlemekte, yasallaştırmakta ve pratiğe geçirilmesi için yönlendirmelerde bulunmaktadır. Teorik anlamda yapılan bu çalışmaların uygulamaya geçmesiyle birlikte bireylerin, kişisel verilerin gizliliği ve güvenliği konusunda bilinçlenip sistemi desteklemeleri bu sürece ivme kazandıracaktır.



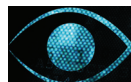
ULUSAL VE ULUSLARARASI YÖNETMELİKLERDE KİŞİSEL SAĞLIK VERİSİ MAHREMİYETİNİN KORUNMASI

KAYNAKLAR

- [1] Directive 95/46/EC of The European Parliament and of The Council, Available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF>
- [2] Türkiye Cumhuriyeti Anayasası, Available: http://global.tbmm.gov.tr/docs/constitution_en.pdf
- [3] Avrupa İnsan Hakları Sözleşmesi, Avrupa Antlaşmaları Serisi, no. 5, Available: http://www.echr.coe.int/Documents/Convention_2014_1_TUR.pdf
- [4] Kişisel Verilerin Korunması Hakkında Yasa Tasarısı md.3/ç., Available: <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>
- [5] Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 Numaralı Avrupa Konseyi Sözleşmesi, Available: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
- [6] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Available: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>
- [7] E. McCallister, T. Grance, and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", Recommendations of the National Institute of Standards and Technology, *NIST Special Publication 800-122*, April 2010.
- [8] Kişisel Sağlık Verilerinin Korunması Bir Haktır, Available: <http://www.ttb.org.tr/index.php/Haberler/ksv-4171.html>
- [9] AHİM, K.U. v. FINLANDIYA DAVASI (Başvuru no: 2872/02), Available: <http://hudoc.echr.coe.int/sites/eng/pages/search.%20aspx?i=001-89964>
- [10] Avrupa İnsan Hakları Mahkemesi, Küçüklerin Korunması, Available: http://www.inhak.adalet.gov.tr/tematik/cocuklar/kucuklerin_korunmasi.pdf
- [11] AHİM, Z v. FİNLANDIYA (Başvuru no. 22009/93), Available: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58033>
- [12] Protection of personal data, Available: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- [13] D. Elgesem, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data," *Ethics and Information Technology*, vol. 1, no. 4, pp. 283-293, 1999.
- [14] Sağlık Hizmetlerinde Kişisel Veri Toplanması Hakkında TPD Hasta Mahremiyeti Görev Grubu Raporu, Available: http://78.189.53.61/-/49UPK/Sunu/huseyin_soyal.pdf
- [15] 5237 sayılı Türk Ceza Kanunu md. 135 vd., Available: <http://www.tbmm.gov.tr/kanunlar/k5237.html>
- [16] Türk Medeni Kanunu, Available: <http://www.tbmm.gov.tr/kanunlar/k4721.html>
- [17] Avrupa Birliği Temel Haklar Şartı md. 8, Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf
- [18] M. D. Birnhack, "The EU Data Protection Directive: An Engine of a global regime", in *Elsevier Computer Law and Security Report*, 2008, vol. 24, pp. 511.
- [19] Ç.Z. Ünsal, "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", *Hacettepe Hukuk Fakültesi Dergisi*, 3(1) 2013, 99-124.
- [20] Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme, Available: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
- [21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Available: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
- [22] Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması Ve Değerlendirilmesi, Available: <http://www.kiselsaglikverileri.org/hakkinda.php?id=32>
- [23] WMA General Assembly, Washington, DC, USA, October 2002.
- [24] European Charter of Patients' Rights Basis Document*, Rome, November 2002.
- [25] Hasta Hakları Yönetmeliği, Available: <http://www.haksay.org/?q=node/18>
- [26] "Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı", *T.C. Sağlık Bakanlığı*, Available: <http://www.saglik.gov.tr/TR/belge/1-17634/kisisel-saglik-verilerinin-islenmesi-ve-veri-mahremiyet-.html>
- [27] An Introduction To ISO 27799 (ISO27799), Available: <http://www.27000.org/iso-27799.htm>
- [28] Kişisel sağlık verilerinin Elektronik İletişim Yöntemleriyle İletimi, standartları ve çözüm yolları, Available: http://www.saglikbilisimdernegi.org/makaleler.php?mak_id=20
- [29] Protected Health Information: What Does PHI Include?, *HIPAA*, Available: <http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include/>
- [30] R. McClelland ve C.M. Harper, "European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare".
- [31] Medula, Available: <http://www.saglik.gov.tr/TR/belge/1-29730/medula.html?vurgu=medula>
- [32] SağlıkNET, Available: <http://www.e-saglik.gov.tr/SaglikNet/SaglikNetHakkinda.aspx>
- [33] A. Altay, "Sağlık Hizmetlerinin Sunumunda Yeni Açılımlar Ve Türkiye Açısından Değerlendirilmesi", *Sayıştay Dergisi*, Sayı 64.
- [34] I.Sağlık Hukuku Sempozyumu İzmir Üniversitesi'nde, Available: <http://sbe.izmir.edu.tr/haberler/item/253-i-sa%C4%9F%C4%B1k-hukuku-sempozyumu-izmir-%C3%BCniversitesi-nde-%C3%BCzenlendi.html>
- [35] Veri Güvenliği Hakkında Genelge 2005/153, Available: <http://sbsgm.saglik.gov.tr/belge/1-24386/veri-guvenligi-hakkinda-genelge-2005153.html>
- [36] "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule", *National Institute of Standards and Technology*, USA, 2008.
- [37] Health Care Information and Management System Society (HIMSS), Available: <http://www.himss.org/library/ehr/?navItemNumber=13261>
- [38] G. Ögütçü, N. A. G. Köybaşı, ve S. Cula, "Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi", 2011.
- [39] World Medical Association Declaration of Lisbon on The Rights of The Patient, *The World Medical Association*, INC, Santiago, 2005, Available: <http://dl.med.or.jp/dl-med/wma/lisbon2005e.pdf>
- [40] Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 31.05.2006, Available: <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5510.pdf>
- [41] Veri Güvenliği Hakkında Genelge 2005/153, Available: <http://sbsgm.saglik.gov.tr/belge/1-24386/veri-guvenligi-hakkinda-genelge-2005153.html>

Emre OLCA 2013 yılından itibaren İzmir Üniversitesi Yazılım Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır. Yüksek Lisansını Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği Bölümünde, "An e-Sign Tool For Document Delivery" isimli tez ile tamamlamıştır. Doktorası Ege Üniversitesi Bilgisayar Mühendisliği Bölümünde devam etmektedir. Veri Mahremiyeti ve Güvenliği, Anlamsal Web, Ontoloji, Yazılım Geliştirme Süreçleri alanlarında çalışmalarını sürdürmektedir.

Özgü CAN 2011 yılından itibaren Ege Üniversitesi Bilgisayar Mühendisliği Bölümü Yazılım Ana Bilim dalında Yardımcı Doçent olarak çalışmaktadır. Doktorasını aynı bölümde, "Anlamsal Web için Kişiselleştirilebilir Ontoloji Tabanlı Erişim Denetimi ve Politika Yönetimi" isimli tez ile tamamlamıştır. Yüksek Lisansını "Asal Sayı Örtüntüleri ve Goldbach Sanısı Üzerine Bir Çalışma" isimli tez ile 2002 yılında Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü'nde yapmıştır. Anlamsal Web, Politika Yönetimi, Erişim Denetimi, Bilgi Güvenliği, Veri Anonimleştirme ve Kişiselleştirme konularında akademik ilgi alanına sahiptir.



Adli Bilişim ve Etmen Tabanlı Sistemler

A. Emekci, E. Kuğu

Özet—Bu çalışmada, adli bilişim ile etmen tabanlı sistemler alanlarının entegrasyonu incelenmiştir. Adli bilişim; teknoloji ve teknolojik ürünlerin hayatımızdaki yerinin giderek genişlemesi ve çeşitlenmesine paralel olarak gelişen ve kullanılan yöntem, teknik ve ürünlerin sürekli yenilenmesini gerektiren çok dinamik bir alandır. Özellikle bilgisayar ve iletişim sistemlerinin baş döndürücü bir hızla geliştikleri günümüz dünyasında, depolama kapasitelerindeki artış, sistemlerin dağıtık bir yapıda genişlemesi ve mobilitenin sınır tanımazlığı adli bilişim alanında kullanılacak yeni yöntem, teknik ve ürünlere ihtiyaç duyulduğunun habercisidir. Bu noktada, ortaya çıkan yeni ihtiyaç ve problemlerle başa çıkılmasında, etmen tabanlı sistemlerin adli bilişim alanına büyük katkı yapacağı değerlendirilmektedir. Çalışmada, etmen tabanlı sistemlerin adli bilişim alanındaki uygulamaları etraflıca incelenmiş, bu doğrultuda halihazırda ve gelecek dönemde etmen tabanlı sistemlerin adli bilişim alanında daha etkin kullanılmasına dönük değerlendirmeler yapılmıştır.

Anahtar Kelimeler— Adli bilişim, Akıllı sistemler, Etmen, Etmen tabanlı sistemler

Abstract—The subject of this paper is a research on the integration of digital forensics and agent-based systems fields. Digital forensics is a very dynamic field that necessitates modernized and upgraded methods, techniques and tools in parallel with the expansion of technology and its products in our lives. Especially, the incredibly fast progress in computer and telecommunication systems in today's world, increasing capacity of data storage, distributed structure of the systems and no-boundaries in mobility are the harbingers of some new methods, techniques and tools needed in digital forensics. At this point, it is estimated that agent-based systems can well contribute to digital forensics field to cope with the emerging needs and challenges. In this study, a wide range of the applications of agent-based systems on digital forensics field has been examined, and in this direction, some inferences have been made for the more effective usage of agent-based systems on the field of digital forensics.

Index Terms—Agent, Agent-based systems, Digital forensics, Intelligent systems

I. GİRİŞ

GÜNÜMÜZDE her alanda olduğu gibi, belki çok daha fazlaca, bilgisayar ve iletişim alanlarında en belirleyici ve önemli unsurlardan bir tanesi hızdır. Buna paralel olarak,

Adem Emekci, Hava Harp Okulu, Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, Türkiye. (e-posta: adem.emekci@gmail.com)

Emin Kuğu, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye. (e-posta: e.kugu@hho.edu.tr)

adalete ilişkin yapılan işlemlerle ilgili olarak “Gecikmiş adalet, adalet değildir” sözünü duymayacağımızı sanıyorum yoktur. Özellikle teknolojik imkânlarla çok az maliyetle ve hemen herkesçe çok kolay erişilebilir olması, üretilen her türlü verinin de kahir ekseriyetle elektronik ortamda üretilmesi ve tutulması sonucunu doğurmuştur. Bu kadar çok elektronik verinin üretildiği bir ortamda, suç örgütleri ya da bireylerce işlenen suçlarda, işlenen suçlara ilişkin elde edilen deliller arasında elektronik verilerin oranının artması da olağan bir sonuçtur.

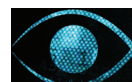
1965 yılında Intel firmasının kurucularından Gordon Moore'un, yapacağı bir konuşmaya hazırlık yaptığı süreçte gözlemlediği bir durum bilişim dünyasının geleceğini çizmiş gibidir. Moore Kanunu olarak bilinen bu gözleme göre, ortalama her 18-24 aylık dönemlerle yonga kapasitesi, işlemci hızı ve veri depolama kapasitesi iki katına çıkmaktadır [1]. Günümüzde de büyük oranda doğruluğunu sürdüren bu çıkarım, maalesef adli bilişim alanı için incelenmesi gereken verilerin giderek artıyor olması gibi bir sorun oluşturmaktadır. Bilişim sistemlerinin ve teknolojik ürünlerin artık çok yaygın olarak kullanılıyor, sistemlerin karmaşık ve dağıtık bir yapı gösteriyor olması adli bilişim alanının ilgilenmesi gereken diğer sorunlar olarak göze çarpmaktadır.

Adli bilişim alanındaki yukarıda bahsedilen problem sahalarının hafifletilmesi noktasında, etmen tabanlı sistemlerin katkısının büyük olacağı düşünülmektedir. Çalışmanın diğer bölümleri ve ele alınacak konular şöyle olacaktır: Bölüm 2’de adli bilişim ve uygulama alanları, Bölüm 3’te etmen tabanlı sistemler, Bölüm 4’te etmen tabanlı sistemlerin adli bilişim alanındaki uygulamaları ele alınacak, Bölüm 5’te iki alan arasındaki entegrasyonun geliştirilmesi üzerine bir değerlendirme yapılacaktır ve Bölüm 6’da da sonuç ile çalışma tamamlanacaktır.

II. ADLİ BİLİŞİM VE UYGULAMA ALANLARI

Adli bilişim kavramının ortaya çıkması, bilişim ve bilgisayar teknolojilerinin gelişmesine ve suç işlemede bir unsur olmaya başlamasına paralel olarak 1980’li yılların sonlarına dayanmaktadır. Ancak adli bilişim uygulamalarından biri olan veri kurtarma işlemini de dikkate aldığımızda, aslında 1970’lerin ilk dönemlerine kadar gitmemiz gerekir [2]-[3].

Adli bilişim, herhangi bir suça konu olarak elde edilmiş bulunan elektromanyetik/elektro-optik ortamlarda muhafaza edilen, taşınan, iletilen vb. verilerin hukuk kurallarına uygun olarak tespiti, elde edilmesi, toplanması, saklanması,



derlenmesi ve yine uygun teknikler kullanılmak suretiyle analiz edilmesi sonucu elde edilecek suça ilişkin kanıtların adli makamlara sunulması işlemleri bütünüdür [4]-[5]. Uygulamada intihar gibi çok basit bir olaydan, uyuşturucu tacirlerinin iletişimlerinin ortaya çıkarılmasına, sosyal medya ortamında bir şahsa yönelik hakâretten, çok sayıda müşterisi bulunan bir bankanın veri tabanındaki tüm bilgilerin saldırganlarca ele geçirilmesine ve hatta siber saldırı yöntemleriyle bir ülkenin, diğer bir ülkenin bilgisayar sistemlerini çökertmesine kadar çok geniş bir yelpazeyi ilgilendirmektedir.

Adli bilişim uygulamalarında yapılan işlemler birbirlerine çok yakın olmakla birlikte, işlenen suçun türü, söz konusu elektronik ortam, elektronik ortamın yapısı, delillerin kalıcı-uçucu olması, suç şüphelilerinin uyguladıkları karartma teknikleri ve yapılan işlemlerin zamanı gibi faktörlere bağlı olarak bazı adli bilişim türlerinden bahsetmek mümkündür [5]-[6].



Şekil 1. Elektronik delil ortamları

A. Geleneksel Anlamda Adli Bilişim (Disk Forensics)

Adli bilişimin ilk uygulamaları kalıcı veriler üzerindeki işlemler olmuştur. Bilgisayar sabit diski, USB bellek, hafıza kartları, CD/DVD/Bluray gibi elektronik ortamlardaki işlemleri kapsar. İnceleme yapılan alanları; dosya türleri, işletim sistemleri, işletim sistemi kayıtları, veri kurtarma, şifre çözme, ayrılmamış bölümlerin incelenmesi şeklinde sıralayabiliriz.

B. Canlı Adli Bilişim (Live Forensics)

Bir siber suçun araştırılmasında ya da şifreli bir dosyanın şifresini elde etmek amacıyla bazı durumlarda ilgili bilgisayarın belleğindeki (RAM) verilere ulaşmak gerekebilir. Bu sayede, bir siber saldırıda o an bilgisayarda hangi işlemlerin çalıştığı, hangi portların açık olduğu gibi bilgilere ya da örneğin PGP şifreleme programını kullanan bir şüphelinin uzak bağlantı yaptığı sunucuya bağlanırken kullandığı parolaya erişmek mümkün olabilecektir.

C. Ağlarda Adli Bilişim (Network Forensics)

Özellikle siber suçların soruşturulmasında, bir bilgisayar sabit diski ya da şüpheliden ele geçirilen bir USB bellek üzerinde yapılacak incelemeler yeterli olmayacaktır. Örneğin, önemli bir bankanın veri tabanlarına saldırganlarca sızma girişimlerinin yapıldığı bir durumu ele alalım. Burada uygulanacak adli bilişim işlemlerinin konusunu bilgisayar ağları ve bu ağlara bağlı sistemler, cihazlar oluşturacaktır. İlgili bankanın bilgisayar ağ yapısı, saldırıların türü, ateş duvarı, saldırı tespit ve önleme sistemleri, günlük kayıtlar ve belki de yönlendirici/anahtarlama cihazları, ağ/e-posta/dosya sunucusularının tamamının incelenmesinin gerektiği bir inceleme söz konusu olacaktır. Ağlarda adli bilişimin uygulama alanları kablolu, kablosuz ve mimarisi itibarıyla bulut bilişim ağ yapılarıdır. Belki kullanımının ve etkilerinin yoğun olması nedeniyle sosyal ağ incelemelerini de bu bölüme dahil etmek mümkündür.

D. Mobil Cihazlarda Adli Bilişim (Mobile Device Forensics)

Günümüzde hemen hemen herkes bir cep telefonu sahibidir. Artık cep telefonları sadece ses iletişimi için değil, akıllı telefonların yaygınlaşması ile belki daha çok veri iletişimi için kullanılmaktadır. Bu adli bilişim türünün ayrı tutulmasının nedenleri, ilk olarak GSM mimarisinin ve SIM kart teknolojisinin kullanılıyor olması, ikinci olarak ise bilgisayarlarda kullanılan standartlardan çok daha geniş bir yelpazede standartların kullanılmasıdır (özellikle verilerin kopyalanmasında cihazlar üzerindeki bağlantı kapılarının çok farklılık göstermesi).

III. ETMEN TABANLI SİSTEMLER

Öncelikle etmen sistemlerin temelini oluşturan yapay zeka ve etmen kavramlarından bahsetmek doğru olacaktır. Yapay zeka (artificial intelligence), normal bir insanın zekice kabul edebileceği şekilde davranan bir bilgisayar işleci oluşturulmasıdır [7]. Etmen (agent) ise, algılayıcıları sayesinde çevresini algılayan ve hareket organlarıyla çevresine katkı sağlayan, kullanıcısının kendisine verdiği hedefler doğrultusunda çalışan, bu hedeflerin gerçekleştirilmesinde otonom (kendi kendine karar verebilen) ve çevresinde başka etmenler varsa onlarla iletişim ve etkileşim halinde, sosyal bir program parçasıdır [8]-[9]-[10]. Etmenlerin özelliklerini; otonom, reaktif, proaktif, uyumlu, süreklilik gösteren, sosyal, esnek, işbirliği ve iş paylaşımına açık olarak sıralayabiliriz [9]. Bu iki kavramdaki özelliklerden akıllı etmen (intelligent agent), akıllı etmenlerden de etmen tabanlı sistemler geliştirilmiştir.

Adli bilişim alanının, her geçen gün artan elektronik ortamdaki verilerin adli açıdan analizinde ihtiyaç duyduğu tam da böyle bir araçtır. Alanın yoğunluğunu hafifletecek reçete; yağınla elektronik ortamdaki veri içerisinden öncelikle konu ile

ilgili olanları tespit etmek, bunları uygun yöntemlerle elde etmek, gerekiyorsa farklı elektronik ortamlar arasında bir örüntü ortaya çıkarmak, kısacası gerekli ile gereksizi ayırt etmek ve bu işlemleri bir adli bilişim uzmanının klasik yöntem ve araçları kullanarak gerçekleştirebileceğinden çok daha süratli ve hatasız bir şekilde yerine getirmektir. İşte adli bilişim alanında ihtiyaç duyulan ve kaldırıcı etkisi oluşturacak böyle bir değişimi, içinde barındırdığı özellikler sayesinde etmen tabanlı sistemler yardımıyla gerçekleştirmek mümkün olabilecektir. Bu bağlamda, çalışmanın bir sonraki bölümünde, bahsedilen adli bilişim alanı ihtiyaçlarından bir kısmını karşılama noktasında akıllı etmen veya etmen tabanlı sistemler yapıları üzerinden geliştirilmiş uygulamalar incelenmiştir.

IV. ETMEN TABANLI SİSTEMLERİN ADLI BİLİŞİM ALANINDAKİ UYGULAMALARI

Literatür taramasında etmen tabanlı sistemler ile adli bilişim alanlarının entegrasyonu adına bir çok çalışma yapıldığı görülmüştür. Gerçekleştirilen çalışmalar ve ortaya çıkan ürünlere bakıldığında; etmen tabanlı sistemlerin, yapılan işlem ve incelemelerin daha hızlı ve verimli hale getirilmesi doğrultusunda temel adli bilişim işlemlerinden, fiziki delillere ilgili kolluk uzmanlarınca erişiminin zor olması ya da ilgili sistemin bir RAID yapısı ya da bulut bilişim mimarisinde olması nedeniyle sistemin çalışmasını sekteye uğratmadan uzak bağlantı yoluyla elektronik delillerin toplanmasına, suç şüphelilerinden ele geçen cep telefonlarının veri tabanlarının kopyalanmasından, gerçekleşmiş ya da devam etmekte olan bir siber saldırının tespiti, ilgili delillerin elde edilmesi ve analizinin yapılmasına kadar bir çok uygulamaya rastlanmıştır. Bu uygulamaları aşağıdaki alt başlıklarda ele alacağız.

A. Temel Adli Bilişim İşlemlerine İlişkin Uygulamalar

İlk olarak temel adli bilişim uzmanlarının işlerini kolaylaştıran ve zamanı daha etkin kullanmalarına imkân sağlayan MADIK uygulamasına değineceğiz. MADIK (Multi-Agent Digital Investigation ToolKit), aslında temel adli bilişim incelemelerinin uygulandığı bir çok etmenli sistem yaklaşımıdır [11]-[12]. Bu kısımda sadece temel incelemeye ilişkin özelliklerini ele alacağız. MADIK uygulaması içerisinde altı adet etmen geliştirilmiştir. Bu etmenler ve işlevleri şöyledir:

--HashSetAgent: Elektronik ortamdaki tüm dosyaların MD5 özetlerini (hash) çıkaran ve bu özetleri kendi veri tabanındaki bilinen sistem dosyaları (örneğin Windows işletim sistemlerindeki System32 klasöründeki dosyalar) ile incelemeye gerek duyulmayacak yazılım dosyalarının (örneğin Java kurulum dosyaları) özetleri ile karşılaştırarak örtüşenleri incelenecek dosyalar arasından eleyen etmendir.

--FilePathAgent: Elektronik ortamdaki kurulu bulunan yazılımların varsayılan klasör/dosya yollarını veri tabanında tutan ve incelemeyi kolaylaştıran etmendir.

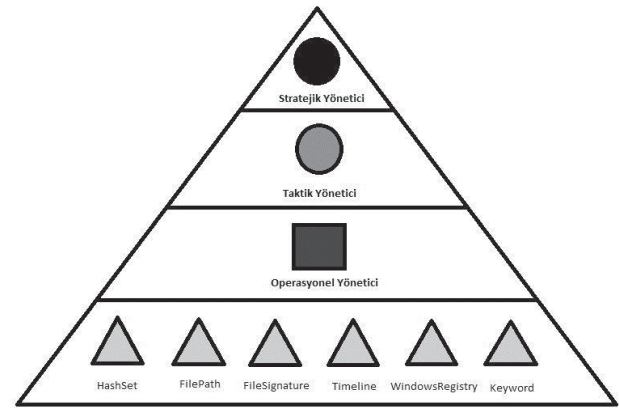
--FileSignatureAgent: İncelenen dosya uzantılarının, dosya başlıkları (file header) ile uyumlu olup olmadığını

inceleyen etmendir.

--TimelineAgent: Dosyaların oluşturulma, son erişim ve değiştirilme zamanlarını çıkaran etmendir. Yazılımların kurulum zamanları, yedeklemeler, internet tarayıcısı üzerindeki işlemlerin incelenmesinde yardımcı olur.

--WindowsRegistryAgent: Windows tabanlı işletim sistemlerinde sistemin kurulum zamanı, bilgisayar zaman ayarlaması, taşınabilir ortam bilgilerinin tespitinde yardımcı olan etmendir.

--KeywordAgent: Elektronik ortamdaki e-posta adresleri, URL bilgileri, kredi kartı bilgileri gibi standartlık içeren verilerin tespitine yardımcı olan etmendir.



Şekil 2. MADIK mimarisi

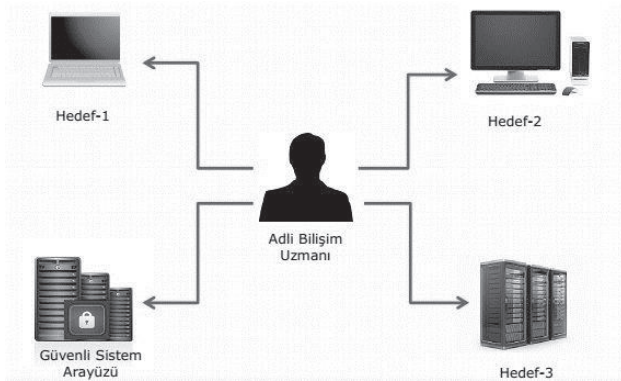
Diğer bir uygulama ise adli bilişim kapsamında spam e-posta incelemelerine yardımcı olmak amacıyla, yapay zeka ve veri madenciliği teknikleri kullanılarak geliştirilmiş olan EMADIK uygulamasıdır [13]. MADIK içerisindeki etmenler ile aynı isim ve işlevlere sahip etmenlerin e-posta incelemesinde kullanıldığı bir yapıdır.

B. Ağlarda Adli Bilişime İlişkin Uygulamalar

Günümüzde artık işlemlerin büyük çoğunluğunu bilgisayar, akıllı cep telefonları kullanılarak internet üzerinden ya da örneğin iç ağına sahip bir firma için bilgisayar ağları üzerinden gerçekleştirilmektedir. Örneğin, bir kolluk görevlisinin bir suç kapsamındaki soruşturmayı yürüten savcı tarafından bir firmaya ait ağına bağlı bazı çalışanların kullandıkları bilgisayarları kopyalamak ve incelemek üzere ya da bir sistem güvenlik yöneticisinin firma güvenlik müdürü tarafından firmanın iç ağına bağlı bilgisayarlara zararlı bir yazılım bulaşması üzerine problemin giderilmesi için görevlendirildiğini düşünelim. Devam eden bölümde, bahsedilen bu gibi durumlarda yapılacak işlemlerin yasal çerçevede ve sağlıklı bir şekilde yapılabilmesi için geliştirilmiş iki ticari uygulama ele alınmıştır.

Aynı amaçla geliştirilmiş bu iki uygulama, Guidance Software firmasının ürünü EnCase® Enterprise (EE) [14] ve AccessData firmasının ürünü AccessData® Enterprise'dır [15]. Her iki uygulama da, bir ağ içerisinde gerekli delillere güvenli

bir altyapı bağlantısı üzerinden erişim sağlayarak, ilgili bilgisayar üzerinde adli bilişim kurallarına bağlı kalarak ön inceleme yapmaya, ilgili bilgisayar diskinin ya da RAM'inin kopyasını almaya ve RAM'de bulunan canlı bilgileri incelemeye imkan vermektedir. Yine her iki uygulama da sunucu-istemci mimari yapısı içerisinde; delillere erişecek bir inceleme bilgisayarı, hedef bilgisayara yüklenecek bir etmen (EE için servet, AccessData Enterprise için agent) ile sistemin güvenliğinin (bağlantı ve yetkilendirme güvenliği) ve yapılan işlemlerin adli bilişim açısından sağlıklı olmasının sağlanması (işlemin kim tarafından, ne zaman, ne şekilde yapıldığı ve hangi işlemlerin gerçekleştirildiği) amaçlarıyla kullanılan bir güvenli sistem arayüzünden oluşmaktadır. Bu uygulamalar kullanılarak, merkezî olarak yürütülen bir soruşturmada ya da bir firmanın farklı yerlerde bulunan birimlerinin ağına bulaşmış bir zararlı yazılımın incelenmesinde, şayet yapılan işlemler bir suç soruşturması kapsamında ise gizlilik ve sistemin çalışmaya devam etmesi sağlanacak, eğer konu bir zararlı yazılım incelemesi ise sistemlerin çalışması sekteye uğratılmayacak, yapılacak işlemler de hem bilgi güvenliği ve hem de adli bilişim noktasında yasal ve sağlıklı bir şekilde gerçekleştirilebilecektir.



Şekil 3. Bilgisayar ağlarında adli bilişim uygulaması

Bilgisayar ağlarının çok dinamik bir yapıda olması, ağ üzerindeki trafiğe ilişkin; kim, nerede, ne zaman, ne amaçla, hangi yetkiyle, ne yapmış gibi sorulara cevap verebilecek şekilde tüm verilerin kaydının tutulmasını zorunlu hale getirmiştir. Bir sisteme bir saldırı gerçekleştiğinde, öncelikle saldırı esnasında tespiti ve engellenmesi, eğer saldırı gerçekleşmiş ve sonlanmışsa da bu saldırının izlerinin tespiti ve kaynağının ortaya çıkarılmasında bizi sonuca ulaştırmada yardımcı olacak işte az önce sözü edilen kayıtlardır. Ancak gerek bu kayıtların standart olmayışı ve karmaşık yapıda olmaları, gerekse kayıtların çok fazla ve insan gözüyle incelenmesinin mümkün olmayışı bazı pratik çözümleri gerektirmiştir. Bu noktada etmen tabanlı sistemlerin ağ üzerindeki işlemlerin analizinde kullanılmasına ilişkin bazı çalışmalar yapıldığı görülmüştür.

Bu kısımda ilk olarak JADE (Java Agent DEvelopment Framework) platformu [16] üzerinde geliştirilmiş etmen tabanlı bir uygulama ele alınmıştır [17]. Uygulamanın amacı, dağıtık mobil etmen yapısı üzerinden ağ trafiğinin ve ağ

kayıtlarının elde edilerek, bu verilerin analizinin yapılmasında incelemeyi yapan adli bilişim personeline bir arayüz yordamıyla yardımcı olmaktır. Uygulama bir merkezi ve üç adet de mobil olmak üzere dört bölümden oluşmaktadır. Uygulamada; ağ trafiği, sızma tespit sistemi ve bir ağ sunucusu üzerindeki işlemlerin kayıtları geliştirilmiş etmenler ile elde edilerek bu kayıtlar üzerinden merkezi ağ adli bilişim etmeni kontrol ve koordinesinde analizler yapılmaktadır. Merkezdeki adli bilişim etmeni üzerinden tüm veriler tek noktadan bir arayüz vasıtasıyla takip edilebilmekte ve gerekli analizler gerçekleştirilebilmektedir.

İkinci olarak ise, ateş duvarı (firewall) üzerindeki kayıtların incelenmesini konu alan bir uygulama ele alınmıştır [18]. Bir bilgisayar ağı üzerindeki ateş duvarı kayıtlarının çoklu etmen mimarisi yordamıyla elde edilmesi ve incelenmesi konu edilmiştir. Uygulamada üç etmenli bir yapı öngörülmüştür. Bir etmen tarafından (collector agent) ateş duvarı üzerindeki kayıtların bir kopyası elde edilerek kayıt numarası, kaydın tarihi, zamanı, kaynak-hedef IP adresleri ve port numaraları ile kullanılan protokol bilgileri bir veri tabanına aktarılmaktadır. Bir diğer etmen (inspector agent) tarafından veri tabanındaki kayıtlar incelenerek, bilgi tabanındaki kurallara göre normal ya da zararlı işlem olarak belirlenmektedir. Zararlı olarak belirlenen işlemler, bir sonraki adımdaki etmene (investigator agent) ay, gün ve işlem numarası tabloları şeklinde yapılandırılarak aktarılmaktadır. Buradan sonraki aşamada ise, sağlanan bir arayüz yordamıyla adli bilişim personeli ya da ağ güvenlik birimi tarafından bu tablolar incelenerek istenen sonuçlara ulaşılabilmektedir.

C. Mobil Cihazlarda Adli Bilişime İlişkin Uygulamalar

Bu kısımda benzer mantıkla çalışan üç uygulama ele alınmıştır. Her üç uygulamada da, cihazın veri tabanları cihaza yüklenen bir etmen yardımıyla kopyalanır ve istemci-sunucu mimari yapısında analiz bilgisayarına aktarılır. Cihaza yüklenen etmen, kopyalama işleminin bitiminde kendiliğinden cihazın belleğinden silinmekte ve böylece cihazdaki verilerin orijinalliğinin bozulmasının önüne geçilmiş olmaktadır.

Bu uygulamalardan ilki, ticari bir uygulama olan ve birçok telefon modeli ve işletim sistemi ile uyumlu çalışabilen Oxygen Forensic® Suite ürünüdür [19]. Bir diğeri, Blackberry marka cep telefonlarının veri tabanlarındaki verilerin kopyalanması ve analizine ilişkin BAAT (Blackberry Acquisition and Analysis Tool) uygulamasıdır [20]. Son uygulamamız da, Android tabanlı cep telefonlarının kopyalanmasında ve veri tabanlarının analizinde kullanılan SAFT uygulamasıdır [21].

D. Adli Bilişim Sistemlerine İlişkin Uygulamalar

Bu kısımda, ilk olarak daha önce bahsettiğimiz MADIK uygulamasının sistem tarafını ele alacağız [11]-[12].

MADIK'te dört katmanlı bir yapı düşünülmüştür. Yukarıdan aşağı olacak şekilde; *Stratejik, Taktik, Operasyonel Yönetici* katmanları ile *Uzman* katmanlarından oluşmaktadır. Bu şekilde bir hiyerarşik yapı oluşturulmak suretiyle; incelenecek elektronik deliller, bir ön inceleme sayesinde değerlerine göre sınıflandırılmakta, rutin ve tekrar mahiyetindeki işlemler azaltılmakta, deliller arasında bir korelasyon oluşturulmakta ve iş paylaşımı sağlanmaktadır. En son aşamada MADIK sisteminden geçen elektronik deliller, insan adli bilişim uzmanlarının kontrolünde değerlendirilerek nihâi kararlar verilmektedir.

Ele alacağımız diğer bir sistem, adli bilişim işlemlerinin gerçekleştirileceği bir ortam olarak bulut bilişim mimarisini kullanan CUFF (Collaborative Forensic Framework) sistemidir [22]. CUFF sistemi; *CUFF Link* adı verilen ve sistemin diğer unsurları arasındaki iletişimi sağlayan bir haberleşme platformu, *Analysis Block* adı verilen ve iş paylaşımını koordine eden bir analiz merkezi, delillerin muhafaza edildiği ve ilgililerce paylaşımının sağlandığı bir veri deposu ve tüm bu işlemlerin adli bilişim uzmanlarınca takibine imkân veren bir arayüzden oluşmaktadır. CUFF sayesinde, çok farklı problemlerle karşılaşan uzmanlar arasında fikir ve tecrübe alış veriş sağlanmakta ve ayrıca iş dağılımı yapılarak işlemlerin daha kısa sürede tamamlanması imkânı elde edilmektedir.

V. DEĞERLENDİRME

Önceki bölümlerde, adli bilişim ve etmen tabanlı sistem kavramları ile bu iki alan arasında bir entegrasyon sağlanması noktasında yapılan çalışmalar incelenmiştir. Bilişim ve iletişim sektörlerindeki gelişmelere paralel olarak ilgi yelpazesi genişleyen adli bilişim alanı, artık klasik yöntem, teknik ve ürünlerin yetersiz kaldığı bir zaman dilimine girmiştir. Yapılan bazı çalışmalarda, adli bilişim alanının çıkmaza girmesi muhtemel konular şöyle sıralanmıştır [2]-[22]:

--Veri depolama kapasitelerindeki ve dolayısıyla elektronik delil ortam kapasitelerindeki artış

--Özellikle cep telefonu teknolojisindeki gelişmelere paralel olarak gömülü sistemlerdeki artış ve donanım arayüzlerindeki çeşitlilik

--İşletim sistemlerindeki ve dosyalama sistem formatlarındaki gelişmeler

--Bir davaya ilişkin elde edilen elektronik ortamlardaki deliller arasındaki korelasyonun ortaya çıkarılması gerekliliği

--Yaygın kriptografik uygulamalar

--Zararlı yazılımlardaki artış ve çeşitlilik bağlamında geçici bellek incelemelerinde yaşanan zorluklar

--Belki de en önemlisi bulut bilişim mimarisinin giderek yaygınlaştığı bir ortamda klasik adli bilişim uygulamalarının neredeyse tamamen geçersiz/yetersiz kalması

--Bilişim ve iletişim dünyasını takip etmekte çok yavaş kalan yasal düzenlemeler ve yaşanan problemler

Problem sahasının giderek yoğunlaştığı bir alan olarak, içine

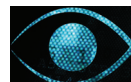
düştüğü/düşeceği çıkmazların telafisinde adli bilişim alanı, birçok alandan olduğu gibi etmen tabanlı sistemlerden de pekala faydalanabilir. Bu bağlamda; veri depolama teknolojisindeki kapasite artışı ve düşük maliyetlerle orantılı olarak elektronik delil korelasyonunun ortaya çıkarılması, internete bağlanan cihaz çeşit ve sayısındaki artış dikkate alındığında internet ve sosyal ağ incelemeleri, bulut bilişim teknolojisinin getirdiği sorunlar, kriptanaliz yeteneklerinin artırılması, siber saldırıların artık profesyonel anlamda siber ordulara dönüşümünün yaşandığı günümüz dünyasında saldırı tespit, önleme ve analiz yeteneklerinin artırılmasında etmen tabanlı sistem uygulamalarının adli bilişim alanına çok katkı sağlayabileceği öngörülmektedir.

VI. SONUÇ

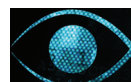
Bu çalışmada, adli bilişim ile etmen tabanlı sistemler alanlarının entegrasyonu incelenmiştir. Adli bilişim kavramı ve türleri açıklanmış, etmen tabanlı sistemler ve özellikleri ele alınmış, etmen tabanlı sistemlerin temel adli bilişim işlemleri, ağlarda adli bilişim, mobil cihazlarda adli bilişim ve adli bilişim sistemlerine ilişkin uygulama örnekleri incelenmiş ve hâlihazırdaki katkı alanları ile günümüzde ve gelecekte adli bilişim alanının yaşaması muhtemel problem alanlarına yönelik etmen tabanlı sistem uygulamalarının yapabileceği katkı ve girdiler değerlendirilmiştir.

KAYNAKLAR

- [1] S. Mueller, *Upgrading and Repairing PCs*. Pearson Education, Inc., USA, 20th edition, 2012, p.16.
- [2] S. L. Garfinkel, "Digital forensics research: The next 10 years", *Digital Investigation*, 7:64-73, 2010. The Proceedings of the Tenth Annual DFRWS Conference.
- [3] I. Khoury and E. Caushaj, "Computer Forensic", [Online]. Available: http://www.secs.oakland.edu/~iskhoury/Computer_Forensic_final.pdf
- [4] F. Gallegos, "Computer Forensics: An Overview", *Information Systems Control Journal*, Vol.6, 2005.
- [5] H. Önal, "Bilişim Sistemlerinde Adli Bilişim Analizi ve Bilgisayar Olayları İnceleme - 101", *Bilgi Güvenliği Akademisi*, [Online]. Erişilebilir: http://www.bga.com.tr/calismalar/computer_forensic101.pdf
- [6] J. Sammons, *The Basics of Digital Forensics*. Elsevier Inc., USA, 2012, pp.2-3.
- [7] F. Mitchell, "The Use of Artificial Intelligence in Digital Forensics: An Introduction", *Digital Evidence and Electronic Signature Law Review*, 7:35-41, 2010.
- [8] M. Wooldridge, *An Introduction to Multiagent Systems*. John Wiley & Sons Ltd., Sussex, England, 2002, p.15.
- [9] I. Ademu, C. Imafidon, and D. Preston, "Intelligent Software Agent Applied to Digital Forensics and its Usefulness", 2012, [Online]. Available: http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf
- [10] I. Ademu and C. Imafidon, "Agent-Based Computing Application and its Importance to Digital Forensic Domain", [Online]. Available: <http://world-comp.org/p2012/ICA7716.pdf>
- [11] Bruno W. P. Hoelz, G. Ralha Celia, Rajiv Geeverghese, and Hugo C. Junior, "A Cooperative Multi-Agent Approach to Computer Forensics", *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 2:477-483, 2008.
- [12] Bruno W. P. Hoelz, G. Ralha Celia, Rajiv Geeverghese, "Artificial Intelligence Applied to Computer Forensics", *24th Annual ACM Symposium on Applied Computing, SAC'09, Computer Forensics Track*, 211-217, Honolulu, Hawaii, USA, ACM Press, 2009.



- [13] S. B. Bandgar, M. Sale and B. B. Meshram, "Artificial Intelligence Applied to Digital Email for Forensic Application", ISSN: 2249-0558, 2012.
- [14] S. Bunting, *EnCase Computer Forensics The Official EnCE: EnCase Certified Examiner Study Guide*. John Wiley & Sons Inc., USA, 3rd edition, 2012, pp.176-180.
- [15] AccessData, AD Enterprise, [Online]. Available: <http://www.accessdata.com/solutions/digital-forensics/ad-enterprise>
- [16] T. Italia Lab (TILAB). Java Agent DEvelopment Framework - JADE, [Online]. Available: <http://jade.tilab.com>
- [17] A. Nagesh, "Distributed Network Forensics Using JADE Mobile Agent Framework", [Online]. Available: https://technology.asu.edu/files/documents/tradeshaw/Dec06/asha_nagesh_report.pdf
- [18] H. Bensefia and N. Ghoualmi, "A Mutli-Agent System for Firewall Forensics Analysis" International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 25-33, *The Society of Digital Information and Wireless Communications*, ISSN: 2220-9085, 2011.
- [19] Oxygen Forensics, Oxygen Forensic® Suite, [Online]. Available: <http://www.oxygen-forensic.com/>
- [20] [18] S. K. Sasidharan and K. L. Thomas, "BlackBerry Forensics: An Agent Based Approach for Database Acquisition", *Advances in Computing and Communications, Communications in Computer and Information Science Vol.190, 2011*, pp. 552-561.
- [21] SAFT Mobile Forensics, [Online]. Available: <http://www.signalsec.com/saft/>
- [22] M. Mabey and G. J. Ahn, "Towards Collaborative Forensics: Preliminary Framework", *IEEE International Conference on Information Reuse and Integration (IRI), 2011*, pp.94-99.



Mobil Platformda AKD Tabanlı Görüntü Damgalama

A.Uçar, Y. Becerikli

ÖZET—Günümüzde akıllı telefonlardan çekilen görüntülerin doğrudan cihaz üzerinden internette paylaşılması özellikle gençler arasında oldukça yaygın kullanılır hale gelmiştir. Fakat bu görüntüler internete yüklendikten sonra izinsiz olarak kopyalanabilmekte ve kullanılabilir. Burada bir telif hakkı sorunu ortaya çıkmaktadır. İşte bu sorunun çözümü için, akıllı telefonda fotoğraf çekerken, fotoğrafın içerisine görünmez veri gizleyen (damgalayan) bir uygulama geliştirilmiştir. Damgalama işlemi için Ayrık Kosinüs Dönüşümü (AKD) esaslı, görünmez ve dayanıklı bir metot görüntü sıkıştırma yapılmaksızın kullanılmıştır. Çeşitli saldırılara karşı içerdiği gizli bilgiyi muhafaza etme yeterliliği test edilmiş ve raporlanmıştır. Uygulama Windows Phone 8 işletim sistemine sahip, Nokia Lumia 820 üzerinde gerçekleştirilmiştir.

Anahtar Kelimeler—Damgalama, telif hakkı koruma, ayrık kosinüs dönüşümü, akıllı telefon

Abstract—Nowadays, it has been very common among young people that photographs taken by smart phones are shared directly on the internet via the device. However, these images can be copied or misused without permission after being uploaded on the internet. At this point, the issue of copyright comes up. An application that conceals invisible data into the image has been developed for the solution of this problem. A Discrete Cosine Transform based, invisible and robust method has been used without image compression. The application's capability to protect the concealed data from various attacks has been tested and briefly reported. The application has been operated on Nokia Lumia 820, which has Windows Phone 8 operating system.

Index Terms—Watermarking, copyright protection, discrete cosine transform, smartphone

I. GİRİŞ

Hayatımızın her alanında yer alan, pazara sunulduğu andan itibaren hızla yaygınlaşan kişisel bilgisayarlar ile vazgeçilmez iletişim aracı olan cep telefonlarının, yüksek çözünürlüklü kameraların bir araya gelmesi ile ortaya çıkan akıllı telefonlar son yılların en önemli teknolojik gelişmelerinden biridir. Akıllı telefonlar, boyutlarının

küçülmesi, performansının artması, erişilebilir fiyatlara ulaşması ile birlikte hızla yaygınlaşmıştır. Bu durumu internet ve kablosuz haberleşme alanındaki gelişmelerin takip etmesi ile hem akıllı telefon kullanıcılarının sayısı artmış hem de birçok dijital platforma hızla erişim imkânı sağlanmıştır.

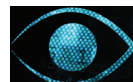
Günümüzde akıllı telefonlardan en yaygın kullanılan dijital platformlar hiç şüphesiz sosyal medya platformlarıdır. İnsanlar günlük hayatlarında akıllı telefonlarından fotoğrafladıkları görüntüleri ve pek çok bilgiyi sosyal medya üzerinden paylaşmaktadırlar. Fakat bu resimler internete yüklendikten sonra izinsiz olarak kopyalanabilmekte, kullanılabilir. Bazen de sahibi tarafından internette paylaşılmayan bilgiler casus yazılımlar ve kötü niyetli kişiler tarafından cihazlardan doğrudan kopyalanabilmekte ve istenildiği gibi kullanılabilir. Burada bir telif hakkı sorunu ortaya çıkmaktadır. İşte bu sorunun çözümü için, akıllı telefonda fotoğraf çekerken görüntü içerisine görünmez veri gizleyen bir uygulama geliştirilmiştir.

Akıllı telefon teknolojisi henüz yeni sayılabilecek bir gelişme olmasına rağmen araştırmacıların dikkatini çekmiş, sınırlı sayıda da olsa görüntü damgalama uygulamaları akıllı telefonlar üzerinde de gerçekleşmiştir. Android sistem üzerinde kaos teorisi tabanlı kırılğan bir görüntü damgalama uygulamasında, 512x512 boyutlarında bir görüntünün damgalanmasında geçen süre yaklaşık 3 sn civarında ölçülmüştür[1]. Yine bu çalışmada, frekans uzayındaki dayanıklı görüntü damgalama uygulamaları çok devasa işlemler gerektirdiğinden ve mobil cihazların sınırlı kaynakları olduğu için bu tür uygulamalarda çok daha az hesaplama gerektiren bu metodun tüm cihazlar üzerinde daha uygulanabilir olduğu vurgulanmıştır. Başka bir çalışmada, görüntüyü internetteki platformlara yüklemeyen damgalayan, Red, Green, Blue (RGB) renk değerlerini ayrıştırıp, G(yeşil) kanalında kaotik seri tabanlı veri gizleme işlemi yapan ve G kanalındaki değerlere göre damgayı messy algoritması ile oluşturan yine piksel uzayında görüntü damgalayan bir android uygulanması gerçekleştirilmiştir [2].

Android sistem üzerinde, frekans dönüşümü(DCT) tabanlı “hymnMark” olarak adlandırılan görüntü damgalama uygulamasında Koch ve Zhao(1995)’nın algoritması üzerinde bazı değişiklikler ve optimizasyonlar yapılarak kullanılmış, ayrıca güç tüketim değerleri ve görüntü üzerine bazı saldırılar yapılarak dayanıklılık değerleri raporlanmıştır [4]. Cep telefonu kameralarından yakalanan görüntüler için önerilen bir çalışmada ise görüntüyü hem frekans dönüşümü tabanlı(DWT)

A. U. Kocaeli Üniversitesi, Bilgisayar Mühendisliği, Görüntü İşleme Laboratuvarı, İzmit, Kocaeli, 41380, TÜRKİYE (sorumlu yazar telefon: +90262 303 3569; e-posta: ali.ucar@kocaeli.edu.tr).

Y. B. Kocaeli Üniversitesi, Bilgisayar Mühendisliği, Kocaeli, 41380, TÜRKİYE (e-posta: ybecerikli@kocaeli.edu.tr); Yalova Üniversitesi, Bilgisayar Mühendisliği; Elektronik ve Haberleşme Mühendisliği; YUBİTAM Araştırma Merkezi, Yalova, TÜRKİYE, (e-posta: ybecerikli@yalova.edu.tr).



ardından da piksel uzayında kırılğan damgalayan bir yöntem önerilmiş, ataklara karşı dayanıklılık sonuçları raporlanmış ama herhangi bir mobil platformda uygulama sonuçlarına değinilmemiştir [5]. İnternete görüntü paylaşırken otomatik olarak görüntüyü yeniden boyutlandırın ve dayanıklı damgalayan farklı bir çalışmada ise, Haar dalgacık dönüşümü temelli yaklaşım ile görüntüye veri gizlenmiştir [6].

Bu çalışmada Windows Phone işletim sistemine sahip, Nokia Lumia 820 akıllı telefonu üzerinde, fotoğraf çekerken, dayanıklı bir metotla görüntü damgalayan mobil bir uygulama geliştirilmiştir. Damgalanan görüntülerin dayanıklılığı, uygulama performansı test edilmiş açıkça sunulmuştur. Bu çalışma Windows Phone ile yapılan ilk dayanıklı görüntü damgalama uygulaması olmasının yanı sıra, fotoğraf çekerken ekranda görünen her bir frame dahil, damgalanmamış görüntünün hiçbir zaman var olmaması ve işlem performansı en önemli farklılığıdır.

II. DONANIM VE YAZILIM

A. Donanım

Bu çalışmada görüntü damgalama uygulamasının gerçekleştirileceği platform olarak, Windows Phone 8, cihaz olarak ise Nokia Lumia 820(Şekil) seçilmiştir.

Windows Phone 8, Visual C++ 2012 destekler ve bu sayede C/C++ dilinde yerel kod(native code) ile uygulama geliştirmeye imkân sağlar. Tüm Windows Phone 8 uygulamaları (tüm uygulamaların native yani yerel koda ihtiyacı olmasa da) yerel kod kullanabilecek şekilde tasarlanmıştır [7]. Aynı zamanda, mobil masaüstü uygulamaları için Windows Runtime kullanımı da mümkündür. Projenin yanında ayrıca eklenecek bir Windows Runtime Compenent projesi ile gerçek zamanda (Run Time) kamera, ses-konuşma, network, konum vb gibi özelliklere erişilebilir [7]. Bu makalede gerçekleştirilen uygulama native code ile geliştirilmiştir. Bu sayede Runtime da kameranın yakaladığı görüntülerin değerleri doğrudan bellekteki adresinden okunarak damgalanmış görüntü elde edilmiş ve sonrasında ekranda görüntülenmiştir.

B. Yazılım

Orijinal görüntünün, yani damgasız görüntünün hiçbir zaman var olmaması prensibine dayalı, mobil platformda dayanıklı bir yöntem ile damgalayarak fotoğraf çeken bir uygulama geliştirilmiştir. Her ne kadar bellekte damgalanmamış görüntü kareleri ham halde kısa süre yer alsalar da, ekranda damgalanmış halleri gösterilir ve telif hakkı yerleştirilmemiş (damgalanmamış) görüntünün hiçbir zaman var olmamasından kasıt budur.

Bu çalışmada gerçekleştirilen uygulamada, fotoğraf çekme sırasında ekranda görüntülen 640x480 boyutlarındaki her bir video karesi damgalanarak görüntülenir ve fotoğraf çekme butonuna basılarak yakalanan görüntü de bu video karelerinden biridir.

III. DAYANIKLI DAMGALAMA VE DAMGA ÇIKARIMI

Damgalama renkli görüntünün, RGB renk modelinde Blue(mavi) katmanı üzerinden gerçekleştirilir. Green(yeşil) ve Red(Kırmızı) katmanları üzerinde herhangi bir işlem yapılmaz. Damgalama işlemi için AKD tabanlı yöntem kullanılmıştır.

Gö mü verisi yerleştirme veya damgalama işlemi için görüntünün mavi katmanı 8x8 lik bloklara ayrılır. Her bir bloğa iki boyutlu AKD uygulanır. Sonuçta 8x8 adet AKD frekans bileşeni elde edilir. Her 8x8 lik bloğa 1 bit veri yerleştirilir. Bu nedenle 640x480 boyutlarındaki görüntü için yerleştirilebilecek maksimum gö mü verisi, 4800 bittir. Gö mü verisi yerleştirme işlemi yapıldıktan sonra TAKD uygulanarak damgalanmış görüntü elde edilmiş olur.

İki Boyutlu AKD formülü denklem (1) TAKD formülü denklem (2) de yer almaktadır[8].

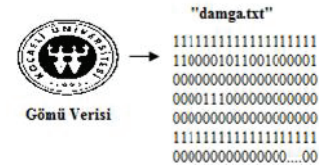
$$F(u, v) = \alpha(u) \alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left(\frac{(2x+1)u\pi}{2N}\right) \cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (1)$$

$$f(x, y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u) \alpha(v) F(u, v) \cos\left(\frac{(2x+1)u\pi}{2N}\right) \cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (2)$$

Bu çalışmada gö mü verisi yerleştirmek için orta frekans bandındaki (4,2) (5,3) nolu AKD katsayısı seçilmiştir[9]. Gö mü verisi 1 ise (5,2) de bulunan AKD frekans katsayısı, (4,3) de bulunan AKD katsayısı bileşeninden büyük olması gerekir. Değ ilse yer değ iştirilir. Eğ er gö mü verisi 0 ise (4,3) de bulunan AKD frekans katsayısı, (5,2) de bulunan AKD frekans katsayısından büyük olması istenir, değ ilse yer değ iştirilir.

Seçilen frekans bileşenleri arasındaki fark az olduğ undan bir dayanıklılık sabiti (k) tanımlanmıştır ve gö mü verisi 1 ise (5,2) > (4,3) koşulu sağ landıktan sonra k değ eri (5,2) katsayısına eklenir. Gö mü verisi 0 olduğ u durumda ise (5,2) < (4,3) koşulu sağ landıktan sonra k değ eri (4,3) katsayısına eklenir[9].

Damga verisi olarak, siyah-beyaz ikili renkte 80x60 boyutlarındaki görüntü seçilmiştir (Şekil 1). Siyah olan pikseller “1” beyaz olanlar ise “0” olacak şekilde damga verisi bir text dosyasına yazılarak uygulamanın gerçekleştirildiği Nokia Lumia 820’ye yüklenmiştir.



Şekil 1. Gö mülecek damganın binary koda dönüştürülerek “damga.txt” dosyasına yazılması

Damga kontrolü için ise damgalama işlemi taklit edilir. Damga olduğ u düşünölen görüntü 8x8’lik bloklara ayrılarak her bir bloğa AKD uygulanır. Her bloktaki (4,3) ve (5,2) nolu katsayılar kontrol edilir. (5,2) de bulunan katsayı (4,3)’de bulunan katsayıdan büyük ise gö mü verisi “1” değ ilse “0” kabul edilir. Tüm blokların kontrolünden sonra elde edilen 4800 elemanlı bit dizisinden, “1”ler siyah, “0”lar beyaz çizdirilerek 80x60 boyutlarında gö mü verisinin gö rsel hali elde

edilir.

IV. BULGULAR

Görüntü damgalama çalışmalarında dayanıklılığın yanında Tepe Sinyal Gürültü Oranı (PSNR) da önemli bir değerlendirme kriteridir. PSNR, orijinal görüntüyü baz alarak, damgalanmış görüntüdeki bozulma değerini ifade eder [10].

Bu çalışmada geliştirilen uygulamada ise orijinal görüntü hiçbir zaman var olmadığı için, telefon kamerasından alınan orijinal görüntüler ile damgalanmış arasında PSNR hesaplanamaz. Bu sorunu çözmek için, bu çalışmada kullanılan yöntem sabit görüntülere uygulanmış, Lena, Baboon, Peppers, Tiffany görüntüleri damgalanarak PSNR değeri hesaplanmıştır. PSNR (3) değeri hesaplanması için öncelikle MSE (4) değeri hesaplanmalıdır.

$$MSE = \frac{\sum_{M,N} [I(i,j) - K(i,j)]^2}{M \times N} \quad (3)$$

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (4)$$

Dayanıklılık sabiti (k) değeri, insan göz sistemi(IGS) tarafından fark edilemeyecek kadar küçük, saldırılara dayanabilecek kadar yüksek olmalıdır. Bu nedenle farklı (100-900 arasında) k değerleri için PSNR değerleri (EK-A, Tablo I) ve damga çıkarım doğruluk oranları hesaplanmıştır (EK-A, Tablo II). Yapılan denemeler sonrası hem damga dayanıklılığı hem de PSNR değerlerinin kabul edilebilir seviyelerde olması için k değerlerinin 900 olmasına karar verilmiştir.

Windows Phone 8 platformunda medya galerisine görüntü kaydetme işlemi ancak jpeg formatında yapılabilmektedir. Ancak uygulama ekranında görüntülenen damgalı her bir görüntü Bitmap formatındadır. Bu nedenle kaydedilmek istenen her bir görüntü jpeg olarak kaydedilir. Bir diğer deyişle kaydedilen görüntüler cihaz tarafından jpeg sıkıştırma saldırısına maruz kalır.

Geliştirilen uygulama aracılığı ile belirlen 900 dayanıklılık sabiti değeri ile 6 farklı görüntü çekilmiş (Ek-B, Şekil 1) ve bu görüntülere Photoshop CS3© bazı saldırılar uygulanmıştır. Bunlar, Despeckle, Gaussian, Sharpen ve Sharpen Edge filitreleri ile yeniden boyutlandırma (resize) ve jpeg sıkıştırma saldırılarıdır. Saldırı uygulanmış görüntülere damga verisi kontrolü işlemi yapılmış, çıkartılan damga verisi orijinal damga ile karşılaştırılmıştır (Ek-B, Tablo 3), yüzdeli (%) ifadeler çıkarılan gömü verisinin doğruluk oranını vermektedir. Bu verilerden yola çıkarak, damganın büyük ölçüde korunduğu söylenebilir.

V. SONUÇ VE ÖNERİLER

Damgalanmış görüntülerin çeşitli saldırılara karşı dayanıklı olduğu, çok sayıda saldırı uygulanarak tespit edilmiştir. Ayrıca facebook, instagram ve whats up gibi görüntü paylaşımının sık kullanıldığı sosyal medya ortamlarına da damgalanmış görüntüler yüklenerek test edilmiş ve damganın korunduğu görülmüştür. Damgalanmış görüntü ile orijinal görüntü arasındaki bozunma, PSNR>34 ölçülmüştür. Ayrıca Despeckle, Gaussian, Sharpen ve Sharpen Edge filitreleri ile yeniden boyutlandırma (resize) ve jpeg sıkıştırma saldırılarına karşı dayanıklı olduğu dayanıklı olduğu tespit edilmiştir. Gerçekleştirilen uygulama ekranda gösterdiği her bir frame i damgaladığı için saniyede 640x480 boyutlarında 4-5 frame ekranda gösterebilmektedir(5 fps).

Frekans uzayında dayanıklı görüntü damgalama gibi çok fazla işlem gerektiren yöntemlerin, oldukça yüksek kapasitelere ulaşmış mobil platformun sağlamış olduğu bazı olanaklar da kullanılarak performanslı bir şekilde gerçekleştirilebildiğinin gösterilmesi, Windows Phone 8 platformunda literatürde bu konuda yapılan ilk çalışma olması ve platformun bu anlamda performans ve yeterliliklerinin ortaya konması, literatürde iyi bilinen AKD tabanlı görüntü damgalama metodunun, ekranda görüntülenen her bir görüntü karesine, literatürden farklı olarak sıkıştırma işlemi yapılmaksızın ve yüksek dayanıklılık sabiti değeri ile uygun PSNR sonuç değeri elde ederek uygulanması bu çalışmanın alana en belirgin katkıları olduğu düşünülmektedir.

Her geçen gün daha hızlı ve daha performanslı akıllı telefonlar piyasaya sürülmektedir. Sonraki çalışmalarda daha güçlü işlemciye sahip daha hızlı akıllı telefonlar üzerinde, hızlı AKD algoritmaları [11] ile 30 fps hızında eşzamanlı görüntü damgalama uygulamaları gerçekleştirilebileceği düşünülmektedir. Görüntü bloklara ayrılıp, her bir bloğa birbirinden bağımsız işlemler uygulandığından, çok çekirdekli mobil platformlarda işlemler parçalara ayrılarak ve farklı çekirdeklere paylaştırılarak daha verimli uygulamalar geliştirilebileceği öngörülmektedir.

EKLER

EK-A

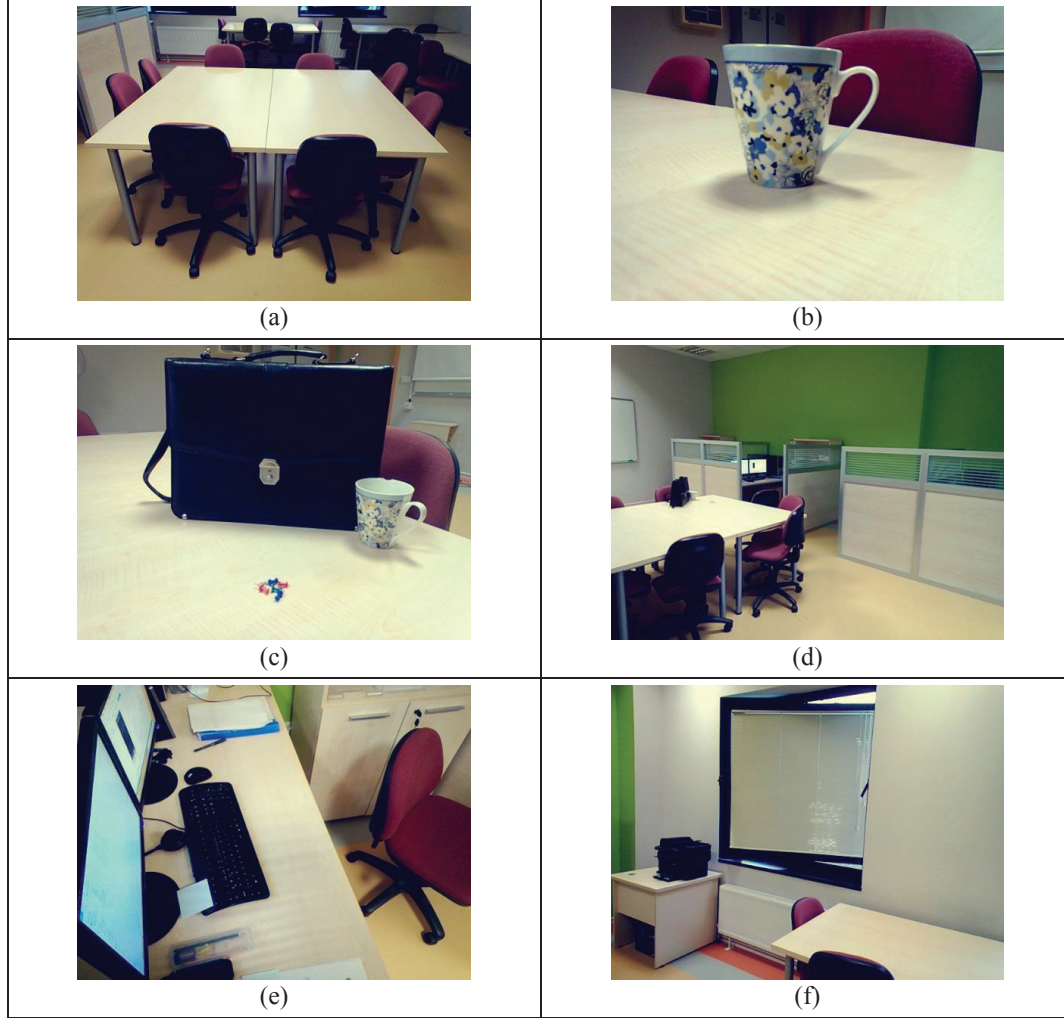
TABLO I
 FARKLI DAYANIKLILIK SABİTİ DEĞERLİ İÇİN PSNR DEĞERLERİ

	k	900	800	700	600	500	400	300
Lena.jpg	PSNR	36,14	36,68	37,23	37,81	38,37	38,93	39,43
Baboon.jpg	PSNR	34,01	34,39	34,76	35,13	35,48	35,79	39,43
Peppers.jpg	PSNR	34,70	35,19	35,70	36,23	36,76	37,27	37,75
Tiffany.jpg	PSNR	36,78	37,33	37,90	38,48	39,07	39,65	40,18

TABLO II
 FARKLI DAYANIKLILIK SABİTİ DEĞERLİ İÇİN DAMGA ÇIKARIM DOĞRULUK ORANLARI

	k	900	800	700	600	500	400	300
Çıkarılan damga "Lena.jpg"		%98,85	%98,6	%98,3	%97,9	%97,37	%96,5	%95

EK-B



Şekil 1. Uygulama aracılığı ile çekilen farklı görüntüler

TABLO III
ÇEKİLEN GÖRÜNTÜLERE UYGULANAN SALDIRILAR SONRASI DAMGA ÇIKARIM BAŞARIMI

	1	2	3	4	5	6	7	8	9	10	11	12
(a)	%99,6	%99,4	%96,3	%91,9	%88,6	%99,2	%99,5	%98,7	%97,4	%99,4	%99,1	%97,6
(b)	%99,3	%98,8	%95,6	%91,8	%88,9	%99	%99,2	%97,6	%96,1	%99,1	%98,4	%97,2
(c)	%99,2	%98,9	%95,4	%91,5	%88,4	%98,9	%99,1	%98,1	%96,8	%99,1	%98,9	%97,2
(d)	%98,6	%98,5	%95,4	%91,4	%88,4	%98,7	%98,8	%97	%95,5	%98,7	%97,9	%97,0
(e)	%98,5	%98,3	%95,4	%91,5	%88,7	%98,4	%98,4	%97,3	%96,0	%98,6	%98,1	%96,6
(f)	%98,6	%98,5	%95,3	%91,5	%88,8	%98,6	%98,5	%97,7	%96,4	%98,9	%98,5	%96,8

Sutun numaraları şu ifadeleri temsil etmektedir: 1. Saldırı uygulanmadan damga çıkarım başarımı, 2. Despeckle saldırısı, 3. Gaussian %3 saldırısı, 4. Gaussian %6 saldırısı, 5. Gaussian %10 saldırısı, 6. Sharpen saldırısı, 7. Sharpen Edge saldırısı, 8. Resize %80, 9. Resize %60, Jpeg Quality=80, Jpeg Quality=60, Jpeg Quality=50. (a),(b),(c),(d),(e),(f) EK-B Şekil 1 deki görüntüleri temsil etmektedir.

TEŞEKKÜR

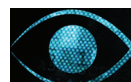
Cihaz destekleri ile uygulamanın sonuçlarının gerçek platformda test edilmesine olanak tanıyan, Microsoft Türkiye ve Sayın Mustafa Kasap'a teşekkür ederiz.

KAYNAKLAR

- [1] Palma Hernandez C., Torres-Huitzi C., A fragile watermarking scheme for image authentication in mobile devices, Electrical Engineering Computing Science and Automatic Control (CCE), Merida City, 26-28 Oct. 2011.
- [2] Patil P.M., Shinde S., Arekar C.V., Bhandwalkar N.M., Copyright for Images with Chaotic Sequence, International Journal of Research, 2014, 1, 96-99.
- [3] Koch E., Zhao J., Towards Robust and Hidden Image Copyright Labeling, IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, 20-22 June, 1995.
- [4] Miao N., He Y., Dong J., hymnMark: Towards Efficient Digital Watermarking on Android Smartphones, Worldcomp-Proceedings, <http://worldcomp-proceedings.com/proc/p2012/ICW6177.pdf> (Ziyaret tarihi: 30 Haziran 2014).
- [5] Jassim, T., Abd-Alhameed, R., Al-Ahmad, H. (2013, February). A new robust and fragile watermarking scheme for images captured by mobile phone cameras. In Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, 12-14 February, 2013.
- [6] Chen, Y. H., Huang, H. C., A Copyright Information Embedding System for Android Platform, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference, Dalian, 14-16 Oct, 2011.
- [7] URL-1: [http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj681687\(v=vs.105\).aspx](http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj681687(v=vs.105).aspx), (Ziyaret tarihi: 30 Haziran 2014).
- [8] Jain, A.K., Fundamentals of Digital Image Processing, Englewood Cliffs, Editor: Colleen Brosnan, NJ, Prentice Hall, 150-153, 1989.
- [9] Yeşilyurt, M., Özcerit, A. T., Yalman, Y., & Ertürk, İ. Sayısal İmgeler için Ayrık Kosinüs Dönüşümü Esaslı Veri Gizlemenin Ataklara Dayanıklılığı, Akademik Bilişim Konferansı, Uşak, 1-3 Şubat, 2012
- [10] Ichigaya A., Kurozumi M., Hara N., Nishida Y., Nakasu E., A method of estimating coding PSNR using quantized DCT coefficients, Circuits and Systems for Video Technology, IEEE Transactions on, 2006, 16(2), 251-259.
- [11] SooKim H., TaePark K., Fast DCT algorithm with fewer multiplication stages, Electronics Letters, 1998, 34(8), 723-724.

A.UÇAR 1988 yılında Malatya'da doğdu. 2005 yılında Alanya lisesinden mezun oldu. 2010 yılında Süleyman Demirel Üniversitesi Elektronik Bilgisayar Eğitimi'nde lisans eğitimi tamamladı. 2014 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği anabilimdalında yüksek lisans eğitimi tamamladı. Genel çalışma alanları: Görüntü işleme ve insan bilgisayar etkileşimi

Y.BECERİKLİ 1991 yılında Yıldız Teknik Üniversitesi Elektronik Haberleşme Mühendisliği bölümünde lisans eğitimi tamamladı. İstanbul Teknik Üniversitesi Elektronik Haberleşme Mühendisliği'nde 1994 yılında yüksek lisansını tamamladı. 1998 yılında Sakarya Üniversitesi Elektrik-Elektronik Mühendisliği anabilimdalında doktora eğitimi tamamladı. 1992-2000 yılları arası Sakarya Üniversitesinde Araştırma Görevlisi, 2000-2005 yılları arası Kocaeli Üniversitesi Bilgisayar Mühendisliği bölümünde Yardımcı Doçent, 2005-2011 yılları arası Kocaeli Üniversitesi Bilgisayar Mühendisliği bölümünde Doçent ünvanı ile çalıştı. 2011 yılından itibaren Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümünde Profesör olarak öğretim üyeliğine devam etmektedir. Aynı zamanda 2013 yılından beri Yalova Üniversitesi Bilgisayar Mühendisliği bölümünde yarı zamanlı olarak öğretim üyeliği görevini yürütmektedir. Genel çalışma alanları: Akıllı sistemler ve kontrol, optimal kontrol, sinyal ve görüntü işleme, dalgacık ağları, stokastik süreç kontrolü, optimizasyon teorisi. Dergi hakemlikleri, IEEE Transactions on Neural Networks, IEEE Transactions on Fuzzy Systems, IEEE Control System Technology, IEEE Trans. on Signal Processing, IEEE Transactions on Systems, Man, and Cybernetics-Part C, ASME Journal of Dynamic Systems, Measurement, and Control, AIP Chaos, The Mediterranean Journal of Measurement and Control, Computers and Electrical Engineering (Elsevier), The Canadian Journal of Chemical Engineering, IEE Proc. Vision, Image & Signal Processing, ISA Transactions, Advances in Engineering Software, Journal of Intelligent & Fuzzy Systems, Circuits, Systems & Signal Processing, Digital Signal Processing and MECHANICAL SYSTEMS AND SIGNAL PROCESSING. (Home page: <http://bilgisayar.kocaeli.edu.tr/ybecerikli>)



Recommendations on Future Operational Environments' Command Control and Cyber Security

K. Goztepe

Abstract—It is a well-known fact that today a nation's telecommunication networks, critical infrastructure, and information systems are vulnerable to growing number of attacks in cyberspace. Cyber space contains very different problems involving various sets of threats, targets and costs. Cyber security is not only problem of banking, communication or transportation. It also threatens core systems of army as command control. Some significant recommendations on command control (C2) and cyber security have been suggested for army computing environment in this paper. This study addresses priorities of “what should be done for a better army cyber future” to cyber security researchers.

Index Terms—Command Control (C2), Army, Future Operations, Cyber Security.

I. INTRODUCTION

INITIALLY, wars were conducted via physical instruments and signs like whistles or flags. Especially with the usage of telegraph in Crimean War [1] in the 19th century, remote command and control (C2) became possible. The rapid development of the instruments like satellites [2] within the space dimension increased the range of C2, while the improvement of ground positioning systems [3] increased the precision of C2, and lastly computers and internet increased the obscurity of C2.[4]

Although the C2 instruments have changed through the history [5], its crucial role in warfare has kept its importance; it is a necessity to have sheltered, mobile, and modern C2 centers, while it is indispensable to train the leaders to effectively put to use this capability [6].

The more electronics and mobile devices are improved the more the air, land, sea, and space become cyber environments [7]. The cyber security became a state issue, where a cyber-threat for a security system of a state is accepted as a *casus belli*. Cyber-attack has been defined as “an attack, via cyberspace, targeting an enterprise's use of cyberspace for the

purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information” by National Institute of Standards and Technology (NIST) [8]. Besides the cyber defense and cyber-attack capability has also gained importance; however, there is no sufficient legal basis for such an operation [9]. That is why, states focus on identifying the imminent threat and staving it off by state-sponsored (non-state) cyber-attacks, instead of directly applying it.

II. WHAT SHOULD BE DONE FOR A BETTER CYBER FUTURE?

A. Purpose of the Study

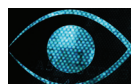
Complexity of modern cyber security is increasing all over the world. Today it is a fact that manage cyber threats and cyber incidents without leveraging various collaboration instruments with different partners is not possible. Cyber-attacks constitute a serious challenge to national security and demand greater attention from all public and civil establishments. This study mention main topics about cyber security especially for army. The main issues needed to be done in terms of future operational environments' command control and cyber security are given below.

B. Main Issues for Cyber Security

Interoperability is a fundamental principle for the operation of joint and coalition forces (Fig.1). Army should have the capability to operate in any place of the world with the ability of “interoperability for joint and coalition operations”. It is also crucial that the joint situational picture of the operational area be presented to joint headquarters. Additionally, cross-functional structure among the systems should be formed, and centralized C2 systems should be transformed to decentralized C2 systems.

It is a necessity to introduce programs about cyber security in the universities and to encourage the education of qualified individuals about it. The purpose of the cyber exercises held by armies or scientific centers, should be to create awareness. The situational awareness will not be sufficient in future's sophisticated and ambiguous environment. In order to provide all of the functional areas in a C2 headquarters work jointly, situational awareness should be improved by detecting the

Kerim Goztepe, IE, Ph.D. War Colleges Command, Army War College, Dept. of Operations & Intelligence, Yenilevent, 34330, Pbx: +90 212 398-0100/3262, Istanbul-Turkey, e-mail: kerimgoztepe@gmail.com.



RECOMMENDATIONS ON FUTURE OPERATIONAL ENVIRONMENTS' COMMAND CONTROL.....

factors in the environment, apprehending the current situation, and envisaging the future situation (tendency awareness).

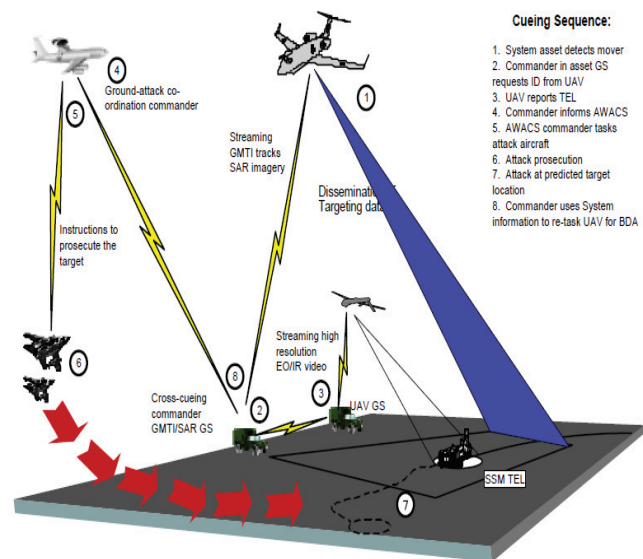


Fig.1. Interoperability [10]

The armies will increase their Network Enabled Capabilities (NEC) in order to eradicate the obscurity of the chaotic future warfare environments, and to provide right information, in the right time, and in the right place (Fig.2) [10]. However, the more the NEC improved, the more the systems/platforms will be exposed to cyber-attacks. 'Embedded Cyber Security Technique' and 'Operational Area Identification and Introduction Systems' [11] should be used to restrain from those attacks.

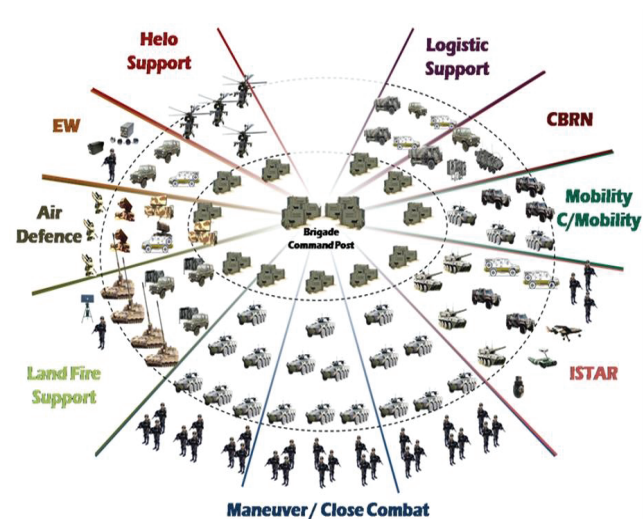


Fig. 2. Army network enabled capability [10]

It is of high importance that an Army, which has mission functions that entails different C2 structures, must have the capability to conduct via a single and centralized C2 system. In addition to this, special weaponry systems for army should be compatible for a sophisticated C2. Today the C2 systems in

army, depends on software and hardware, which are open to cyber-attacks. Thus, 'National Tactic Data Link' is necessary for securing the systems.

Internet search engines are the most sophisticated spy software of the world, since they store all of the data about the users and draw the data map of the world [12]. They can provide the educational levels of the countries, the contacts of the individuals, their social circles, and expenses (Fig.3). This capability renders those engines as the indispensable environment for intelligence that is able to analyze so much data. In order to preserve from the threats of that capability, it is vital to use complicated passwords and to use these systems quantum sufficit.

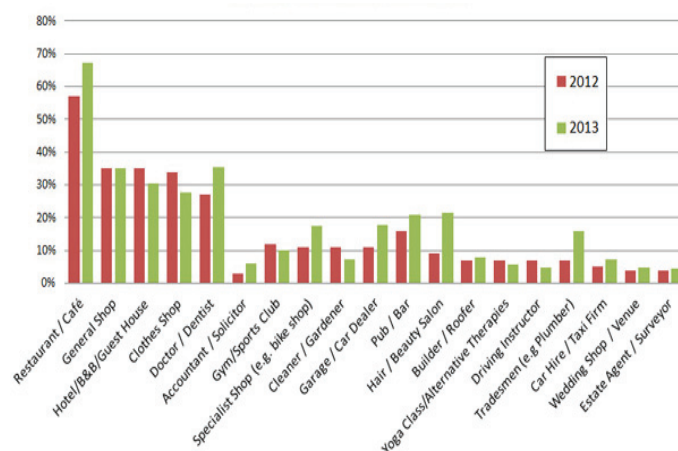


Fig. 3. Search engine usage sample [13]

Depending on the last developments on Cryptology, authentication, access control (for 2 or more people), authorization, strong authentication mechanisms, fast and low-source-spending crypto algorithms, asymmetric crypto algorithms resistant to quantum computers (rather than symmetric crypto) should be used in order to provide data security of the NEC systems. It is known that trying to secure all kinds of data may decrease the effectiveness of the systems or put systems out of action. Thus, it is essential that, which data is worth security, be decided effectively. Instead of commencing the crisis and operations process with intelligence function and following with operation function, the process should be defined from the crisis phase cross functionally and jointly.

Network enabled capability gains the upper hand. In order to make use of this capability, it is vital to have communications networks that enable current systems, platforms, and nodal points function together. Additionally, information and nodal systems are required to process the data and prepare it compatible with the users' needs. Moreover, an organization structure and a training system (of the users and the decision makers) that effectively profits from the network-enabled capability are indispensable.

RECOMMENDATIONS ON FUTURE OPERATIONAL ENVIRONMENTS' COMMAND CONTROL.....

C. Command Control and Tactical Issues

In the near future, robotic armies and unmanned land vehicles will be under command, and most of the platforms/systems will depend on satellites. In order to remove weaknesses stemming from satellite signal intervention, a 'National GPS System' is vital. By using national GPS system Decision Support Systems may provide alternative solutions about deployment of artillery weapons and weapon systems, ammunition effect analysis, desired effect, the sort and amount of the ammunition. Metro techniques affect hit rate % 67 percent in the long-range. In this regard, service-based metro systems will be widespread. It is possible to take better decisions than the previous ones, and artificial intelligence systems may be helpful for understanding the intention/course of action of the enemy using Learning Systems.

'Vetronics' systems were introduced with the developments in the land vehicles (Fig.4) [14],[15]. In the middle of the battle, if the commander needs to change his vehicle due to mechanic problems, he will have the capability to use the new vehicle as a command and control vehicle with the help of 'mountable systems' [16].

With the help of tactic wireless net communication system applications, all of the forces, particularly Navy, will have the capability to communicate worldwide securely, based on completely national means.

Studies and researches are in progress on the use of 'Service Based Architecture' by the mobile elements on the field and on the tactical field communication nets. It is predictable that service based architecture will be used on a broader band in between command centers over brigade level in the short and medium term. The C2 systems situational awareness will be available for the single soldier on the field as well as the high level command, parallel to the technologic developments, and functional capabilities will increase with that. Identification system is as important as detection system on the unmanned aerial vehicles, in that context, by help of Terahertz technology, which follows the terahertz rays that objects radiate, the identification of the weapons, explosive, chemical, and biological materials and similar security inspections will be available.

It is possible to use network enabled capability in strategic, operative, and tactic levels; however, it will be difficult to use it in single soldier / single vehicle level regarding the hardships of the combat. Thus, it is vital to define the levels that network enabled capabilities are planned to operate.

With the help of a data exchange system, different platforms should have the ability to activate the weapon systems of each other. Most of the systems in army are compatible with platform-based operation, rather than network enabled ones, which may cause problems in the long run.

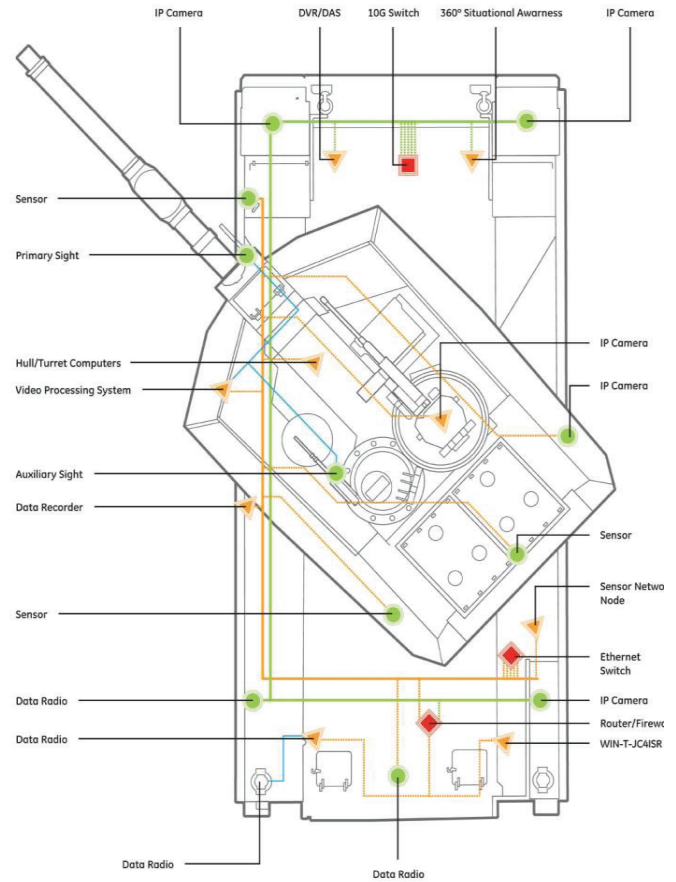


Fig. 4. Vetronics for a main battle tank [17]

III. CONCLUSION

Recommendations on future operational environments' command control and cyber security has been discussed in this paper. The studies' goal is to make curious researchers some main topics about army and cyber security issues.

It is known that in order to form a new effective defense technology base, focused on the needs of army, long term planning, application, and tracking activities should be handled with strategic management approach [18],[19]. In this context, regarding command, control and information technologies excellence nets C4ISR technologies, which are compatible with network centric capability, should be prioritized. Autonomous command and control technologies in land, navy and air force vehicles, real time data integration and data fusion, cyber defense, strategy and tactics improvement, protected core, and national nets should also be prioritized.

It is fundamental that national software and hardware be used in order to be secure from or least affected from threats. Human-education-technology synergy be provided for a sufficient cyber defense, and that a national cyber army and a cyber-defense supreme board be formed. It is also important to

RECOMMENDATIONS ON FUTURE OPERATIONAL ENVIRONMENTS' COMMAND CONTROL.....

promote a cyber-market while improving the research & development about cyber security.

One of the fundamental concept in battlefield environment is information flow and security of obtained information. It is well known fact by cyber experts that physical components added to a cyber-system considerably increase the difficulty of determining information flow.

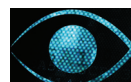
Today's armies have sophisticated command control infrastructures includes complex interactions of cyber components. Confidentiality of operational environment requires advanced security integration models. I believe that this work provides an approach for some of the complexities involved in command control and cyber security protection for army.

REFERENCES

- [1] A. D. Lambert, The Crimean War: British Grand Strategy Against Russia, 1853-56. Ashgate Publishing, Ltd., 2011.
- [2] N. Celandroni, F. Erina, G. Alberto, O. Gabriele, R. Cesare, L. Michele, B. Igor. "A survey of architectures and scenarios in satellite-based wireless sensor networks: system design aspects." International Journal of Satellite Communications and Networking, 31(1), 2013, pp. 1-38.
- [3] J. Rantakokko, R. Joakim, S. Peter, H. Peter, C. Jonas, T. David, G. Fredrik, J. Magnus, and G. Mathias, "Accurate and reliable soldier and first responder indoor positioning: multisensor systems and cooperative localization." Wireless Communications, IEEE 18, no. 2, 2011, pp. 10-18.
- [4] S.D. Meinrath, L. James, and L. Benjamin. "A Growing Digital Divide: Internet Freedom and the Negative Impact of Command-and-Control Networking." IEEE internet computing 15, no. 4, 2011, pp. 75-79.
- [5] J. Erickson, The Soviet High Command: a Military-political History 1918-1941: Vol. 3. Routledge, 2013.
- [6] D.S. Alberts, and E.H. Richard. Power to the edge: Command control. in the information age. Office of the Assistant Secretary Of Defense Washington Dc Command and Control Research Program (CCRP), 2003.
- [7] S.K. Das, "Pervasive computing vs. cyber-physical systems: A perspective from smart environments." In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on, 2012, pp. 105-105.
- [8] R. Kissel (Ed.). (2011). Glossary of key information security terms, DIANE Publishing, National Institute of Standards and Technology (NIST), 2011
- [9] F. Cohen, "Simulating cyber-attacks, defences, and consequences." Computers & Security 18, No. 6, 1999, pp. 479-518.
- [10] NATO Interoperability, <http://publicintelligence.net/nato-interoperable-istar-system-concept-of-employment/>
- [11] J. Andress, and S. Winterfeld. Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier, 2011.
- [12] Technology News, <http://c4i-technology-news.blogspot.com.tr/2011/10/forza-nec-moves-on.html>, access time, July, 2014
- [13] W. Mettrop, and P. Nieuwenhuysen. "Internet search engines—fluctuations in document accessibility." Journal of Documentation 57, no. 5, 2001, pp. 623-651.
- [14] Local Consumer Review Survey 2013, <http://www.brightlocal.com/2013/06/25/local-consumer-review-survey-2013/>, access time, July, 2014.
- [15] D. Abdulmasih, P. I. Oikonomidis, R. Annis, P. Charchalakis, and E. Stipidis. "In-vehicle monitoring and management for military vehicles' integrated vetronics architectures." Journal of Systems Architecture, 60, no. 4, 2014, pp.405-418.
- [16] A. Deshpande, "Vetronics systems integration: survivability strategies for future modular vetronics architectures." PhD diss., University of Brighton, 2013.
- [17] Vetronics Architectures <http://eecatalog.com/vme/2012/02/02/vetronics-architectures-emerge-to-facilitate-network-enabled-operations/>, access time, 2014.
- [18] K. Goztepe, I. Cehreli, S. E. Sensoy, A Decision Framework for Combat Cloud Computing Strategy. 6th International Information Security & Cryptology Conference, 2013.
- [19] K. Goztepe, Designing Fuzzy Rule Based Expert System for Cyber Security. International Journal of Information Security Science, 1(1), 2012, pp. 13-19.



Dr. Kerim Goztepe received the B.S.degree in System Engineering from Turkish Military Academy in 1998. He was accepted in Marmara University and received M.S. degree in Engineering Management in 2003. He started doctoral education in Industrial Engineering, Institute of Science and Technology at Sakarya University and graduated in 2010. He is interested in fuzzy logic, neural network, multicriteria decision making and cyber security for open source systems. Dr. Kerim Goztepe is an author of more than thirty refereed papers, and editor-in-chief of "Journal of Military and Information Science".



RGB Görüntülerin Bit Değişimi ve Ripplet-I Dönüşümü Tabanlı Şifreleme ile Filigranlanması

H. Yaşar, M. Ceylan

Özet—Bu çalışmada ikili sayı formatında gizli görüntüler ve 24 bit RGB formatında taşıyıcı görüntüler kullanılarak bir filigranlama uygulaması gerçekleştirilmiştir. Filigranlama, bit değişimi ile taşıyıcı görüntünün yeşil renk uzayı üzerinde yapılmıştır. Gizli görüntüler, Ripplet-I dönüşümü tabanlı şifreleme algoritması ile şifrelenmiştir. Üç adet taşıyıcı görüntü ve iki adet gizli görüntü kullanılarak yapılan çalışmada görüntüler arasındaki değişimleri ölçmek amacıyla tepe sinyal gürültü oranı (TSGO) kullanılmıştır.

Anahtar Kelimeler—Rippet-I dönüşümü, görüntü şifreleme, filigranlama, tepe sinyal gürültü oranı (TSGO)

Abstract—In this study, a watermarking application is made using secret images in binary format and host images in 24 bits RGB format. This watermarking is made with bite by exchange the green space of the host images. The secret images are encrypted with a algorithm based Ripplet-I transform. In this study that is made by using three host images and two secret images, peak signal-to-noise ratio (PSNR) is used in order to measure the changes between the images.

Index Terms—Ripplet-I transform, image encryption, watermarking, peak signal to noise ratio (PSNR)

I. GİRİŞ

Kriptolama kökenleri çok eski tarihlere dayanan kapsamlı bir çalışma alanıdır. Özellikle bilgi güvenliği sağlamak amacıyla askeri alanda yaygın şekilde kullanılmaktadır. Yakın zamana kadar çoğunlukla metinler üzerine uygulanan kriptolama teknikleri, sinyallerin hayatımıza yaygın olarak girmesi ile bu alanda da kullanılmaya başlanmıştır.

Görüntülerin kriptolanması üzerine çok çeşitli yöntemler ortaya atılmıştır. 1999 yılında Guo ve Yen [1] aynalama benzeri bir sistem ile görüntü şifrelemesi gerçekleştirmiştir. Yer değiştirme permutasyonu kategorisinde yer alan bu yöntemde karmaşık yapılı sistemden üretilen ikili sayı formatındaki diziye bağlı olarak görüntü pikselleri karıştırılmaktadır. Yine Gou ve Yen tarafından yapılan bir başka çalışmada ise [2] karmaşık yapılı görüntü şifreleme

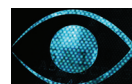
algoritması oluşturulmuştur. Bu algorithmda karmaşık yapılı sisteme dayalı kaotik dizi üretilmektedir. Bu dizi, başka bağlı bir dizinin oluşturulmasında kullanılır. Yeni oluşturulan diziye bağlı olarak görüntünün pikselleri yeniden düzenlenmektedir. 2000 yılında Chang ve arkadaşları [3] tarafından vektör kuantalamaya dayalı görüntü şifreleme yapılmıştır. Bu teori temel olarak; görüntü sıkıştırmadaki en iyi performansın her zaman sabitlerin yerine görüntü özelliklerinin kodlanmasıyla elde edilebileceğini belirten Shannon'un oran-bozulma teorisinden türetilmiştir. 2001 yılında Maniccam ve Bourbakis [4], SCAN dili ile görüntü şifreleme üzerine çalışmıştır. Bu çalışmada daha önce ortaya konan SCAN dili ile şifrelemenin bazı eksiklikleri giderilerek görüntülerde kayıpsız sıkıştırma ve şifreleme yapılmıştır.

Görüntüler üzerinde şifreleme çalışmalarının yaygınlaşması filigranlama çalışmalarına temel oluşturmuştur. 2000' li yıllardan itibaren görüntülerde filigranlama konusu üzerinde çok yoğun çalışılan bir alan haline gelmiştir. Bu çalışmaların çeşitlenmesinde gizli ve taşıyıcı görüntülerin boyutları ve formatları etkili olmuştur. Kırmızı, mavi ve yeşil olmak üzere ayrı ayrı görüntü temsil kabiliyeti bulunan 3 renk uzayına sahip olması sebebiyle 24 bit derinlikli RGB formatındaki görüntüler taşıyıcı görüntü olarak filigranlama işlemlerini kolaylaştırıcı bir yapıya sahiptir. Gizli görüntülerin ikili sayı formatında olması ise daha kolay ve gizli görüntülerin yeniden elde edilmesinde daha az kayıp ile filigranlama yapılmasını sağlamaktadır. Bu sebeple literatürde 24 bit derinlikli RGB formatındaki taşıyıcı görüntüler ve ikili sayı formatındaki gizli görüntülerin kullanıldığı çok sayıda filigranlama çalışması gerçekleştirilmiştir.

2001 yılında Yu ve arkadaşları tarafından [5] sinir ağını temel alan bir filigranlama çalışması yapılmıştır. 2004 yılında Tsai ve arkadaşları [6] tarafından gerçekleştirilen çalışmada ise renk nicemleme kullanılmıştır. Bu çalışmada gizli görüntüler, veri şifreleme standartları (DES) ile şifrelenmiştir. Shen ve arkadaşları [7] tarafından 2005 yılında yapılan başka bir filigranlama çalışmasında destek vektör regresyondan yararlanılmıştır. Bu çalışmada 4 adet taşıyıcı görüntü kullanılmış ve 1 adet taşıyıcı görüntü için sonuçlar verilmiştir. Aynı yıl Ni ve arkadaşları [8] filigranlama için yinelemeli haritalama kullanmışlardır.

2007 yılında Mostefa ve Khamadja [9] görüntüye ait kırmızı, mavi, yeşil uzaylar (RGB) ve ton, doygunluk, parlaklık uzayları (HSV) arasındaki benzerliklerin değiştirilmesine dayalı yeni bir filigranlama algoritması

Hüseyin Yaşar, Selçuk Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik A.B.D. Yüksek Lisans Öğrencisi, mihendise@gmail.com
Yrd. Doç. Dr. Murat Ceylan, Selçuk Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği Öğretim Üyesi, mceylan@selcuk.edu.tr



geliştirmişlerdir. Aynı yıl Tsai ve Sun [10] tarafından yapılan başka bir çalışmada destek vektör makinesi kullanılmıştır. Kuo ve Cheng [11] tarafından temel eksen analizi kullanılarak yapılan filigranlama çalışması ise 6 adet taşıyıcı görüntü ile test edilmiştir.

2008 yılında Santhi ve arkadaşları [12] tarafından gerçekleştirilen çalışmada ayırık dalgacık dönüşümü, ayırık kosünüs dönüşümü, tekil değer ayrışımı kullanılarak hibrit bir algoritma geliştirilmiştir. Aynı yıl Fu ve Shen [13] doğrusal diskriminant analizi kullanarak filigranlama yapmıştır.

2009 yılında Gindy ve arkadaşları tarafından ayırık kosünüs dönüşümü ve yeşil renk uzayı [14, 15] kullanılarak iki filigranlama çalışması yapılmıştır. Bu çalışmalarda kullanılan gizli ve taşıyıcı görüntüler aynıdır. Mohanty [16] tarafından geliştirilen filigranlama algoritması ile 97 - 108 dB arasında değişen tepe sinyal gürültü oranı (TSGO) elde edilmiştir. RGB formatındaki taşıyıcı görüntülerin YCbCr formatına çevrilerek işlendiği çalışmada Lv ve arkadaşları [17] destek vektör regresyon kullanmışlardır. Lai ve Wu [18] tarafından çok ölçekli blok eşleştirme yöntemi kullanılarak yapılan filigranlama çalışması 8 adet taşıyıcı görüntü ile test edilmiştir.

2010 yılında Hu ve arkadaşları [19], karmaşık yapılı bir filigranlama algoritması geliştirmiştir. Ayrıca Fındık ve arkadaşları [20], parçacık sürü optimizasyonu ve k-en yakın komşu yöntemlerine dayanan çalışmada 3 adet taşıyıcı görüntü kullanmıştır. Yine aynı yıl Hui-qin ve arkadaşları [21] Arnold dönüşümünü kullanarak filigranlama yapmıştır. Pei ve arkadaşlarının [22] yaptığı başka bir çalışmada tekil değer

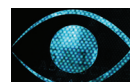
ayrışımı kullanılmıştır. Behnia ve arkadaşları [23] tarafından geliştirilen ve karmaşık haritalama kullanılarak yapılan başka bir çalışmada ise 3 farklı ikili sayı formatındaki gizli görüntü, 1 adet taşıyıcı görüntünün 3 farklı renk (kırmızı, yeşil, mavi) uzayına filigranlanmıştır. 2011 yılında Fındık ve arkadaşları [24] tarafından yapay bağışıklık tanıma sistemine dayalı filigranlama çalışması yapılmıştır. Aynı yıl Niu ve arkadaşları [25] tarafından yapılan filigranlama çalışmasında ise örneklemesiz contourlet dönüşümü kullanılmıştır. 2012 yılında Dang ve Kinsner tarafından [26] dalgacık dönüşümü ve yapay sinir ağlarını temel alan bir filigranlama çalışması yapılmıştır. Yine aynı yıl Vahedi ve arkadaşları [27] genetik algoritmali optimizasyon tekniklerinden yararlanmışlardır.

2013 yılında Moghaddam ve Nemati [28] 3 adet taşıyıcı görüntü üzerinde geliştirilmiş yayılmacı rekabet algoritması kullanmışlardır. Zhu ve arkadaşları [29] filigranlama için RGB taşıyıcı görüntülerin kırmızı ve yeşil renk uzaylarını kullanmışlar ve gizli görüntüleri veri şifreleme standartları (DES) ile şifrelemişlerdir.

Yapılan çalışma sonuçlarının birbiri ile karşılaştırılmasında çalışmalarda kullanılan taşıyıcı ve gizli görüntüler ile görüntü boyutları önemlidir. Literatür çalışmalarında filigranlama konusunda ortak bir görüntü veritabanı oluşturulamamıştır. Çalışmalarda kullanılan taşıyıcı görüntüler, taşıyıcı görüntü boyutları, gizli görüntü boyutları ve çalışma sonucunda elde edilen TSGO değerleri hakkındaki ayrıntılı bilgiler Tablo I' de verilmiştir.

TABLE I
LİTERATÜR ÇALIŞMALARINDA KULLANILAN GÖRÜNTÜLER VE ÇALIŞMA SONUÇLARINA AİT BİLGİLER

Çalışma	Taşıyıcı Görüntü	Taşıyıcı Görüntü Boyutu	Gizli Görüntü Boyutu	TSGO (dB)
Yu ve ark. [5]	Lena, Baboon	480 × 512	32 × 32	46.097 - 45.924
Tsai ve ark. [6]	Lena, Airplane, Baboon, House, Peppers, Sailboat	512 × 512	64 × 64 128 × 128	31.6947 - 38.6624
Shen ve ark. [7]	Lena, Plane, Baboon, Peppers	512 × 512	35 × 25	41.23
Ni ve ark. [8]	Plane	512 × 512	64 × 64	44.9029
Mostefa ve Khamadja [9]	Lena, Peppers, Mandrill, Flower	512 × 512 640 × 480	----	41.91 - 47.02
Tsai ve Sun [10]	Lena, Baboon, F16	512 × 512	64 × 64	41.5267 - 38.7774
Kuo ve Cheng [11]	Lena, Baboon, House, Peppers, Sailboat, Airplane	512 × 512	64 × 64	39.8102 - 47.3769
Santhi ve ark. [12]	Lena	512 × 512	64 × 64	26.7912
Fu ve Shen [13]	Lena, Baboon, F16	512 × 512	35 × 25	41.25 - 41.52
Gindy ve ark. [14]	Lena	512 × 512	96 × 64	57.5
Gindy ve ark. [15]	Lena	512 × 512	96 × 64	58.4
Mohanty [16]	Lena, Mig21, F16, Mandril, Pepper	256 × 256	----	97 - 108
Lv ve ark. [17]	Lena, Baboon, Peppers	512 × 512	32 × 32	46.7975 - 47.3500
Lai ve Wu [18]	F16, House, Lake, Lena, Peppers, Splash, Tiffany, Tree	512 × 512	----	36.88 - 40.83
Hu ve ark. [19]	Lena	512 × 512	60 × 60	43.5
Fındık ve ark. [20]	Baboon, F16, Lena	512 × 512	64 × 64	39.63 - 42.76
Hui-qin ve ark. [21]	Lena	256 × 256	64 × 64	63.246
Pei ve ark. [22]	Peppers	256 × 256	128 × 128	31.4249
Behnia ve ark. [23]	Madineh	512 × 512	128 × 128	30.11
Fındık ve ark. [24]	Baboon, Lena	510 × 510	32 × 32	41.83 - 42.76
Niu ve ark. [25]	Baboon, Lena, Mandrill	512 × 512	32 × 32	40.57 - 41.67
Dang ve Kinsner [26]	Baboon, Lena, Airplane-F16, House	512 × 512	64 × 64	42.9
Vahedi ve ark. [27]	Baboon, Lena, Mandrill	512 × 512	64 × 64	39.2722 - 41.7428
Moghaddam ve Nemati [28]	Baboon, Lena, F16	512 × 512	64 × 64	43.8422 - 45.6295
Zhu ve ark. [29]	Lena	960 × 960	120 × 120	36.7365



II. METOD

A. Ripplet-I Dönüşümü ve Alt Şifreleme Görüntüsü

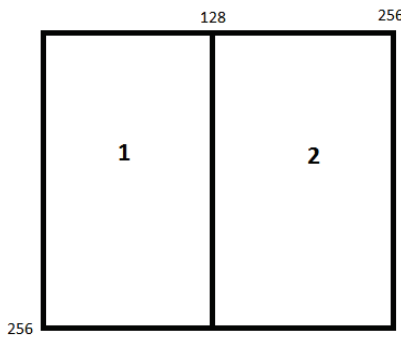
Curvelet dönüşümü 1999 yılında Candes ve Donoho [30] tarafından ortaya atılmıştır. Çok yaygın bir etki yaratan Curvelet dönüşümü bir çok görüntü işleme uygulamasında sıklıkla kullanılmıştır. 2010 yılında Xu ve arkadaşları [31] tarafından destek (c) ve derece (d) parametreleri eklenerek Curvelet dönüşümü geliştirilmiş ve Ripplet-I dönüşümü tanımlanmıştır. Ripplet-I dönüşümü polar koordinatlarda a ölçek parametresi olmak üzere Eşitlik (1)'de verilen şekilde tanımlanır. Bu eşitlik $c=1$, $d=2$ değerleri için Curvelet dönüşümünü ifade etmektedir.

$$\hat{\rho}_\theta(r, w) = \frac{1}{\sqrt{c}} a^{\frac{1+d}{2d}} W(a.r) V\left(\frac{a^{\frac{1}{d}}}{c.a} . w\right) \quad (1)$$

Görüntü işleme uygulamalarında dönüşümün ayrık versiyonu kullanılmakta olup ayrık Ripplet-I katsayıları Eşitlik (2)'de verildiği şekilde hesaplanır.

$$R_{j,\vec{k}} = \sum_{n_1=0}^{M-1} \sum_{n_2=0}^{N-1} f(n_1, n_2) \cdot \overline{\rho_{j,\vec{k}}(n_1, n_2)} \quad (2)$$

Bu çalışmada $c=1$, $d=3$ değerleri için taşıyıcı görüntünün mavi renk uzayı üzerinden ayrık Ripplet-I dönüşümü kullanılarak ayrık Ripplet-I katsayıları elde edilmiştir. Elde edilen katsayı grubu içinden 2 adet 128×256 boyutunda ki katsayı hücresi işlemlerde kullanılmıştır. Katsayı matrislerinin mutlak değerleri alınmış ve ayrı ayrı matrislere ait ortalama değerler hesaplanmıştır. Matris elemanları matrisin ortalama değerine bölünerek normalizasyon işlemi gerçekleştirilmiştir. Elde edilen matrisler en yakın sayıya yuvarlanarak Şekil 1'de verildiği şekilde dizilmiş ve 256×256 boyutundaki alt şifreleme görüntüsü oluşturulmuştur. Bu çalışmada gizli görüntülerin boyutu 256×256 olduğu için alt şifreleme görüntüsünün boyutları bu şekilde oluşturulmuştur. Ayrık Ripplet-I katsayıları ile farklı boyutta ve yerleşimde alt şifreleme görüntü matrisi üretmek de mümkündür.

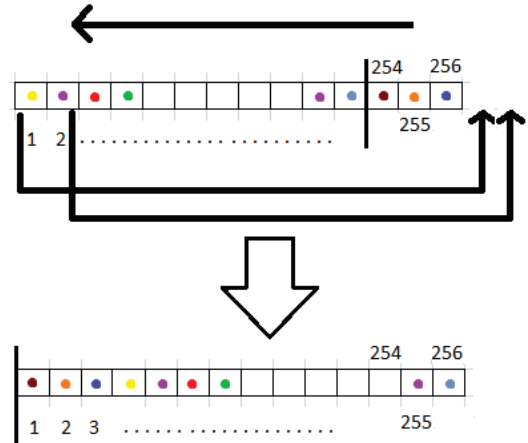


Şekil 1. Ayrık Ripplet-I katsayı matrislerinin dizilimi ($c=1$, $d=3$, fltname1=9/7, fltname2=pkva, 1=C {4} {1}, 2=C {4} {2})

B. Şifreleme Algoritması

Guo ve Yen [1, 2] tarafından görüntü özellikleri kullanılarak piksel yer değişikliği ile bağlı şifreleme yapılmıştır. Bu çalışmada piksel yer değişikliği için statik özellikler yerine görüntü üzerinden elde edilen özelliklerin kullanılmasının şifreleme işlemini daha karmaşık hale getirdiği görülmüştür.

Bu çalışmada görüntü özellikleri kullanılarak piksellerin yerlerinin değiştirilmesi suretiyle ön şifreleme yapan bir algoritma oluşturulmuştur. Çalışmada gizli görüntüler ikili sayı formatında olup iki boyutludur. Buna göre gizli görüntünün herhangi bir matris hücresi "0" veya "1" olmak üzere iki değer alabilir. Bu durumda gizli görüntü matrisinin herhangi bir satırı boyunca matris hücre değerlerinin toplamı "0" ile "satır uzunluk değeri" arasında olmak zorundadır. Bu durum sütunlar için de geçerlidir. Ön şifreleme algoritmasında bu durumdan hareketle öncelikle satır düzeyinde her satır kendi satırındaki matris hücrelerinin toplamına eşdeğer basamak kadar sola kaydırılmıştır. Burada satır başının satır sonundan devam ettiği kabul edilmiştir. Sırasıyla bütün satırlar için aynı işlemin tamamlanmasının ardından sütunlar aynı yöntemle yukarı yönlü olarak kaydırılmıştır. Şekil 2, yapılan bu işlemi satır düzeyi için göstermektedir.

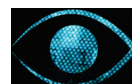


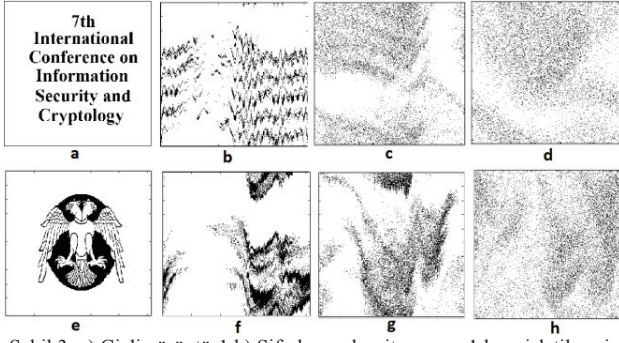
Şekil 2. Piksel kaydırma işlemi
(satıra ait piksel değerlerinin toplamı 253 olması durumunda)

Bu şifreleme algoritması kısaca şu şekilde özetlenebilir.

- 1) $M \times N$ boyutundaki görüntünün 1.satırındaki matris hücresi değerlerini topla.
- 2) Satırı, toplama eşdeğer basamak kadar sola (satır başı satır sonundan devam eder) kaydır.
- 3) 1-2 basamakları M adet satır için tekrarla.
- 4) $M \times N$ boyutundaki görüntünün 1. sütunundaki matris hücresi değerlerini topla.
- 5) Sütunu, toplama eşdeğer basamak kadar yukarı (sütun başı sütun sonundan devam eder) kaydır.
- 6) 4-5 basamakları N adet sütun için tekrarla.

Ön şifreleme algoritması arka arkaya birden çok kez tekrarlanabilir. Şekil 3'de çalışmada kullanılan iki adet gizli görüntü ve şifreleme algoritmasının 1, 5 ve 20 kez çalıştırılması ile elde edilen görüntüler verilmiştir. Bu algoritmanın tersine işletilmesi ile gizli görüntüler tam doğrulukla yeniden elde edilebilir.





Şekil 3. a) Gizli görüntü-1 b) Şifreleme algoritmasının 1 kere işletilmesi sonucu oluşan görüntü c) Şifreleme algoritmasının 5 kere işletilmesi sonucu oluşan görüntü d) Şifreleme algoritmasının 20 kere işletilmesi sonucu oluşan görüntü e) Gizli görüntü-2 f) Şifreleme algoritmasının 1 kere işletilmesi sonucu oluşan görüntü g) Şifreleme algoritmasının 5 kere işletilmesi sonucu oluşan görüntü h) Şifreleme algoritmasının 20 kere işletilmesi sonucu oluşan görüntü

Çalışmada bu aşamadan sonra ön şifreleme yapılmış gizli görüntünün, alt şifreleme görüntü matrisi referans alınarak tekrar şifrelenmesi gerçekleştirilecektir. Alt şifreleme görüntü matrisi oluşturulmasının amacı ön şifrelemede olduğu gibi statik özellikler yerine görüntü üzerinden elde edilen özelliklerin kullanılmasıdır. Alt şifreleme görüntü matrisi Ripplet-I dönüşümü ile elde edilebileceği gibi başka özellik çıkarma yöntemleri ile de oluşturulabilir. Ancak bu çalışmada giriş parametre sayısının fazla olmasının şifreleme güvenliğini artıracığı düşünüldükçe Ripplet-I dönüşümü tercih edilmiştir.

Alt şifreleme matrisi $f(i,k)$, gizli görüntü matrisi $g(i,k)$, sonuç matrisi $l(i,k)$ olmak üzere şifreleme işlemi eşitlik (3)' de tanımlanmıştır.

$$l(i,k) = \begin{cases} g(i,k), f(i,k) = 2m+1, m \in \{0,1,2,\dots\} \\ g(i,k), f(i,k) = 2m, m \in \{0,1,2,\dots\} \end{cases} \quad (3)$$

Bu eşitliğe göre matrisler üzerinde aynı koordinatlar için alt şifreleme matris değeri tek ise gizli görüntü değeri aynen korunarak sonuç matrisine atanırken alt şifreleme matris değeri çift ise gizli görüntü değerinin tersi alınarak sonuç matrisine atanmaktadır. Bu bağlı şifreleme çok daha karmaşık biçimlerde de gerçekleştirilebilir.

C. Filigranlama

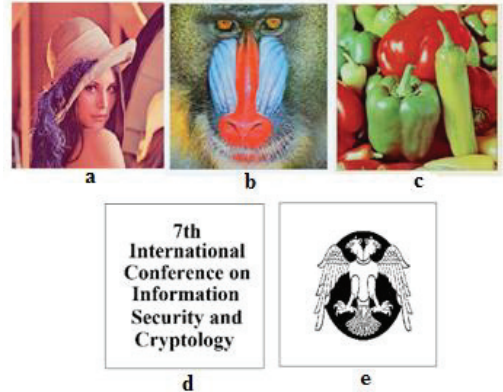
Filigranlama çalışmalarının birincil amacı taşıyıcı görüntüde en az bozulma ile filigranlama yapılması, filigranlama algoritması tersine işletildiğinde en yüksek doğruluk ile gizli görüntünün yeniden elde edilmesidir. Ayrıca filigranlanmış görüntüye karşı saldırı yapılması durumunda bile gizli görüntünün kabul edilebilir bir doğrulukla yeniden elde edilmesi istenir. Filigranlama çalışmalarında ikincil amaç ise elde edilen filigranlanmış görüntünün taşıyıcı görüntü ile aynı formatta veya herhangi bir formatta kaydedilebilmesi ve kaydetme işleminde görüntü bit derinliğinin taşıyıcı görüntüye göre artmamasıdır. Bu kriterler çerçevesinde taşıyıcı görüntüye ait piksel değerlerinin değiştirilmesi sıklıkla kullanılan bir yöntemdir. 2011 yılında Dehkordi ve arkadaşları [32] bit değişimi ile gerçekleştirilen filigranlama çalışmalarının

dışarıdan saldırılara karşı direncini incelemiştir. Çalışma sonucunda, tüm saldırılara rağmen bit değişimi ile gerçekleştirilen filigranlamada gizli görüntülerin kabul edilebilir bir doğrulukla yeniden elde edildiği görülmüştür. Aynı yıl, Bamatraf ve arkadaşları [33] tarafından gri tonlama taşıyıcı görüntüler ve ikili sayı formatındaki gizli görüntüler kullanılarak en anlamsız bittten en anlamlı bite doğru değişim yapılması durumunda elde edilecek TSGO değerleri karşılaştırılmıştır. 2012 yılında benzer bir çalışma Chopra ve arkadaşları [34] tarafından yapılmıştır.

Bu çalışmada şifreleme işlemleri tamamlanmış gizli görüntü ile taşıyıcı görüntünün birleştirilmesi taşıyıcı görüntünün yeşil renk uzayında bit değişimi ile yapılmıştır. En anlamsız bittten en anlamlı bite doğru değişim yapılarak filigranlanmış görüntüde meydana gelen TSGO değişimleri incelenmiştir. Taşıyıcı görüntü ve gizli görüntülerin boyutları eşit olmadığı için filigranlama taşıyıcı görüntünün sağ alt tarafına merkezlenerek yapılmıştır.

D. Taşıyıcı ve Gizli Görüntüler

Bu çalışmada 256×256 boyutlarında iki adet ikili sayı formatlı gizli görüntü, 24 bit RGB formatında ve 512×512 boyutlarında üç adet taşıyıcı görüntü (Lena, Baboon ve Peppers) kullanılmıştır. Gizli görüntülerden bir tanesi yazı, bir tanesi şekil içeriklidir. Çalışmada kullanılan görüntüler Şekil 4' de toplu olarak verilmiştir.



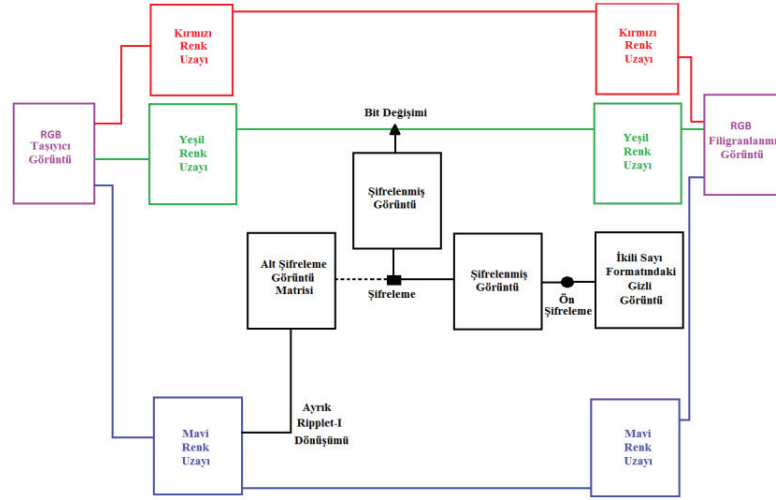
Şekil 4. a) Taşıyıcı görüntü-1 (Lena) b) Taşıyıcı görüntü-2 (Baboon) c) Taşıyıcı görüntü-3 (Peppers) d) Gizli görüntü-1 e) Gizli görüntü-2

III. DENEYLER

A. Deneyler

Önerilen filigranlama çalışmasında öncelikli olarak gizli görüntülere 20 kez ön şifreleme algoritması uygulanmıştır. Bu aşamadan sonra 24 bit derinliğe sahip RGB formatında, 512×512 boyutlarındaki taşıyıcı görüntünün mavi renk uzayı üzerinden Ripplet-I dönüşümü kullanılarak alt şifreleme görüntü matrisi elde edilmiştir. Elde edilen alt şifreleme görüntü matrisi kullanılarak 256×256 boyutlarındaki gizli görüntüler tekrar şifrelenmiştir. Son olarak şifrelenmiş gizli görüntü ile taşıyıcı görüntünün yeşil renk uzayı birleştirilmiştir. Birleştirme işlemi taşıyıcı görüntü yeşil renk uzayının en anlamsız bitinden en anlamlı bitine doğru sıra ile yapılarak filigranlanmış görüntü ile taşıyıcı görüntü arasında oluşan

TSGO değerleri hesaplanmıştır. Sistemin genel çalışmasını anlatan blok diyagram Şekil 5’ de verilmiştir.



Şekil 5. Filigranlama algoritması blok diyagramı

B. Sonuçların Değerlendirilmesi

RGB formatında $M \times N$ boyutlarında f referans görüntü, g test görüntüsü olmak üzere iki görüntü arasındaki TSGO Eşitlik (4) ile hesaplanır. Bu denklemde yer alan Karesel Ortalama Hatası (KOH) Eşitlik (5)’ de verilmiştir. RGB görüntülerde TSGO hesaplanırken kırmızı, yeşil, mavi renk uzayı için ayrı ayrı KOH hesaplanarak ortalaması alınır.

$$TSGO = 10 \cdot \log_{10} \left(\frac{255^2}{(KOH(K) + KOH(Y) + KOH(M))/3} \right) \quad (4)$$

$$KOH(f, g) = \frac{1}{MN} \cdot \sum_{i=1}^M \sum_{j=1}^N (f_{i,j} - g_{i,j})^2 \quad (5)$$

KOH değeri sıfıra yaklaşırsa TSGO sonsuza yaklaşır. Bu durum test görüntüsü ile referans görüntünün maksimum derecede örtüşüğünü gösterir.

IV. SONUÇLAR VE TARTIŞMA

Çalışmada 512×512 boyutlarında üç adet taşıyıcı görüntü ve 256×256 boyutlarında iki adet gizli görüntü kullanılmıştır. Çalışma sonucunda bir adet taşıyıcı görüntü (Lena) ve bir adet gizli görüntü (Gizli görüntü-1) için en anlamsız bitten en anlamlı bite doğru bit değimi yapılması ile elde edilen filigranlanmış görüntüler Şekil 6’ da verilmiştir. Bütün taşıyıcı ve gizli görüntüler için filigranlama sonucunda elde edilen TSGO sonuçları ise Tablo II’ de görülmektedir.

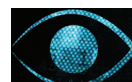
Yapılan çalışmada elde edilen ve Tablo II’ de verilen sonuçlar ile Tablo I’ de verilen literatür çalışma sonuçları karşılaştırıldığında en anlamsız 5. bitin değiştirilmesine kadar elde edilen sonuçların literatürde elde edilen sonuçlardan daha iyi olduğu görülmektedir. Tablo I’ de yüksek başarıyla elde edilen sonuçların literatürde elde edilen sonuçlardan daha iyi olduğu görülmektedir. Tablo I’ de yüksek başarıyla elde edilen sonuçların literatürde elde edilen sonuçlardan daha iyi olduğu görülmektedir.



Şekil 6. a) En anlamsız bitin değiştirilmesi b) 2.en anlamsız bitin değiştirilmesi c) 3.en anlamsız bitin değiştirilmesi d) 4.en anlamsız bitin değiştirilmesi e) 5.en anlamsız bitin değiştirilmesi f) 6.en anlamsız bitin değiştirilmesi

TABLO II
FİLGİRLANMIŞ GÖRÜNTÜLERE AİT TSGO (dB) DEĞERLERİ

		Taşıyıcı Görüntüler		
		Lena	Baboon	Peppers
Gizli Görüntü-1 (256 × 256)	En anlamsız bitin değiştirilmesi	62.07	61.07	61.73
	2.en anlamsız bitin değiştirilmesi	58.45	58.90	59.56
	3.en anlamsız bitin değiştirilmesi	56.11	55.86	55.67
	4.en anlamsız bitin değiştirilmesi	53.74	52.97	52.82
	5.en anlamsız bitin değiştirilmesi	50.04	49.47	49.72
	6.en anlamsız bitin değiştirilmesi	46.51	47.46	46.72
Gizli Görüntü-2 (256 × 256)	En anlamsız bitin değiştirilmesi	62.15	61.63	61.66
	2.en anlamsız bitin değiştirilmesi	59.42	58.87	58.56
	3.en anlamsız bitin değiştirilmesi	55.81	56.63	55.11
	4.en anlamsız bitin değiştirilmesi	52.45	53.30	52.25
	5.en anlamsız bitin değiştirilmesi	49.49	49.79	50.05
	6.en anlamsız bitin değiştirilmesi	46.71	46.43	47.18



Bu durum elde edilen bu matrisin 24 bit ile ifade edilebilmesini veya RGB formatında kaydedilmesini engellemektedir.

Filigranlamanın anlamsız bitler üzerinden yapılması yüksek TSGO değerleri üretmektedir. Ancak filigranlamada kullanılan bit anlamsızlaştıkça filigran görüntüsü saldırılara karşı daha korumasız hale gelmektedir. Filigranlamada kullanılan bitler anlamlı tarafa doğru değıştikçe TSGO değerleri ve filigranlanmış görüntü kalitesi azalmaktadır. Ancak filigranın saldırılara karşı direnci artmaktadır. Bu durum bit değışimi ile yapılan filigranlama çalışmalarında, filigranlanmış görüntü kalitesi ve koruma arasında bir tercih yapmayı gerektirmektedir.

Bu çalışma ile, taşıyıcı ve gizli görüntüye ait görüntü özelliklerinin birlikte kullanıldığı, piksel yer değıştirme kategorisinde yer alan yeni bir şifreleme algoritması oluşturulmuştur. İlk defa, RGB formatlı taşıyıcı görüntüler ve ikili sayı formatındaki gizli görüntüler için bit değıştirme ile filigranlama yapılarak sonuçlar literatüre kazandırılmıştır. Bu sonuçlar bundan sonra yapılacak ve saldırılara karşı bit değışimine göre daha yüksek savunmaya sahip olması beklenen filigranlama çalışmalarının hedefleri konusunda bilgi vermektedir.

Filigranlama çalışmalarında son yıllarda gizli görüntüler için ikili sayı formatındaki görüntülerin yanında 24 bit RGB formatlı görüntülerde kullanılmaya başlanmıştır. 24 bit RGB formatlı gizli görüntülerin, görüntü boyutları değıştirilerek ikili sayı formatında ifade edilmesi mümkündür. Önerilen algortimanın bu kapsamda 24 bit RGB formatındaki gizli görüntülerin filigranlanmasında kullanılabileceği öngörülmektedir.

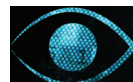
KAYNAKLAR

- [1] J. Guo and J. Yen, "A new mirror-like image encryption algorithm and its VLSI architecture," in *10 th. VLSI Design/CAD Symposium*, Taiwan, 1999, pp. 327-330.
- [2] J. Yen and J. Guo, "A new chaotic image encryption algorithm," *National Lien-Ho College of Technology and Commerce*, Taiwan, China.
- [3] C. Chang, M. Hwang and T. Chen, "A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software*, vol. 58, pp. 83-91, 2000.
- [4] S. S. Maniccam and N. G. Bourbakis, "Lossless image compression and encryption using SCAN," *International Journal of Pattern Recognition*, vol. 34, pp. 1229-1245, 2001.
- [5] P. Yu, H. Tsai and J. Lin, "Digital watermarking based on neural networks for color images," *Signal Processing*, vol. 81, pp. 663-671, 2001.
- [6] P. Tsai, Y. Hu and C. Chang, "A color image watermarking scheme based on color quantization," *Signal Processing*, vol. 84, pp. 95-106, 2004.
- [7] R. Shen, Y. Fu and H. Lu, "A novel image watermarking scheme based on support vector regression," *The Journal of Systems and Software*, vol. 78, pp. 1-8, 2005.
- [8] R. Ni, Q. Ruan and H. D. Cheng, "Secure semi-blind watermarking based on iteration mapping and image features," *Pattern Recognition*, vol. 38, pp. 357-368, 2005.
- [9] I. B. Mostefa and M. Khamadja, "A new approach to adapt and insert a watermark in colour images," in *International Conference on Signal Processing and Communications*, Dubai, 2007, pp. 760-763.
- [10] H. Tsai and D. Sun, "Color image watermark extraction based on support vector machines," *Information Sciences*, vol. 177, pp. 550-569, 2007.
- [11] C. Kuo and S. Cheng, "Fusion of color edge detection and color quantization for color image watermarking using principal axes analysis," *Pattern Recognition*, vol. 40, pp. 3691-3704, 2007.
- [12] V. Santhi, N. Rekha and S. Tharini, "A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color," in *International Conference on Communication and Networking*, St. Thomas, 2008, pp. 1-7.

- [13] Y. Fu and R. Shen, "Color image watermarking scheme based on linear discriminant analysis," *Computer Standards & Interfaces*, vol. 30, pp. 115-120, 2008.
- [14] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "Watermarking of colour images in the DCT domain using Y channel," in *International Conference on Computer Systems and Applications*, Rabat, 2009, pp. 1025-1028.
- [15] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "A frequency domain adaptive watermarking algorithm for still colour images," in *International Conference on Advances in Computational Tools for Engineering Applications*, Zouk Mosbeh, 2009, pp. 186-191.
- [16] S. P. Mohanty, "A secure digital camera architecture for integrated real-time digital rights management," *Journal of Systems Architecture*, vol. 55, pp. 468-480, 2009.
- [17] X. Lv, H. Bian and Y. Yang, "Color image watermarking using support vector regression," in *International Congress on Image and Signal Processing*, Tianjin, 2009, pp. 1-4.
- [18] C. Lai and J. Wu, "Robust image watermarking against local geometric attacks using multiscale block matching method," *J. Vis. Commun. Image R.*, vol. 20, pp. 377-388, 2009.
- [19] X. Hu, W. Tian, Y. Zheng, X. Lian and W. Ruan, "A blind digital watermarking algorithm based on chaotic systems," in *International Conference on Electrical and Control Engineering*, Wuhan, 2010, pp. 12-15.
- [20] O. Findık, İ. Babaoğlu, E. Ülker, "A color image watermarking scheme based on hybrid classification method: Particle swarm optimization and k-nearest neighbor algorithm," *Optics Communications*, vol. 283, pp. 4916-4922, 2010.
- [21] W. Hui-qin, H. Ji-chao and C. Fu-ming, "Color image watermarking algorithm based on the arnold transform," in *International Conference on Communications and Mobile Computing*, Shenzhen, 2010, pp. 66-69.
- [22] S. Pei, H. Liu, T. Liu and K. Liu, "Color image watermarking using SVD," in *International Conference on Multimedia and Expo*, Suntec City, 2010, pp. 122-126.
- [23] S. Behnia, M. Teshnehlab and P. Ayubi, "Multiple-watermarking scheme based on improved chaotic maps," *Commun Nonlinear Sci Numer Simul.*, vol. 15, pp. 2469-2478, 2010.
- [24] O. Findık, İ. Babaoğlu and E. Ülker, "A color image watermarking scheme based on artificial immune recognition system," *Expert Systems with Applications*, vol. 38, pp. 1942-1946, 2011.
- [25] P. Niu, X. Wang, Y. Yang and M. Lu, "A novel color image watermarking scheme in nonsampled contourlet-domain," *Expert Systems with Applications*, vol. 38, pp. 2081-2098, 2011.
- [26] H. V. Dang and W. Kinsner, "An intelligent digital colour image watermarking approach based on wavelets and general regression neural networks," in *International Conference on Cognitive Informatics & Cognitive Computing*, Kyoto, 2012, pp. 115-123.
- [27] E. Vahed, R. A. Zoroofi and M. Shiva, "Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles," *Digital Signal Processing*, vol. 22, pp. 153-162, 2012.
- [28] M. E. Moghaddam and N. Nemat, "A robust color image watermarking technique using modified imperialist competitive algorithm," *Forensic Science International*, vol. 233, pp. 193-200, 2013.
- [29] Y. Zhu, X. Yu and X. Liu, "An image authentication technology based on digital watermarking," in *International Conference on Sensor Network Security Technology and Privacy Communication System*, Nangang, 2013, pp. 179-183.
- [30] E. J. Candes and D. L. Donoho, "Curvelets-A surprisingly effective nonadaptive representation for objects with edges," in *Curves and Surface Fitting*, A. Cohen, C. Rabut, L. Schumaker, Ed. Nashville: Vanderbilt University Press, 1999, pp. 105-120.
- [31] J. Xu, L. Yang and D. Wu, "Ripplelet: A new transform for image processing," *Journal of Visual Communication and Image Representation*, vol. 7, pp. 627-639, 2010.
- [32] A. B. Dehkordi, S. N. Esfahani and A. N. Avanaki, "Robust LSB watermarking optimized for local structural similarity," in *19 th. Iranian Conference on Electrical Engineering*, Tehran, 2011, pp. 1-6.
- [33] A. Bamatraf, Z. Ibrahim, M. N. M. Salleh, "A new digital watermarking algorithm using combination of least significant bit (LSB) and inverse bit," *Journal of Computing*, vol. 3, pp. 1-8, 2011.
- [34] D. Chopra, P. Gupta, G. Sanjay and A. Gupta, "LSB based digital image watermarking for gray scale image," *IOSR Journal of Computer Engineering*, vol. 6, pp. 36-41, 2012.

Hüseyin YAŞAR 2010 yılında Selçuk Üniversitesi Elektrik-Elektronik Mühendisliği bölümünden mezun olmuştur. 2011 yılından bu yana T.C Sağlık Bakanlığı merkez teşkilatı bünyesinde mühendis olarak çalışmaktadır. 2011 yılında Selçuk Üniversitesi Fen Bilimleri Enstitüsünde başladığı yüksek lisans eğitimi halen devam etmektedir. Araştırma alanları görüntü işleme, medikal görüntü işleme ve tıbbi teşhis destek sistemleridir.

Murat CEYLAN Selçuk Üniversitesi Elektrik-Elektronik Mühendisliği bölümünde yardımcı doçent olarak görev yapmaktadır. 2004 yılında yüksek lisans, 2009 yılında doktora derecesi kazanmıştır. Araştırma alanları çok boyutlu görüntü işleme, biyomedikal sinyal-görüntü işleme ve yapay sinir ağlarıdır. Yirmi beşin üzerinde dergi ve konferans bildirisi yayınlamıştır. Ayrıca IEEE üyesidir.



Android Zararlı Yazılımlarını Tespit Etme, İmza Oluşturma ve Sınıflandırma

Ömer Faruk Acar¹

Özet— Mobil cihazların hızlı gelişimi ve yaygınlaşması ile birlikte bu cihazların ve üzerinde çalışan uygulamaların güvenliği bir sorun haline gelmiştir. Mobil işletim sistemlerinden özellikle Android işletim sisteminde çok yüksek oranda güvenlik tehditleri tespit edilmiştir [1][2]. Doğası gereği mobil ortamlardaki zararlı yazılımların tespit edilmesi için kullanılacak yöntemlerde bugüne kadar geliştirilen yöntemler maalesef başarısız olmaktadır. Bu bildiri kapsamında Android işletim sistemi için geliştirilmiş zararlı yazılım tespit etme altyapısı, imza algoritması, diğer zararlı yazılımlarla ilişkilendirme yöntemlerinden ve test çalışmalarından bahsedilmektedir.

Anahtar Sözcükler— Android, Zararlı Yazılım, İmza Algoritmaları

Abstract—Security concern of applications for mobile platforms become one of the hot topics with the rapid evolution and wide usage of mobile devices. A notable amount of security threats have been identified on the mobile operating systems, more specifically on Android operating system, recently. [1][2] Developed methods that was used for the detection of malwares for other platforms tend to fail in the mobile environment, because of the nature and structure of malicious software. To mitigate this problem, in this paper, a new malware detection infrastructure, developed for the Android operating system, signature algorithms, correlation with other malware families and evaluation of proposed system are discussed.

Index Terms— Android, Malware, Signature Algorithms

I. GİRİŞ

Mobil platformlardaki tehlikeler diğer platformlarda olduğu gibi her geçen gün artmakta ve geliştirilen zararlı yazılımlarda gittikçe karmaşıklaşmaktadır. Yeni nesil Zararlı yazılımlar, statik ve dinamik analize olanak vermemek için farklı teknikler kullanmakta böylece tespit edilmesi ve analiz edilmesi zorlaşmaktadır.

Çoğunlukla temiz bir uygulamaya eklenerek paketlenen ve geçerli uygulama marketi dışındaki marketlerden yayılan bu zararlı yazılımlar kendilerini karmaşıklaştırma (obfuscation) ve şifreleme(encryption) gibi yöntemleri kullanarak çok iyi gizleyebilmektedir. Çalışma öncesinde yapılan literatür taramalarında mevcut güvenlik çözümlerinin çalışma prensipleri araştırılmıştır. Mevcut mobil güvenlik

çözümlerinde mobil cihazlardaki pil, işlem gücü, bellek gibi kısıtlardan dolayı sadece imza tabanlı kontrollerin gerçekleştirildiği tespit edilmiştir.

Mevcut uygulama marketine bakıldığında zararlı yazılımları(malware) tespit etmek için kullanılan birçok güvenlik uygulaması olduğu görülür fakat yapılan çalışmalarda bu uygulamaların başarı oranlarının düşük olduğu ve hatalı tespit (false positive) oranlarının yüksek olduğu gözlemlenmiştir[3].

Bilgisayarlarda olduğu gibi Android dünyasında da bir zararlı yazılımı tespit etmek için güvenlik uygulamaları zararlı yazılımdan çıkardıkları imzaları (signature) karşılaştırmak suretiyle tarama gerçekleştirmektedir. Bu noktada iki problem ortaya çıkmaktadır.

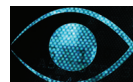
Birincisi, bir zararlı yazılım imzası oluşturulduktan sonra eğer zararlı yazılıma, kod karmaşıklaştırma (obfuscation), tekrar paketleme (repackage), dosya/paket adlarını değiştirme(Rename), kod akışını değiştirme(reorder code), araya anlamsız kodlar yerleştirme(insert junk code), karakter katarlarını şifreleme(encrypt strings) gibi işlemler uygulandıktan sonra güvenlik uygulaması tarafından bu zararlı yazılım tespit edebilir mi?

İkincisi, sadece imza karşılaştırması yaparak dinamik analiz gerçekleştirmeden mevcut ve henüz tespit edilememiş(zero day) zararlı yazılımlar yakalanabilir mi?

Belirtilen bu sorunlara çözüm olarak yapılan araştırmalarda statik analiz ve dinamik analiz yöntemleri önerildiği [3][4] fakat bu yaklaşımların ve çözümlerin tüm durumlar için toptan bir çözüm sunmadığı görülmüştür. Mevcut çoğu çözüm normal şartlar altında başarılı olmakta fakat yeni nesil zararlı yazılımların atlatma teknikleri kullanmasıyla başarısız olmaktadır. Bazı çalışmalarda doğrudan zararlı yazılım tespit etmek yerine davranışlar ve seçilen özelliklere göre belirli skorlamalara gidildiği ve sonuçta bu skora göre sınıflandırmalar yapıldığı belirtilmektedir.[10] Bu bildiride anlatılan çözümde tüm yaklaşımlar katmanlı bir yapıda belirli bir sırayla yapılarak etkin ve başarılı bir çözüm elde edilmeye çalışılmıştır.

Yapılan çalışma kapsamında bu soruların cevabını verebilecek en iyi analiz ortamı oluşturulması ve bahsi geçen yöntemlere dayanıklı bir kimliklendirme için imza algoritması çalışmaları gerçekleştirilmiştir. Bildiri kapsamında bu çalışmanın ayrıntıları ve sonuçları değerlendirilecektir.

¹ Ömer Faruk ACAR, HAVELSAN A.Ş., Ankara; e-posta: oacar@bgt.havelsan.com.tr



ANDROİD ZARARLI YAZILIMLARINI TESPİT ETME, İMZA OLUŞTURMA VE SINIFLANDIRMA

II. ZARARLI YAZILIM TESPİT YÖNTEMLERİ

Zararlı yazılım tespiti konusunda çok fazla sayıda çalışma bulmak mümkündür. Farklı yaklaşımlar denenerek en az hata ile bilinen ve bilinmeyen zararlı yazılımlar tespit edilmeye çalışılmaktadır. Bunun için Statik ve Dinamik analiz yöntemleri kullanılmaktadır.

Çalışma sırasında güvenlik çözümlerinin başarı oranını ölçmek amacıyla mevcut zararlı yazılımlardan seçilmiş örnekler ve geliştirilen zararlı yazılım Virustotal[5] ortamı üzerinde bulunan antivirüs uygulamalarına taratılmış ve tespit oranları Tablo 1'de gösterilmiştir. Zararlı yazılım seçiminde zararlı yazılım türü (adware, RAT, Spyware v.s.) ve farklı zararlı kabiliyetler (SMS gönderme, uzaktan komut satırına erişim, reklam gösterme v.s.) açısından çeşitlilik sağlayacak örnekler tercih edilmiştir.

TABLO 1
ZARARLI YAZILIM YAKALANMA ORANLARI

Malware İsmi	Antivirüs Başarı Oranı		
	Tespit Edebilen	Tespit Edemeyen	Tespit Edilme Oranı %
Chuli	19	28	40,43
CI4	30	17	63,83
Fakemart	22	25	46,81
Plankton	8	39	17,02
İkno	19	28	40,43
Lena	30	17	63,83
PuppyWidget	10	37	21,28
RootSmart	30	17	63,83
Leadbolt	10	37	21,28
SSUCL	25	22	53,19
Stels	25	22	53,19
SystemSecurity	31	16	65,96
Örnek Zararlı Yazılım	0	47	0
Ortalama :			42,39

Yapılan testlerde tek başına hiçbir metodun tam olarak başarılı olduğunu söylenemez. Fakat ortaya birden fazla yöntemden oluşan karma model oluşturulduğunda (çalışmada bu model, katmanlı analiz olarak adlandırıldı) her katmanda yapılan analiz diğer katmanlardaki üretilen sonuçlarla değerlendirildiğinden hem yanlış tespit(false positive) oranı düşmekte hem de toplamda bir örnek kümesi içindeki zararlı yazılım veya zararlı yazılım olmasa bile bazı zararlı davranışlar gerçekleştiren uygulamaların tespit oranı çok yüksek olmaktadır.

A. İmza Tabanlı

Statik analiz yöntemlerinden biri olan imza çıkarma yöntemi mobil güvenlik alanında ilk kullanılmaya başlayan tespit yöntemidir. Bu yöntem, zararlı yazılıma ait hangi özelliklerin imza çıkarmada kullanılacağına ve bu imzayı oluşturmada nasıl bir algoritma kullanılacağına göre çeşitlenmektedir. Genellikle kod içerisinde belirgin bazı kısımlar alınarak bunlardan zararlı yazılıma özgü bir imza çıkartılmaktadır. [7][8] Android uygulamaları için örnek verilecek olursa, kullandığı izinler(permissions), kod içerisinde geçen bilgiler (String values), kullanılan sistem çağrıları (system call) örnek

olarak verilebilir.

Bu verilerden çıkartılan bir veri kümesi (data set) oluşturulduktan sonra seçilen algoritmaya göre hesaplatılarak uygulamayı tanımlayacak bir değer elde edilmektedir. Genellikle imza çıkarma işlemi için özet (hash) algoritmaları kullanılmaktadır[18] fakat bu algoritmalar uygulamadaki en ufak bir değişiklikte çok farklı sonuçlar çıkardığı için imza çıkarma işleminde başarılı olamamıştır. Bu problemten dolayı bulanık özet(fuzzy hash) algoritmaları kullanılmaya başlanmış [9] ve iki imza değeri arasında ilişki kurulabilmiştir. Fakat bu da yeterli olmamıştır. Bir imza parçasından diğer imzaları hesaplayabilme, küçük boyutlu veriler içinde ilişki (correlation) hesaplamaları yapma ihtiyacı doğduğu için farklı algoritmalar üretilmelidir. Bu çalışma kapsamında kullanılan karakter katarları üzerinde arama yapmayı sağlayan algoritmalar ve bu algoritma içerisinde ötelemeli özet(Rolling hash) algoritmaları çözüm olarak sunulmuştur. İmza algoritmalarında en önemli kural her bir örnek için tekilliğin(unique) sağlanmış olmasıdır. Aksi takdirde algoritma başarısız demektir.

B. İlişki (Korelasyon) Hesaplama

Yapı olarak imza tabanlı yöntemle benzese de imza tabanlı yöntemdeki gibi birebir eşleştirerek kontrol etme yerine bütünü daha küçük parçalara ayırıp istatistiksel olarak parçaların birbirine benzerliği hesaplanmaktadır. Bu yöntemde bazen makine öğrenmesi, yapay sinir ağları gibi yeni yaklaşımlarda kullanılmaktadır. Burada önemli olan yüzde yüz bir eşleştirme değil eldeki bilinen zararlı yazılım verilerine göre incelenen uygulamanın bu verilerden ne kadarını içerdiği veya hangi kısımların benzer özelliklerden oluştuğunun tespit edilmesidir.

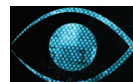
İlişki hesaplama yöntemi kullanılırken en fazla sınıflandırma algoritmaları kullanılmaktadır. Bu algoritmaların Android uygulamalarından çıkartılan özelliklere göre benzerliği hesaplamada ne kadar başarılı olduğu bildiri içerisinde ayrı bir başlık altında toplanmıştır.

C. Davranışsal Kalıplar

Bahsedilen iki yöntemde de ağırlıklı olarak statik bir inceleme yapılırken bu yöntemde ise bir uygulamanın çalışma sırasındaki davranışları hedef alınmaktadır. Tablo 2'de bahsedilen özellikler izlenerek davranışlardan bir tasarım kalıbı oluşturulmaya çalışılmakta ve böylece benzer davranışları gösteren uygulamalar gruplandırılabilir.

TABLO 2 KULLANILAN ÖZELLİKLER

Uygulama İzinleri	- Permissions
İşlemci Komutları	- CPU Instructions
İşletim Sistemi Çağrıları	- System Call
Ağ Aktiviteleri	- Network Activity(Wi-Fi,3G)
İşlemci Kullanımı	- CPU Usage
Hafıza Kullanımı	- Memory Pattern
Pil Tüketimi	- Battery Usage
Sensor Kullanımı	- Sensor Usage



Bu yöntemde karşılan en büyük sorun uygulamanın her zaman aynı davranışı sergilememesidir. Mesela, sadece SMS ile aktif hale gelen bir zararlı yazılım izlendiğinde herhangi bir davranış sergilemeyeceği için tasarım kalıbını oluşturacak yeterli veri elde edilemeyecektir. Diğer yöntemlerden avantajlı olduğu kısımlar ise uygulamada yapılan kod karmaşılaştırma(obfuscation), şifreleme(encryption) gibi işlemler davranış şeklini değiştirmedikleri için analiz başarılı olmaktadır.[6] Ayrıca, çalışma esnasında kullanıcı davranışları simüle edilerek komuta kontrol sunucusu (C&C) ile yapılan haberleşme, sonradan kod indirip çalıştırma (Dynamic code loading and payload execution) gibi işlemler bu yöntemde tespit edilebilmektedir.[15][16][17]

III. İMZA ÇIKARMA

İyi bir imza algoritması geliştirmek zararlı yazılım analizinde en çok zorlanılan aşamalardan birisidir çünkü geliştirilen imza, tüm atlatma tekniklerinden etkilenmemeli, performanslı olmalı ve anlamlı sayılardan(bitlerden) oluşmalı ki sınıf seviyesinde veya metod seviyesinde karşılaştırmalar yapılabilir. Bildiri kapsamında yapılan çalışma sırasında da mevcut özet algoritmaları (hash) ve karakter katarları(String) üzerinden arama yapabilen, özet çıkartabilen algoritmalar araştırıldı. Çalışmalar sırasında farklı algoritmalar test edildi. Bilişim sistemlerinde imza oluşturmak için kullanılabilecek gelişmiş Elliptic Curve, Elgamal İmza Şeması, NSA tarafından geliştirilmiş Dijital İmza Algoritması gibi algoritmalar zararlı yazılımın oluşturulan farklı varyantları üzerinde farklı imzalar çıkardığı için başarısız olmuştur. Bu durum sonrasında genellikle adli analiz çalışmalarında kullanılan bulanık özet algoritması (fuzzy hash) uyarlanmaya çalışılmıştır. Bu algoritma da, büyük veri setlerinden oluşturulan imzalarda benzerlik oranı vermesi yönüyle başarılıydı fakat küçük boyutlu veri kümelerinde (metot ve sınıf numarası) hesaplama yapmak için uygun değildi. Sonunda test edilen algoritmalar içerisinde Karp-Rabin algoritmasının mevcut durum için uygun olduğu gözlemlendi. Testlerde çok küçük veri setleriyle bile imza oluşturulabiliyor, performanslı çalışıyordu tek sorun farklı sayıdaki ve farklı uzunluktaki değerleri karşılaştırmak gerekiyordu. Bunun içinde bir özet algoritması olarak “Rolling Hash” algoritmaları incelenerek özelleştirilmiş bir algoritma kullanıldı.

Özetle, Rabin-Karp algoritmasında her bir sistem çağrısının(system call) tablodaki karşılık gelen değerini girdi olarak alıp bunu öncede belirlenmiş bir asal sayı ile metod içerisinde kaçınıcı sıradaysa bu sistem çağrısı asal sayının bu sıra sayısı kadar üssü alınıp çarpılması ve elde edilen değerlerin toplanması ile hesaplanmaktadır. Formülüzede edilecek olursa, hesaplanacak özet değeri H olsun. Girdi olarak verilen metod içerisindeki sistem çağrılarının tablodaki karşılık değerleri de $c_1 + \dots + c_k$ şeklinde bir seri olsun. Önceden belirlenmiş asal sayı da a olsun.

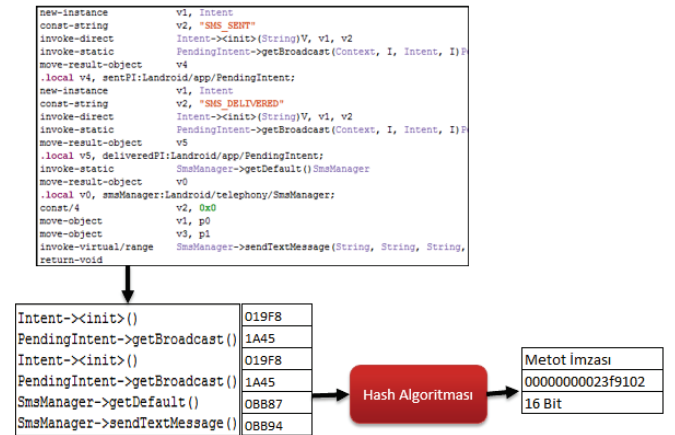
$$H = c_1 a^{k-1} + c_2 a^{k-2} + c_3 a^{k-3} + \dots + c_k a^0 \quad (1)$$

Bu formül Java dilinde gerçekleştirilmiştir. Burada önemli olan hesaplanan özet değerin önceki ve sonraki hesaplanan değer ile doğrudan ilişkili olması ve yeni bir sistem çağrısı eklendiğinde ya da çıkartıldığında bunun rahatlıkla hesaplanabilmesidir.

```
final static BigInteger primenumber = new BigInteger("11");
public BigInteger hashcalculator(String deger)
{
    int tmplength=deger.length();
    tmpcarpan = BigInteger.ONE;
    smallhash=BigInteger.ZERO;
    for (int j=0; j < tmplength ; ++j) {
        int karakter=deger.charAt(j);
        String unicodevalue=String.valueOf(karakter);
        BigInteger unicodeBigInteger=new BigInteger(unicodevalue);
        smallhash=smallhash.add( \
        unicodeBigInteger.multiply(primenumber.pow(j)));
    }
    return smallhash;
}
```

Şekil 1. Rolling Hash Algoritması

Büyük resime bakıldığında Şekil 2’de görüldüğü üzere bir metod içindeki sistem çağrıları tespit edilip tüm çağrılarının belirli bir numara verildiği sistem çağrıları tablosundaki değeri bulunup sırayla özet algoritmasına girdi olarak verilmektedir. Çıkan değer o metoda ait imza değeridir.

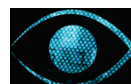


Şekil 2. Metottan imza çıkarma adımları

Yine aynı şekilde tüm metotlardan elde edilen özetler küçükten büyüğe sıralanarak (kod bulanıklaştırma ile sıranın değiştirilmesi yönteminden etkilenmemesi için) özet algoritmasına verilmekte ve sınıf imzası hesaplanmaktadır. Bu sırada yaygın kullanılan kütüphaneler gibi bazı kodlar temizlenerek imzanın asıl uygulamaya ait değerleri içermesi sağlanmaktadır.

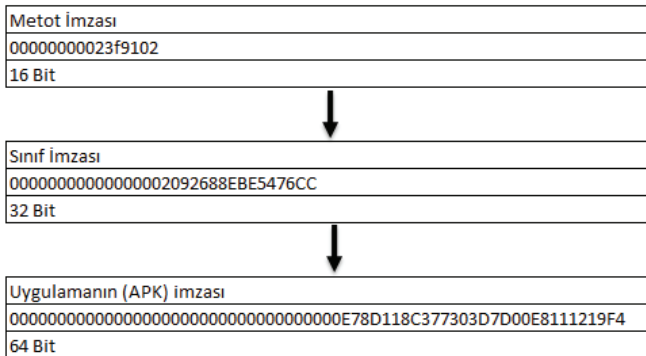
IV. SINIFLANDIRMA ALGORİTMALARININ BAŞARISI

Sınıflandırma algoritmaları, istenilen özellik ya da özelliklere göre birbirine benzeyen veri setlerini gruplamaya yarayan algoritmalar. Bu çalışma kapsamında sınıflandırma algoritmaları başarılı bir imza işleminden sonra elde edilen ham



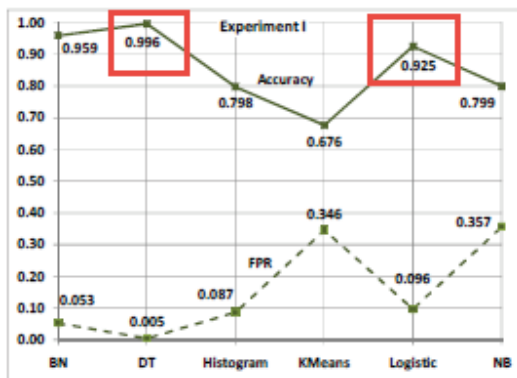
ANDROİD ZARARLI YAZILIMLARINI TESPİT ETME, İMZA OLUŞTURMA VE SINIFLANDIRMA

veriden bilgiye dönüşmüş kümeyi sınıflandırmak için kullanılmıştır. Mevcut zararlı yazılımlardan elde edilmiş imzalar sınıflandırma algoritmaları kullanarak yeni bir uygulama incelendiğinde ne kadar zararlı kod bulunduruyor bunu tespit etmek için kullanılmaktadır [13][14]. Bu amaçla farklı sınıflandırma algoritmalarının performansları değerlendirilerek en az yanlış sonuç üreten algoritma veya birden fazla algoritma seçilerek analiz ortamına dâhil edilmiştir.



Şekil 3. Metot, Sınıf ve Uygulamaya ait imzalar

Bu konuda daha önce yapılmış bir çalışma olan Asaf Shabtai ve Yuval Elovici'ye ait makalede [6] “Bayesian Networks”, “Decision Tree”, “Logistic Regression”, “Naive Bayes”, “Histogram” ve “KMeans” algoritmalarını test etmiş ve en iyi sonuçları Decision Tree ve Logistic Regression algoritmalarından elde etmişlerdir.



Şekil 4. Mobil Uygulama Özelliklerinin Sınıflandırılması

Bu çalışma referans alınarak geliştirilen analiz ortamında “Decision Tree” ve “Logistic Regression” algoritmalarının kullanılması kararlaştırılmıştır.

V. ANDROID GÜVENLİK VE DENETLEME ARACI-ASAT

Mevcut güvenlik çözümlerinin sadece cihaz üzerinde veritabanlarındaki imzaları doğrudan karşılaştırma yaparak zararlı yazılımları tespit ettiklerinin ve başarı oranlarının düşük olduğunun tespit edilmesi üzerine böyle bir çalışma yapılma ihtiyacı ortaya çıkmıştır.[10] Çalışma kapsamında gerçekleştirilen yapı, sunucu tarafında çalışacak analiz ortamı

ve mobil cihaz üzerinde çalışacak güvenlik uygulamasından oluşmaktadır.

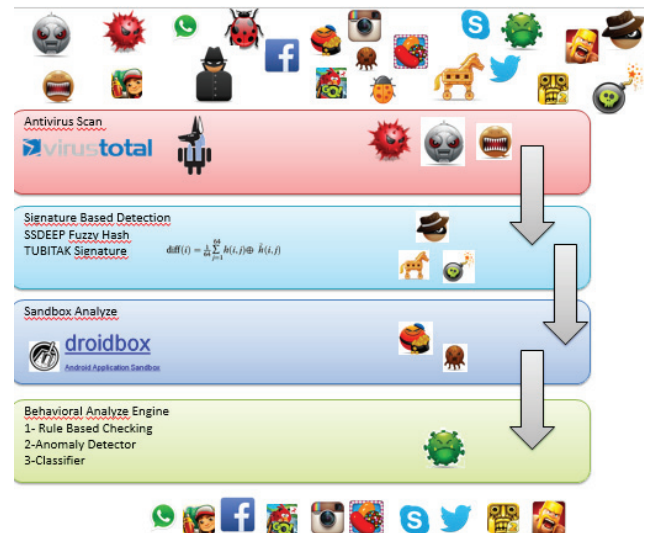
A. Katmanlı Analiz Ortamı

İlk aşamada verilerin toplanabilmesi için tüm marketlerle entegre olup uygulamalara ait “APK” dosyalarının ve uygulama bilgilerinin indirilmesi gerekmektedir.[11][12] Bunun için “Regular Expression” ve “Xpath” sorgularını destekleyen dinamik olarak marketlerin tanımlanabildiği “Scrapy” altyapısını kullanan bir ortam tasarlanmıştır. Ayrıca bu ortam içerisinde dinamik web arayüzleri geliştirilebilecek “Django” altyapısı kullanılarak bir web arayüzü geliştirilmiştir. İndirilen uygulamalar “Androguard” kütüphanesi kullanılarak apk uzantılı dosyalar açılıp alt bileşenlerine ayrıştırılarak tüm üst veri(meta data) bilgileri elde edilmiş ayrıca uygulamaya ait sertifika, paket ismi, kullanılan izinler, içerdiği sınıflar v.s. veritabanına kaydedilmektedir.

Katmanlı analiz ortamında analiz işlemi dört farklı katmanda gerçekleşmektedir.

1. Antivirüs Taraması
2. İmza Algoritmaları ile Kontrol
3. Dinamik Analiz Ortamı (Sandbox)
4. Davranışsal Kalıplar ile Kontrol

Bu dört katmanlı analiz sırasında bir uygulama sonuç olarak temiz, şüpheli, zararlı yazılım şeklinde bir gruba düşmektedir. Temiz ve zararlı yazılım grubuna giren uygulamalara herhangi bir işlem uygulanmazken şüpheli bulunan uygulamalar manuel analiz için araştırmacıya gönderilmektedir. Manuel analiz sonrasında grubuna karar verilerek analiz ortamının güncellenmesi sağlanmaktadır. Bu sayede sürekli canlı ve kendini güncelleyen bir yarı otomatik analiz ortamı geliştirilmiştir.



Şekil 5. Katmanlı Analiz Ortamı

Katmanlı analiz ortamının diğer çalışmalara göre en başarılı olduğu kısım geliştirilen imza algoritmasıyla yapılan tespit başarı oranıdır. Bunu test etmek için mevcut bir zararlı yazılım “DroidChameleon” [3] isimli uygulama değiştirme altyapısı ile değiştirilmiş ve mevcut antivirüslere tarattırılmıştır. Diğer

ANDROİD ZARARLI YAZILIMLARINI TESPİT ETME, İMZA OLUŞTURMA VE SINIFLANDIRMA

antivirüsler değişiklik sonrası bu zararlı yazılımı tespit edemezken geliştirilen imza algoritması aynı imzayı oluşturmaya devam ettiği için tespit edebilmiştir.

SHA256: be90c12ea4a9dc40557a492015164eae57002de55387c7d631324ae396f7343c

Dosya adı: zitmo.apk

Tespit edilme oranı 37 / 52

SHA256: e62bb1c2090817be61c750df764ceaf7cc0fd28ecb446fc35fa4e7a3a8d3432a

Dosya adı: 1-of1.apk

Tespit edilme oranı 19 / 52

SHA256: 02dbb588ba093214482a9e72361f2c8af83d48584ef4a182b721d37ee764e694

Dosya adı: 1-of2.apk

Tespit edilme orani 18 / 52

ID	PackageName	CertificateInfo	APKSignature
10	com.secure.service	REAL	00000000000000000000000000000000000078d118c377303d7d0e8111219f4
12	com.secure.service	REAL	00000000000000000000000000000000000078d118c377303d7d0e8111219f4
13	com.secure.service	REAL	00000000000000000000000000000000000078d118c377303d7d0e8111219f4
14	com.secure.service	REAL	00000000000000000000000000000000000078d118c377303d7d0e8111219f4

Şekil 6. Zararlı yazılımın türevleri ve antivirüs tarama sonuçları

B. Mobil Güvenlik ve Denetleme Uygulaması

Mobil cihaz üzerinde çalışacak uygulamanın en temel görevi arka planda güncel olarak elde edilen akıllı zararlı yazılım bilgilerinden oluşturulan veritabanı (Threat Intelligence Database) ile cihaz üzerinde yüklü uygulamalarda tarama gerçekleştirmektir. Bunun dışından cihaz üzerinde zafiyete neden olabilecek tüm açıklıkları değiştirmek ve ayarları gerçekleştirmek için sıkılaştırma modülü bulunmaktadır.

Çalışma prensibi olarak diğer güvenlik çözümleri gibi imza kontrolü gerçekleştirse de imza yaklaşımındaki dinamik çözümler başarı oranını arttırmıştır. Bir uygulamanın cihaz üzerinde analizi kaynakları çok hızlı bir şekilde tüketeceği için onun yerine uygulamanın hangi kaynaktan indirildiği, uygulama paket adı (package name), uygulama özet(hash) değeri gibi bilgiler analiz ortamına gönderilerek henüz veritabanında bulunmayan bu uygulama kaynaktan indirilip analizi gerçekleştirilip cihaza sadece sonuç ile ilgili bilgiler dönmektedir. Eğer manuel olarak bir uygulama yükleme işlemi gerçekleştirilmişse kullanıcıdan uygulamayı içeren “APK” dosyasının analiz ortamına gönderilmesi istenmektedir.

VI. SONUÇ VE GELECEK ÇALIŞMALAR

Bu çalışma, çok fazla sayıda kaynaktan veri toplayıp işlenmesi, kendine özgü imza algoritması ve birden fazla yöntemi bir arada destekleyen katmanlı analiz ortamı kullanılması yönüyle zararlı yazılıma karşı yeni bir yaklaşım sunmuştur. Farklı yöntem ve tekniklerin bir arada kullanılması, dinamik bir yapı oluşturularak yeni saldırı durumlarına göre rahatlıkla özelleştirilebilmesi başarı oranının artmasına ve hızlı bir şekilde sonuç elde edilmesine olanak sağlamaktadır.

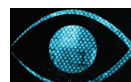
Mevcut çözümlerin yetersiz olduğu bir durumda geliştirilen analiz ortamı oldukça başarılı sonuçlar ortaya çıkarmıştır fakat hala eksik veya zayıf olan kısımlar bulunmaktadır. Örnek olarak, yeni geliştirilen kod karmaşıklıklandırma ortamı [19]

“Bangcle”, mevcut bir uygulamanın kodlarını JAVA katmanından alıp JNI (Java Native Interface) kullanan C++ diline çeviriyor ve bu şekilde derliyor. Bu durum şu anda analiz ortamında farklı imzalar çıkmasına neden olabiliyor. Aynı arayüzü kullanan zararlı yazılımlar henüz ekosistemde pek rastlanmasa da yakın zamanda yaygınlaşacağı tahmin edilmektedir. Bundan dolayı “Smali” dilinde gerçekleştirilen mantık “Assembly” dili içinde uygulanmalı ve test edilmelidir. Gelecek çalışma olarak, ulusal zararlı yazılım veritabanı oluşturmak ve bu veritabanını bir web sayfası/ web servisi aracılığıyla erişime açılması planlanmaktadır. Diğer bir yapılması gereken çalışma mevcut “Sandbox” dinamik analiz ortamlarının ihtiyaca göre uyarlanması yerine ulusal dinamik analiz ortamının geliştirilmesidir. Şu anda sadece kullanıcı katmanı (User Mode) dikkate alınarak tasarlanmış güvenlik çözümünün daha başarılı analiz kabiliyetleri kazanabilmesi için çekirdek katmanında (Kernel Mode) çalışacak şekilde tekrardan tasarlanması gerekmektedir. Bu katmanda çalışması, uygulamaya daha fazla kaynağı izleyip tıpkı IDS/IPS yazılımları gibi dinamik aykırılık tespit(anomaly detection) yeteneği kazandıracaktır.

Yapılan çalışmalar kapsamında halen Android işletim sisteminin güvenlik açısından yeterli özelliklere sahip olmadığı tespit edilmiş olup dinamik izin modeli, ağ erişim kontrolü gibi diğer mobil işletim sistemlerinde bulunan özelliklerin sonraki sürümlerde ekleneceği tahmin edilmektedir.

KAYNAKLAR

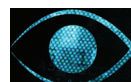
- [1] F-Secure Mobile Threat Report Q12014 http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014.pdf.
- [2] Sophos Mobile Security Threat Report <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf>
- [3] Vaibhav Rastogi, Yan Chen, Xuxian Jiang, DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks, ASIA CCS'13, May 8-10 2013, ACM 978-1-4503-1767-2/13/05
- [4] G. Suarez-Tangil, J. Tapiador, P. Peris-Lopez and A. Ribagorda, 'Evolution, detection and analysis of malware for smart devices', IEEE, 2013.
- [5] <https://www.virustotal.com/>
- [6] A. Shabtai and Y. Elovici, 'Applying behavioral detection on android-based devices', Springer, pp. 235–249, 2010.
- [7] J. Kornblum, 'Identifying almost identical files using context triggered piecewise hashing', Digital investigation, vol 3, pp. 91–97, 2006.
- [8] S. Schleimer, D. Wilkerson and A. Aiken, 'Winnowing: local algorithms for document fingerprinting', pp. 76–85, 2003.
- [9] D. Hurlbut-AccessData, 'Fuzzy Hashing for Digital Forensic Investigators', 2009.
- [10] M. Grace, Y. Zhou, Q. Zhang, S. Zou and X. Jiang, 'Riskranker: scalable and accurate zero-day android malware detection', pp. 281–294, 2012.
- [11] Y. Zhou, Z. Wang, W. Zhou and X. Jiang, 'Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets.', 2012.
- [12] W. Zhou, Y. Zhou, X. Jiang and P. Ning, 'Detecting repackaged smartphone applications in third-party android marketplaces', pp. 317–326, 2012.
- [13] A. Schmidt, R. Bye, H. Schmidt, J. Clausen, O. Kiraz, K. Yuksel, S. Camtepe and S. Albayrak, 'Static analysis of executables for collaborative malware detection on android', pp. 1–5, 2009.



ANDROİD ZARARLI YAZILIMLARINI TESPİT ETME, İMZA OLUŞTURMA VE SINIFLANDIRMA

- [14] Y. Aafer, W. Du and H. Yin, 'DroidAPIMiner: Mining API-level features for robust malware detection in android', Springer, pp. 86--103, 2013.
- [15] T. Petsas, G. Voyatzis, E. Athanasopoulos, M. Polychronakis and S. Ioannidis, 'Rage against the virtual machine: hindering dynamic analysis of Android malware', p. 5, 2014.
- [16] T. Blasing, L. Batyuk, A. Schmidt, S. Camtepe and S. Albayrak, 'An android application sandbox system for suspicious software detection', pp. 55--62, 2010.
- [17] I. Burguera, U. Zurutuza and S. Nadjm-Tehrani, 'Crowdroid: behavior-based malware detection system for android', pp. 15--26, 2011.
- [18] H. Kuzuno and S. Tonami, 'Signature generation for sensitive information leakage in android applications', pp. 112--119, 2013.
- [19] <http://bangcle.com/>

Ömer Faruk Acar, Ege Üniversitesi Bilgisayar Müh. Bölümünden mezun olduktan sonra Hacettepe Üniversitesi Bilişim Enstitüsünde Yüksek Lisansını tamamlamış ve doktora çalışmalarına devam etmektedir. Bilişim (IT) sektörüne web uygulamaları ve KOBİ'lere hazır paket uygulamalar geliştirerek başlamıştır. Sonrasında Türk Telekom A.Ş. bünyesinde Telekom altyapısı üzerine kendini geliştirmiş ve Entegrasyon Uzmanı olarak çalışmıştır. Farklı teknolojiler ve platformlar üzerinde çalışırken hep bir merak ile araştırdığı bu nasıl çalışır? Zafiyet barındırıyor mu? Korumalar nasıl aşılır? Sorularına cevap bulmak için güvenlik alanında uzmanlaşmaya başlamıştır. TÜBİTAK Siber Güvenlik Enstitüsü bünyesinde Veritabanı güvenliği, sızma (penetrasyon) testleri, zararlı yazılım(malware) analizi ve son iki yıldır mobil cihaz güvenliği konularında araştırmalarda bulunmuştur. TR-BOME ekibinin bir üyesi olarak Siber güvenlik olaylarına müdahale etmiştir. Türkiye'deki bankalar, devlet kurumları ve özel sektöre yazılım, danışmanlık, eğitim projeleri gerçekleştirmiştir. Bu çalışmalar sırasında kullanımı yaygınlaşan mobil cihazların nasıl tehlike oluşturduğunu gözlemlemiş ve önlem olarak neler yapılabilir soruları üzerine çalışmalarına devam etmektedir. Şu anda HAVELSAN A.Ş. Siber Güvenlik Takımında siber güvenlik uzmanı olarak görev almaktadır.



Sahte Baz İstasyonu Saldırı Tespit Algoritması

Ömer Faruk ÇELİK, Refik SAMET

Özet— Dünya çapında yaygın olarak kullanılan iletişim sistemi GSM'in bir takım güvenlik problemleri vardır. Bu güvenlik problemlerinden bir tanesi mobil terminal ile baz istasyonu arasında karşılıklı doğrulamanın olmamasıdır. Bu durum GSM'in (baz istasyonlarının ve mobil terminallerin) sahte baz istasyonu ataklarına maruz kalmasına neden olmaktadır. Ayrıca, mobil terminal kimliğinin çalınması, tele kulak, mobil terminal ve baz istasyonu sahteciliği ve diğer ortadaki adam (man-in-the-middle) saldırıları sahte baz istasyonu kullanılarak gerçekleştirilebilmektedir. Bundan dolayı, sahte baz istasyonu saldırılarının tespit edilmesi oldukça önemlidir. Bu makalede sahte baz istasyonu saldırılarının analiz edilmiştir ve bu saldırıların tespit edilmesine yönelik bir algoritma geliştirilmiştir. Ayrıca yapılan simülasyon ile sahte baz istasyon saldırılarının, geliştirilen algoritma yardımıyla tespit edilebilirliği gösterilmiştir.

Anahtar Kelimeler— GSM güvenliği, Baz istasyonu, Sahte baz istasyonu saldırıları, Saldırı tespiti.

Abstract— GSM is widely used communication system around the world and it has some security problems; one of them is lack of mutual authentication between mobile station and base station. GSM (mobile stations and base stations) is subject to fake base station attacks by exploitation of GSM's mutual authentication weakness. In addition, MS identity theft, eavesdropping, impersonation of network/MS attacks and other kinds of man-in-the-middle attacks can be made by fake base station. Thus, detection of fake base station attacks is crucial. This paper presents analysis of fake base station attacks and proposes algorithm for detection those attack. Besides, by the help of proposed algorithm, simulation shows feasibility of fake base station attack detection.

Index Terms— GSM security, Base station, Fake base station attacks, Attack detection

I. GİRİŞ

MOBİL İletişim için Küresel Sistem (Global System for Mobile Communication - GSM), %90 market payı ile dünyada en yaygın kullanılan mobil iletişim sistemi olup, 219 ülke ve bölgede kullanılmaktadır [1]. Uluslararası Telekomünikasyon Birliğinin (International Telecommunication Union - ITU) yaptığı araştırmaya göre 2008 yılı sonunda dünya geneli İnternet kullanan insan sayısı 1,5 milyar iken, 4,1 milyar GSM aboneliği bulunmaktaydı. 2013 yılı sonlarında ise GSM aboneliği sayısı neredeyse 7

milyara ulaşmıştır [2]. 25 yıllık bir teknoloji için bu büyük bir başarıdır. Bununla birlikte, GSM'in yaygın olarak kullanılan bir iletişim protokolü olduğu açıktır ve bu sebeple GSM güvenliği oldukça önemlidir.

GSM teknolojisinin güvenliği, var olduğu andan itibaren araştırmacıların ilgi odağında olmuştur. Ancak, GSM'in güvenlik problemleri hala devam etmektedir. Bu problemlerden bir tanesi, uçtan uca kriptolama kullanılmaması; ikincisi büyük gökkuşağı tabloları (rainbow tables) ile saldırılabilen GSM hava arayüzündeki (um interface) kriptozafiyeti [3]; üçüncüsü ise, Mobil Terminal (MT) ve Baz İstasyonu (BTS) arasında karşılıklı doğrulamanın olmamasıdır. Karşılıklı doğrulama eksikliğini kullanarak tele kulak, MT kimliği çalınması ve seçici yakalama (selective interceptor) saldırıları gibi çeşitli sahte BTS saldırıları yapılabilmektedir. Sahte BTS atakları MT kimliği çalma gibi nispeten tehlikesiz olabileceği gibi insansız hava araçlarının sahte BTS saldırısı kullanarak MT'nin yerini kestirip hava saldırısı yapması gibi ölümcül de olabilmektedir [4]. Bu çalışmada, GSM'in karşılıklı doğrulama zafiyeti ve bu zafiyeti istismar eden sahte BTS saldırıları ele alınacaktır.

Konu ile ilgili literatürde sahte BTS saldırılarının nasıl geliştirileceğine dair çeşitli çalışmalar olmasına rağmen, sahte BTS saldırılarının tespit edilip kullanıcının uyarılmasına yönelik pek bir çalışma bulunmamaktadır. Bu nedenle, sahte BTS saldırılarına karşı önlemlerin geliştirilmesi ve MT kullanıcısının sahte BTS ataklarına karşı uyarılması önem arz etmektedir. Bu çalışmayla, sahte BTS saldırı teknikleri analiz edilmekte ve bu saldırıların tespit edilmesine yönelik bir algoritma önerilmektedir.

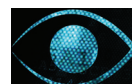
Çalışmanın diğer bölümlerinin içerikleri şöyle özetlenebilir. İkinci bölümde, sahte BTS saldırıları ile ilgili çalışmalar incelenmiştir. Üçüncü bölümde, ilgili GSM protokollerinin analizi yapılmış ve sahte BTS saldırı tespit algoritması önerilmiştir. Dördüncü bölümde, sahte BTS algoritmasının simülasyonu yapılmıştır. Beşinci bölümde ise sonuç ve yapılması planlanan işlere yer verilmiştir.

II. İLGİLİ ÇALIŞMALAR

Yapılan literatür araştırmaları sonucunda sahte BTS saldırılarının tespit edilmesine yönelik çalışmalara rastlanmamasına rağmen, sahte BTS saldırıları ile ilgili incelenen çalışmalar aşağıda özetlenmiştir.

[5] numaralı çalışmada, konferans salonları veya uçaklar gibi MT'lerin aktif olmaması gereken alanlarda, MT'lerin tespit edilip yasaklanması için bir sistem geliştirilmiştir. Çalışmaya göre, MT'ler birkaç durumda kendini şebekeye

Ömer Faruk ÇELİK, Ankara Üniversitesi, Bilgisayar Mühendisliği, Ankara, Türkiye (email:cengofc@gmail.com)
Refik SAMET, Ankara Üniversitesi, Bilgisayar Mühendisliği, Ankara, Türkiye (email:samet@eng.ankara.edu.tr)



tanıtmaktadırlar, yani kendilerine özgü olan IMSI (International Mobile Subscriber Identity) numaralarını şebekeye bildirmektedirler. Bu çalışmada yazarlar bu durumların 3'ünden bahsetmişlerdir: 1) Gelen/giden aramalarla; 2) Zamanlayıcıların (T3211, T3213 ve T3212) süresinin dolmasıyla; 3) Yeni bir bölgeye (Location Area) girilmesiyle. Birinci durum için, MT'nin kendini şebekeye tanıtması RF alıcılar ile tespit edilebilmekte ancak uygulanabilir olmamaktadır. İkinci durumda MT'nin kendini şebekeye tanıtmasının yakalanması zordur çünkü söz konusu zamanlayıcıların süresi her GSM operatöründe değişiklik göstermekte ve bu süreler genellikle saat mertebesinde olmaktadır. Çalışmanın hedefi üçüncü durumla ilgili olup, bu durumun 2 adımı vardır. İlk adım, [6] yardımıyla hedef alandaki bütün aktif BTS'leri devre dışı bırakmaktır. İkinci adım ise, farklı bir LAI (Location Area Identifier) değerine sahip sahte BTS kullanmaktır. Çalışmaya göre, MT ile gerçek BTS'lerin bağlantısı kesildiğinde, MT otomatik olarak yeni BTS'ler arayacaktır. MT'nin bulabileceği tek BTS ise sahte BTS olacaktır. Sonrasında, MT sahte BTS'e bağlanacak ve BTS'in LAI değerinden farklı bir bölgeye ait olduğunu değerlendirecektir. Farklı bölgedeki BTS'e bağlanması lokasyon güncelleme sürecini başlatacak ve MT'nin kendini sahte BTS'e tanıtmasına sebep olacaktır. Bu bilgiler ışığında, sahte BTS saldırılarının anlaşılması için beklenmedik LAI değişiklikleri takip edilmelidir.

[7] numaralı çalışmada, GSM protokolünü hedef alan gerçek zamanlı dedektör sistemi geliştirilmiştir. Geliştirilen dedektör sistemi 3 parçadan oluşmaktadır. Birinci parça, [5]'de geliştirilen "GSM MT dedektörü", ikincisi lokal veri tabanı, üçüncüsü ise seçici yakalama (selective interceptor) cihazıdır. Çalışmayla, belirli bir bölge içinde kalan MT'ler "GSM MT Dedektörü" ile tespit edilmekte ve tespit edilen MT kimlikleri lokal veri tabanında toplanmaktadır. Sonrasında ise, MT'ler lokal veri tabanından kontrol edilerek seçici olarak engellenip bırakılabilmektedir. Bu çalışmada, [5]'e ek olarak MT'nin kendini ağa tanıtması için 2 yöntem daha kullanılmıştır. Bunlar ise, MTlerin açılışa ve çağrı düşüp tekrar bağlanmak istediğinde yaptığı lokasyon güncelleme istekleridir.

[8] ve [9]'da, yazılımsal radyo teknolojisi (software radio technologies - SDR) kullanılarak sahte BTS geliştirilmiştir. Bu çalışmada, [5] ve [7]'nin aksine sahte BTS geliştirilirken, gerçek BTS'ler sinyal bozucu (jammer) ile engellenmemiştir. Ayrıca, sahte BTS geliştirilirken farklı bir yaklaşım ve yazılımsal radyo teknolojisi kullanılması hem masrafları düşürmüş hem de performansı önemli oranda artırmıştır. Geliştirilen sistemde bir tane mühendislik moduna sahip MT kullanılmıştır. Söz konusu MT ile çevredeki aktif BTSler tespit edilebilmektedir. Tespit edilen BTS'ler hücre seçilme kriteri olan C2 parametresine göre (cell reselection criterion) güçlüden zayıfa sıralanmaktadır. Sahte BTS bahse konu MT'den BTS'lere ait bilgileri alıp, ortamdaki en zayıf BTS gibi davranmakta ve hedef MT'lerin kendisine bağlanmasını sağlamaktadır. Gerçek BTS'in taklit edilmesinin sebebi, normal BTS'lerin komşu BTS'lere ait bilgileri BCH (Broadcast Channel) kanalından yayınlamalarıdır. Böylece MT'ler tereddüt etmeden sahte BTS'e bağlanmaktadır. Sahte BTS,

taklit ettiği BTS'in MCC (Mobile Country Code) ve MNC (Mobile Network Code) gibi GSM operatörlerine ait olan bilgilerini de taklit etmelidir. Bu nedenle, her GSM operatörü için ayrı sahte BTS kullanılmalıdır. Bununla birlikte, MT'nin kendini sahte BTS'e tanıtması için MT'lerde lokasyon güncelleme prosedürü tetiklenmelidir. Söz konusu tetiklenme için sahte BTS'in LAI değeri gerçek BTS'lerden farklı olmalıdır. Çalışmadaki en kritik bölüm, sahte BTS'in yayın yapan en güçlü BTS olmasa bile kendini MT'lere seçtirebilmesidir. MT'ler, her 5 saniyede BTS'lerin BCCH (Broadcast Control Channel) kanalını okuyup, C2 parametresine göre BTS'leri güçlüden zayıfa dizmektedir. MT için BTS seçimi BTS'lerin C2 parametrelerine göre yapılmaktadır. C2 parametresi MT'nin BTS'e yakınlığı ve bazı ofset değerleri ile hesaplanmaktadır. Ofset değerlerine pozitif/negatif değerler verilerek MT'nin spesifik bir BTS'i seçimi teşvik edilebilmekte veya engellenebilmektedir. Çalışmada, geliştirilen sahte BTS, C2 parametresini değiştirilerek MT'lerin kısa sürede kendisine bağlanmalarını sağlayabilmiştir. Ayrıca, farklı LAI kullanarak MT'lerde lokasyon güncelleme prosedürü tetiklenebilmiştir. Sonuç olarak, sahte BTS saldırılarının tespit edilebilmesi için sıra dışı C2 değerleri önemli bir gösterge olacaktır. Ayrıca, zayıf olan BTS'in beklenmedik şekilde seçilmesine de dikkat edilmelidir.

Sahte BTS saldırısı, BTS ve MT arasında gerçekleşen bir tür man-in-the-middle saldırısıdır. Yukarıdaki çalışmalara göre, sahte BTS saldırıları için MT'nin BTS'e bağlanması gerekmektedir. Bu bağlantının sağlanması için C2 parametresinin manipüle edilmesi önem arz etmektedir. Ayrıca farklı bir LAI kullanarak MT'nin kimliğinin alınması da gerekmektedir. Sahte BTS saldırı tespit algoritması yukarıdaki yaklaşımlar göz önünde bulundurularak geliştirilmiştir.

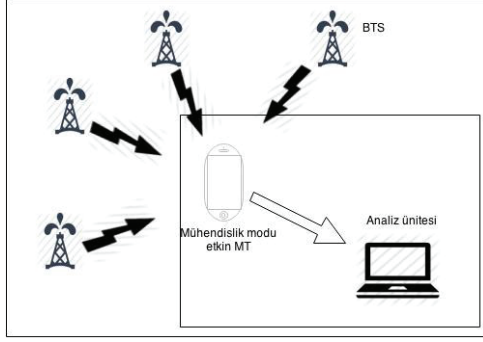
III. SAHTE BAZ İSTASYONU SALDIRI TESPİT ALGORİTMASI

A. Sistem Mimarisi

Önceki bölümlerde bahsedildiği gibi literatür araştırmalarında sahte BTS saldırıları ile ilgili çalışmalar olmasına rağmen, bu saldırıların tespit edilmesine yönelik çalışmaya rastlanılmamıştır. Bu makale, sahte BTS saldırılarının tespiti alanına katkıda bulunacaktır.

Önerilen sistem mimarisi Şekil 1'de verilmektedir.

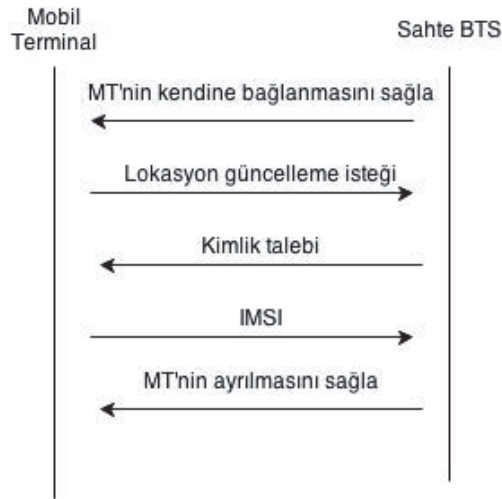
Şekil 1'deki MT, kendi bölgesindeki aktif BTS'leri tespit edip, Cell ID ve LAI gibi bilgileri almak için her BTS'in BCCH kanalını okumaktadır. MT, BTS'lerden topladığı bilgileri "Analiz Ünitesine" yollamaktadır. MT, BTS'lerden okuduğu bilgiyle otomatik olarak hesapladığı C1 (path loss criterion parameter) ve C2 parametrelerini de analiz ünitesine göndermektedir. Analiz ünitesi olarak, geliştirilen algoritmayı çalıştırabilecek herhangi bir PC veya akıllı telefon kullanılabilmektedir. Analiz ünitesi, MT'nin gönderdiği verileri sahte BTS saldırı tespit algoritmasına göre değerlendirip, şüpheli durumlar için kullanıcıyı uyarmaktadır.



Şekil 1: Sistem Mimarisi.

Basit bir sahte BTS saldırısı Şekil 2'deki gibi olmaktadır.

İkinci bölümde ve [10]'da açıklandığı üzere, MT'lerde lokasyon güncelleme tetiklenebilmesi için sahte BTS'in gerçek BTS'lerden farklı bir LAI değeri olmalıdır. MT'nin lokasyonunun takip edildiği durumlarda ise sahte BTS MT'yi tekrar tekrar yakalamak zorundadır. Yani MT'deki LAI değerinin beklenmedik şekilde değişmesi de tespit algoritması için parametre olacaktır.



Şekil 2: Örnek Sahte BTS Saldırısı

B. Protokol Analizi

Sahte BTS saldırıları için, MT'nin yakalanması ve bırakılması çetin bir iştir. [5] ve [7]'de bu iş için sinyal bozucu sistemler kullanılmıştır [6]. Fakat bu sistemlerde her BTS için ayrı bir sinyal bozucu ünite gerekmekte ve sinyal bozucunun zamanlamasını ayarlarken zorluklarla karşılaşmaktadır. Ancak, C2 parametresinin manipüle edilerek kullanılması, hem masrafı düşürmekte hem de performansı önemli ölçüde artırmaktadır [8]. [9] ve [11]'e göre C1 parametresi hücre seçiminde kullanılmakta ve aşağıdaki gibi hesaplanmaktadır.

$$C1 = (A - \max(B, 0)) \quad (1)$$

$$A = RLA_C - RXLEV_ACCESS_MIN \quad (2)$$

$$B = MS_TXPWR_MAX_CCH - P \quad (3)$$

Sınıf 3 DCS 1800'ler için,

$$B = MS_TXPWR_MAX_CCH + POWER_OFFSET - P \quad (4)$$

Yukarıdaki formüllerde;

RLA_C ulaşılan ortalama değerler;

RXLEV_ACCESS_MIN MT'nin sisteme erişmesi için gerekli minimum sinyal seviyesi;

MS_TXPWR_MAX_CCH MT'nin sisteme erişmesi için gerekli olan en fazla TX güç seviyesi,

POWER_OFFSET MS_TXPWR ile karşılıklı olarak kullanılan güç ofset değeri ve

P ise MT'nin maksimum RF güç çıkışıdır.

Bütün değerler dBm formatındadır ve yukarıdaki tanıma göre, C1 değeri MS ve BTS arasındaki mesafe ile ters orantılıdır. C2 parametresi ise hücre seçimi için kullanılır ve aşağıdaki gibi tanımlanır [11].

PENALTY_TIME > 11111 için,

$$C2 = C1 + CELL_RESELECT_OFFSET - TEMPORARY_OFFSET * H(PENALTY_TIME - T) \quad (5)$$

PENALTY TIME = 11111 için,

$$C2 = C1 - CELL_RESELECT_OFFSET \quad (6)$$

Komşu hücreler için,

$$H(x) = 0 \text{ for } x < 0 \quad (7)$$

$$H(x) = 1 \text{ for } x \geq 0 \quad (8)$$

Hizmet veren hücre için,

$$H(x) = 0 \quad (9)$$

T, hesaplanan en güçlü BTS'ler listesinde her BTS için tutulan zamanlayıcıdır.

CELL_RESELECT_OFFSET, TEMPORARY_OFFSET, PENALTY_TIME, CELL_BAR_QUALIFY değerleri opsiyonel olarak BTS'in BCCH kanalından yayınlanmaktadır. Eğer yayınlanmıyorsa olağan değerleri sıfıra eşittir ve bu şekilde C2=C1 olur. Türkiye'nin Ankara ilinde yapılan testlere göre her BTS için C1 ve C2 değerleri olağan koşullarda olduğu gibi birbirine eşit çıkmışlardır. Yukarıdaki hesaplamalara ve [12]'ye göre BTS'ler arasında öncelik tanıma yukarıda bahsedilen opsiyonel parametreler ile yapılmaktadır. Opsiyonel parametreler C2 değerini değiştirmek için kullanılabilir ve BTS'in hesaplanmış C2 değeri ne kadar yüksek olursa MT'nin BTS'i seçme ihtimali o kadar artar. C2 değerinin olağan dışı bir şekilde C1 değerinden farklı olması Şekil 3'de gösterilen sahte BTS tespit algoritması için önemli bir girdi olacaktır.

C. Algoritma Tasarımı

Şekil 3'de sahte BTS tespit algoritmasının akış şeması verilmektedir. Algoritma ağ değerlerini ve MT lokasyonunu değerlendirmektedir. Algoritmada 3 durum bulunmaktadır.

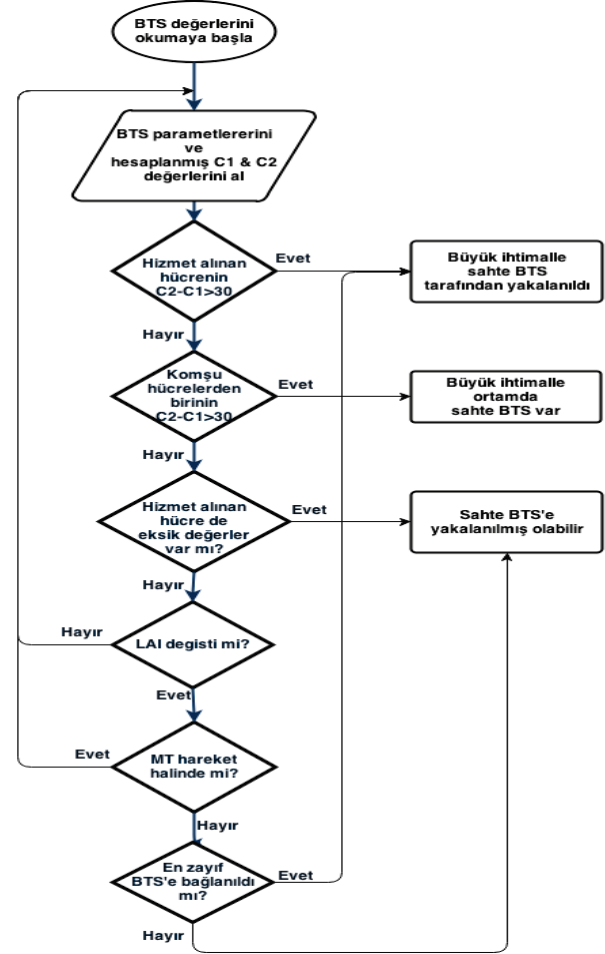
Birinci durum, C2 parametresinin manipülasyonu ile ilgilidir. Önceki bölümlerde açıklandığı gibi C2, ofset parametreleri değiştirilerek hücre seçimini etkilemek için kullanılabilir. MT'nin BTS'e uzaklığını gösteren C1 parametresi yüksek olmasa bile, yani sahte BTS hedef MT'ye en yakın BTS olmasa bile sahte BTS, C2 değerini manipüle ederek MT'lerin kendine bağlanmasını sağlayabilmektedir. [11] ve bu çalışma kapsamında yapılan testlere göre C1 ve C2

parametreleri sıra dışı bir durum olmadığı takdirde birbirine eşitlerdir. Bundan dolayı $C2-C1>30$ olması, sıra dışı bir duruma işaret etmektedir. Birinci durumun da 2 kısmı vardır. Birinci kısımda, hizmet veren hücrenin C2 ve C1 değerleri arasındaki farkın 30'dan fazla olması durumunda, Önerilen algoritma "MT'nin büyük ihtimalle sahte BTS'e yakalandığı" sonucuna varacaktır. İkinci kısımda ise, yani komşu hücrelerden bir tanesinin C2 ve C1 değerleri arasındaki farkın 30'dan büyük olması durumunda, Algoritma "büyük ihtimalle MT'nin yakınlarında sahte BTS çalışmaktadır" sonucuna varacaktır. 30 değeri hatalı pozitif (false-positive) sonuçları elemek için ve BTS-MT arasındaki hava arayüzünde yaşanması muhtemel sinyal bozulmalarını elemine edebilmek için seçilmiştir. Ayrıca, sahte BTS'in MT'leri daha hızlı yakalayabilmesi için C2 ve C1 arasındaki fark 30 değerinden çok daha büyük olmalıdır.

Algoritmadaki ikinci durum, sahte BTS'in eksik konfigürasyonu ile ilgilidir. BTS'ler kendisini tanıtan bazı değerleri BCH kanalından yayınlamak şeklinde yapılandırılmaktadır. Bu değerler arasında Cell ID, MCC, MNC, LAI ve çevredeki BTS'lere ait bilgiler bulunmaktadır [12]. Sahte BTS'in sahada kullanıldığı ve hareket halinde olduğu durumlarda komşu hücreler sürekli değişmekte ve saldırganın değişen komşu hücreleri güncellemesi zaman almaktadır. Bu nedenle, eksik yapılandırılmış BTS'in sahte BTS olması muhtemeldir. Eksik yapılandırılmış BTS için başka bir örnek ise sahte BTS için hiç var olmayan bir Cell ID seçilmesidir [5]. Eğer bağlanılan BTS daha önceki BTS'lerin komşu hücreler listesinde yoksa bağlanılan hücre sahte BTS olabilir. Bunlara ek olarak, hizmet veren hücre o alanda yayın yapan tek hücre ise ve diğer komşu hücrelere ait değerler hizmet veren hücre tarafından yayınlanmıyorsa, diğer BTS'ler sinyal bozucu ile bastırılmış olabilir [7] ve yalnızca bağlanılan sahte BTS'e izin verilmiş olunabilir.

Üçüncü durum farklı LAI kullanılmasını analiz etmektedir. MT'nin kimliğinin alınabilmesi için sahte BTS, MT'de lokasyon güncelleme prosedürünü tetiklemelidir. Yukarıda anlatıldığı gibi, MT'de lokasyon güncelleme prosedürünü tetiklemek için sahte BTS, hizmet veren hücreden farklı bir LAI kullanmalıdır. Bu nedenle, MT hareket etmezken gerçekleşen LAI değişiklikleri şüpheli karşılanmalıdır. Ayrıca, sahte BTS ortamdaki en zayıf BTS'i seçip onun yerine geçmektedir [8], [9]. [9]'da tasarlandığı gibi eğer MT hareket etmiyorsa ve önceki durumda en zayıf olan BTS'e bağlandıysa ve üstüne LAI değişikliği olduysa, MT büyük ihtimalle sahte BTS'e bağlanmış diyebiliriz. Bağlanılan BTS en zayıf olmasa bile eğer MT hareket etmiyorsa ve LAI değişikliği olduysa da sahte BTS'e yakalanmış olabilir.

Sonuç olarak, bahse konu senaryolar çeşitli alarmlar üretmektedir. Algoritmanın bir döngüsünde sadece bir alarm üretilebileceği gibi birden çok alarm da üretilebilmektedir. Algoritma devamlı çalışmalı ve karar yukarıda bahsedilen durumların hepsi göz önünde bulundurulduktan sonra verilmelidir. Sahte BTS tespit algoritmasının yardımıyla, ortamda sahte BTS saldırısının tespitine yönelik alarmlar üretilmekte ve üretilen alarmlar saldırıya maruz kalınmış olunmasına dair önemli ipuçları vermektedir.



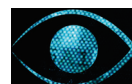
Şekil 3: Sahte BTS Saldırı Tespit Algoritması

IV. GELİŞTİRİLEN ALGORİTMANIN SİMÜLASYONU

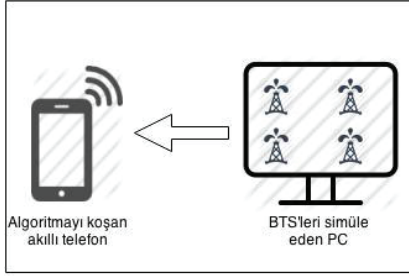
Bu bölümde geliştirilen algoritmanın simülasyonu yer alacaktır. Gerçek ve sahte BTS'leri simüle eden bir program geliştirilip algoritma bu programla test edilmiştir.

BTS'leri simüle eden program Java ile geliştirilmiş olup standart bir PC'de çalışmaktadır. Şekil 1'de bulunan hem Mobil Terminal hem de Analiz Ünitesi için ANDROID işletim sistemi 4.4.4 sürümüne sahip Google Nexus 4 akıllı telefon kullanılmıştır. PC ve akıllı telefon arasındaki iletişim, akıllı telefon tarafından oluşturulan geçici Wi-Fi erişim noktası üzerinden sağlanmaktadır. Geliştirilen algoritma akıllı telefon üzerinde çalışmakta ve algoritma neticesinde oluşan alarmlar akıllı telefonda gösterilmektedir. Simülasyonun mimarisi Şekil 4'de gösterilmektedir.

Algoritmayı çalıştıran ANDROID uygulaması periyodik olarak çalışmakta ve PC tarafından simüle edilen BTS'lerin bilgilerini okumaktadır. Sonrasında, uygulama BTS'den gelen verileri algoritmaya göre değerlendirmekte ve alarmları oluşturmaktadır. Eğer birden çok alarm üretildiyse, uygulama en ciddi olanı ekranda gösterip diğerlerini de bilgi olarak göstermektedir. Algoritmanın döngüleri 30 saniyede bir çalışmaktadır. Her döngüde önce simüle edilen BTS verileri okunmakta, sonrasında akıllı telefonun dahili GPS modülü kullanılarak lokasyon değişikliği hesaplanmaktadır. Ayrıca



okunan bu değerler belirli bir süre akıllı telefonda tutulmakta ve algoritma tarafından değerlendirilip sonuç üretilmektedir.



Şekil 4: Simülasyon Mimarisi

Akıllı telefonda çalışan sahte BTS tespit algoritması Bölüm 3'de anlatılan durumlarla karşılaştığında 3 şekilde uyarıda bulunmaktadır. Birincisi, “yüksek ihtimalle sahte BTS’e yakalandınız” uyarısıdır. Bu uyarıda, MT'nin hizmet aldığı hücre büyük ihtimalle sahte BTS'dir ve yapılan saldırı başarıya ulaşmıştır. İkincisi, “yüksek ihtimalle ortamda sahte BTS çalışmaktadır” uyarısıdır. Bu uyarıda ise komşu hücrelerden birisi büyük ihtimalle sahte BTS'dir ve MT sahte BTS'e yakalanmak üzere olabilir. Üçüncüsü, “sahte BTS'e yakalanılmış olabilir” uyarısıdır. Bu uyarıda ise hizmet alınan hücrenin sahte BTS olma ihtimali vardır. Algoritmanın çalışma döngüsü olarak 30 saniye seçilmiştir, çünkü [9]'da sahte BTS'in telefonların çoğunu yakalaması yaklaşık 40 saniye sürmüştür. Tespit algoritmasını 30 saniyede bir çalıştırarak mevcut saldırıların kaçırılmaması sağlanmaya çalışılmıştır. Gerçek ortamda test edilmesi durumunda, BTS'lerin BCH kanalının okunması zaman alacağı için uygulamanın daha sık çalıştırılması gerekecektir.

Simülasyon algoritmada belirtilen durumları kapsayacak şekilde yapılmıştır. Algoritmadaki birinci durum için 10 tane BTS simüle edilmiş, uygulama gerçek bir MT'de olması gerektiği gibi en yüksek C2 değeri olan 6 BTS'i [11] işleme almıştır. Algoritmayı koştan uygulama, hizmet alınan BTS'deki C2 ve C1 değerleri arasındaki farkın 30'dan büyük olması halinde “Yüksek ihtimalle sahte BTS’e yakalandınız” uyarısı vermiş; komşu BTS'lerin birisindeki C2 ve C1 değerleri arasındaki farkın 30'dan büyük olduğu durumlarda ise “Yüksek ihtimalle ortamda sahte BTS çalışmaktadır” uyarısını vermiştir. İkinci durum için ise; en güçlü 6 BTS içinde farklı MCC veya MNC değerleri olan BTS varsa veya diğer hücrelerin komşu listesinde yayınlamadığı bir Cell ID değerli BTS varsa “Sahte BTS’e yakalanılmış olabilir” uyarısı verilmiştir. Üçüncü durum için ise, MT lokasyon olarak sabit tutulup, MT'nin en zayıf BTS'e farklı LAI değeriyle bağlanmasının sağlandığı durumda “Yüksek ihtimalle sahte BTS'e yakalandınız” uyarısı alınmıştır. MT'nin lokasyonu değiştirilerek, aynı senaryo tekrar edildiğinde ise “Sahte BTS'e yakalanılmış olabilir” uyarısı alınmıştır. Algoritma 30 saniyede bir çalıştığı için lokasyon değişikliği MT'nin hızlı yer değiştirdiği durumları ele almaktadır. Ancak kırsal alanlarda BTS sıklığı azaldığından algoritma yanıltıcı sonuç verebilmektedir. Yapılan testler sonucunda simülasyonun hedef senaryolara karşı beklenen alarmları ürettiği tespit

edilmiştir. Ayrıca, simüle edilen BTS verilerinde sıra dışı bir durum olmadığında algoritmanın uyarı vermediği de gözlemlenmiştir. Algoritmayı çalıştıran MT'nin gerçek veya simüle edilen BTS'lerle çalıştığında aynı verileri işleyecek olmasından dolayı benzer sonuçlar üretmesi beklenmektedir.

Akıllı telefonda çalışan uygulamanın sahte BTS cihazına karşı çalışabilmesi için BTS'lerin verilerini okuyan kısmın değiştirilmesi gerekmektedir. Veri okuma kısmının değiştirilmesi için ya akıllı telefonun radyo modülü kullanılmalı ya da akıllı telefona BTS değerlerini okuyabilen harici bir cihaz bağlanması gerekmektedir. Geliştirilen uygulama yalnızca bir GSM operatörü için kullanılabilmektedir. Geliştirilen uygulamanın bütün GSM operatörleri için kullanılabilmesi için her operatöre ait BTS verilerinin okunabilmesi ve algoritmanın her operatör için tekrar işletilmesi gerekmektedir.

V. SONUÇ

Bu çalışmayla sahte BTS saldırıları analiz edilmiş ve bu saldırıların tespit edilmesine yönelik algoritma geliştirilmiştir. Geliştirilen algoritma simülasyon ortamında test edilip hedef durumlar için algoritmanın beklenen sonuçları ürettiği gözlemlenmiştir. Sahte BTS saldırıları geliştirilmesi konularında çalışmalar olmasına rağmen, sahte BTS saldırılarının tespitine yönelik çalışmaya literatür taramasında rastlanmaması geliştirilen algoritmanın önemini artırmaktadır. Ayrıca, sahte BTS cihazlarının gelişen teknoloji ile kolayca yapılabilmesi, hedefinin GSM gibi oldukça yaygın kullanılan bir teknoloji olması ve sahte BTS saldırıları ile tele kulak ve yer tespiti gibi saldırılar yapılabilmesi de saldırı tespit çalışmasının ne kadar gerekli olduğunu göstermektedir.

Simülasyon algoritmanın nasıl çalıştığını göstermesine rağmen sahte BTS cihazı ile test edilmesi yapılacak işler arasında en önde gelmektedir. Ek olarak, günümüzde üçüncü nesil (3G) oldukça yaygın kullanılmaya başlanmış olup dördüncü nesil (4G) ise gittikçe yaygınlaşmaktadır. Benzer saldırılar 3G ve 4G için de yapılmakta veya saldırı çalışmaları devam etmektedir. Bu saldırılara karşı benzer tespit sistemlerinin geliştirilmesi de yapılması gereken çalışmalar arasındadır.

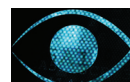
KAYNAKLAR

- [1] Wikipedia, “GSM”, (2014, Ağustos) <http://en.wikipedia.org/wiki/GSM>,
- [2] F.V.D. Broek “Eavesdropping on GSM: State-of-affairs” 5th Benelux Workshop on Information and System Security (WISSec, Kasım, 2010)
- [3] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou ve C. Manifavas “Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAs” Field Programmable Logic and Applications (FPL), 22nd International Conference-IEEE, 2012.
- [4] J.Scahill ve G. Greenwald “The NSA's Secret Role in the U.S. Assassination Program” (Haziran,2014) <https://firstlook.org/theintercept/article/2014/02/10/the-nsa-secret-role/>
- [5] J. Vales-Alonso, F. I. de Vicente, F. J. González-Castaño, and J.M. Pousada-Carballo, “Real-time detector of GSM terminals” IEEE Commun.Lett., vol. 5, pp. 275–276, 2001.
- [6] J.M. Pousada-Carballo, F. J. González-Castaño, F. I. de Vicente, and M.J. Fernández-Iglesias, “Jamming system for mobile communications,”Electron. Lett. vol. 34, pp. 2166–2167, 1998.

- [7] J.F. González-Castaño, J. Vales-Alonso, J. M. Pousada-Carballo, F. Isasi de Vicente ve M.J. Fernández-Iglesias, “Real-Time Interception Systems for the GSM Protocol,” IEEE Transactions on Vehicular Technology, vol. 51, no. 5, Eylül 2002.
- [8] K. Zhou, A. Hu, Y. Song “ A No-Jamming Selective Interception System of the GSM Terminal” 6th International Conference on Wireless Communications Networking & Mobile Computing (WiCOM); 2010, p1-4, 4p 2010
- [9] Y. Song, K. Zhou, X. Chen “Fake BTS Attacks of GSM System on Software Radio Platform” Journal of Networks, vol. 7, no. 2, Şubat 2012
- [10] ETSI “European Digital cellular telecommunications system (Phase 1); Location Registration Procedures, (GSM 03.12-DCS version 3.0.1 Release 1992)
- [11] ETSI “Digital cellular telecommunications system (Phase 2+); Radio subsystem link control, (GSM 05.08 version 8.5.0 Release 1999),” Document ETSI TS 100 911 V8.5.0 (2000-10)
- [12] ETSI “Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode, (GSM 03.22 version 5.3.1 Release 1996),” Document ETS 300 930 December 1998

Ömer Faruk Çelik Orta Doğu Teknik Üniversitesi Bilgisayar Mühendisliği Bölümünden 2009 yılında mezun olmuştur. Ankara Üniversitesi Bilgisayar Mühendisliği bölümünde yüksek lisans eğitimine devam etmektedir. İlgili alanları; bilgi/ağ güvenliği ve büyük veri sistemleridir.

Refik Samet 1983 yılında Ukrayna Ulusal Teknik Üniversitesi Kiev Politeknik Enstitüsünde, teknik sistemlerde otomasyon ve kontrol sistemleri konularında lisans ve yüksek lisans eğitimini tamamlamıştır. 1992 yılında Rusya Bilim Akademisi Kontrol Bilimleri Enstitüsünden Bilgisayar Bilimleri alanında Doktora derecesini almıştır. Ankara Üniversitesi, Bilgisayar Mühendisliği Fakültesinde Doçent ünvanı ile bilimsel hayatına devam etmektedir. Güncel ilgi alanları içerisinde Hata-Tolerans sistem analizi, görüntü işleme, web tabanlı bilgi sistemleri ve gerçek zamanlı modelleme bulunmaktadır. 2000 yılından beri IEEE ve Computer Society’ye üyedir.



Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT

Ammar Jameel Hussein, Seda Yuksel, and Ersin Elbasi

Abstract – In order to achieve a good imperceptibility and robustness, using 4-level DWT algorithm based on dynamic binary host image location and embedding two watermark logos in different DWT levels are proposed for copyright protection and authenticity. In the propounded watermarking algorithm, 5-level DWT is applied to host image to obtain the fifth low frequency sub band (LL5), and examination the dynamic binary location value of selected location for embedding purpose in five different locations in host image using the same algorithm process. Our experimental results demonstrate that our algorithm scheme is imperceptible and robust against several image processing attacks, and watermarked image quality evaluating by calculation of SNR, PSNR, RMSE, and MAE.

Index Terms—Copyright Protection, Discrete Wavelet Transforms, Information Security, Frequency-domain Analysis, Watermarking

I. INTRODUCTION

THE idea of Internet of thing or Internet of everything [1] makes a digital achievement, transmission of digital media is not a simple task. Proving the ownership of digital multimedia being transmitted introduces the requirement of having a robust watermarking scheme, to satisfy this growing necessity. Mostly, an operational digital watermarking scheme should meet elementary requirements which are:

- 1) Imperceptibility: Watermark cannot be realized by human sense, only can be perceived over special handling [6]. In addition, watermarks should not interfere with the media being protected [2].
- 2) Trustworthiness [2]: Assurances that it is difficult to generate counterfeit watermarks, and they should provide trustworthy proof to keep the legal ownership.
- 3) Capacity [6]: This defines how many information bits that can be embedded. Additionally, statements the possibility of embedding multiple watermarks in one object.
- 4) Robustness [6]: The watermark should be robust against general signal processing attacks and malicious operation.

Manuscript received June 29, 2014.

Ammar Jameel Hussein is with the Department of Computer Engineering, Iraqi Board of Supreme Audit, Baghdad, Iraq (email: ammar.jameel.ict@gmail.com).

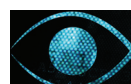
Seda Yuksel is with the Department of Computer Engineering, Çankaya University, Ankara, Turkey (e-mail: seda.yuksel.sy@gmail.com).

Ersin Elbasi is with the Department of Digital Game Design, Ipek University, Ankara, Turkey (e-mail: eelbasi@ipek.edu.tr).

Digital watermarking [3] is a relatively new study zone that attracts the attention of various researchers in academic and business world. This becomes one of the most up-to-date research topics in the multimedia signal processing community. The term of watermarking has a little different meaning, one definition gives the impression to overcome the following [4]: Watermarking is the process of imperceptibly modifying a part of data so as to embed info around the data. The above definition mentions two important features of watermarking. Initially, information embedding should not cause visible changes to the second host medium; the message should be associated to the host medium [5]. Digital watermarking can be classified regarding to several of classes which are [6]:

- 1) Characteristics, robustness (Robust, Fragile and Semi-fragile)
- 2) Attached media, host signal (Image watermarking, Video watermarking, Audio watermarking, Text watermarking and Graphic watermarking)
- 3) Perceptivity (Visible watermark and Invisible watermarking)
- 4) Purpose (Copyright protection watermarking, Tampering tip watermarking, Anti-counterfeiting watermarking and Anonymous watermarking)
- 5) Watermark type (Noise type and Image type)
- 6) Detection process (Visual watermarking, Semi blind watermarking and Blind watermarking)
- 7) Use of keys (Asymmetric watermarking and Symmetric watermarking)
- 8) Domain (Spatial domain and Frequency domain)

Reviewing a previous work, we realize that, Dugad et al. [7] offered discrete wavelet transform based structure for embedded the watermark in low - low (LL) band, coefficients in similar method by way of Cox et al. that had been previously offered by Elbasi and Eskicioglu [8] embedded a pseudorandom sequence as a watermark in two bands (LL and HH) by using DWT [9]. P. Kumhom et al. [10] applied a non-blind watermark scheme that focused on collection the high frequency variety that holds huge sum of information. While Jila Ayubi et al. [11] proposed a watermark scheme built on chaotic maps and DWT, P. Kumar et al et al. [12] used (Haar wavelet) structure designed for rebuilding filter banks, skimming data according to Least Significant Bits of the coefficient. Parthiban V. and Ganesan R. [13] enhanced the robustness of his scheme through grouping of DWT and Singular Value Decomposition (SVD) technique.



DYNAMIC BINARY LOCATION BASED MULTI-WATERMARK EMBEDDING ALGORITHM IN DWT

In our paper, we focus on domain based watermarking techniques (i.e. spatial domain and Frequency domain). Spatial domain watermark indicates fewer confrontations in contradiction of several image processing operations [14], henceforth, termed as a fragile watermarking. Despite the fact that frequency domain techniques like discrete wavelet transform (DWT) [15], discrete Fourier transforms (DFT) [16], and discrete cosine transform (DCT) [17] offer more robustness.

II. DISCRETE WAVELET TRANSFORMS

Wavelets are discovered by Daubechies (1988, 1992) which have been proved to be as successful as the FBI's chosen method of compression for fingerprint data (Brislawn, 1995) [18].

Wavelet transform in two dimensional can be stated as a two dimensional scaling function $\phi(x, y)$ and three two dimensional wavelets $\psi^H(x, y), \psi^V(x, y), \psi^D(x, y)$

Wavelet transform of an image $A(x, y)$ of size is $M \times N$ defined by:

$$W_\phi(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A(x, y) \phi_{j_0.m.n}(x, y) \quad (1)$$

$$W_\psi^i(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A(x, y) \psi^i_{j.m.n}(x, y) \quad (2)$$

Where $i = [H, V, D]$ and j_0 is a random scale.

$W_\phi(j_0, m, n)$ Defines low frequency coefficients of $A(x, y)$,

At scale, j_0 and $W_\psi^i(j, m, n)$ define the horizontal, vertical and diagonal details for scale $j \geq j_0$ [19].

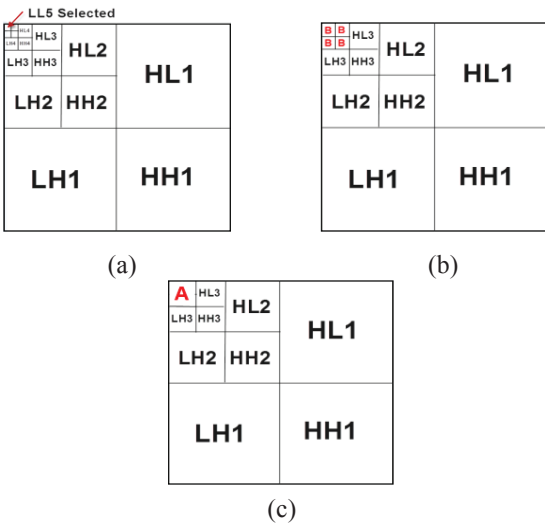


Fig. 1. (a) DWT fifth level of decomposition (b) DWT third level of decomposition and position of first watermark logo (c) DWT fourth level decomposition and position of second watermark

The purpose of DWT idea is to decompose a signal into different resolutions. The lowest frequency sub band includes the almost significant information about the image. While high frequency sub bands include the image details [20]. Fig. 1(a) shows the selection criteria of fifth level DWT decomposition, Fig. 1(b) presents embedding criteria. The first watermark is embedded in the third level of DWT decomposition in (LL3) sub band, while Fig. 1(c) shows the second four watermarks was embedded in the fourth level of DWT decomposition in (LL4, HL4, LH4, HH4) sub bands. They are distributed in different locations inside the image space, and this will improve the robustness and the security of the system.

III. THE PROPOSED SCHEME

In this section of the paper, 5-level DWT based watermarking scheme which uses scaling and translation characteristics of wavelet domain in different levels. Examination of the LL5 sub band acquires a low frequency gray value, then it is transferred it to binary (0, 1) values for the host image. The embedded first watermark logo in LL3 sub band and embedded second watermark logo in all (LL4, HL4, LH4, and HH4) sub bands. Embedding the watermark is shown in the proposed watermarking algorithm Fig. 2(a). The host image is a 512x512 and watermark is a 512x512, and it is applied with 4-level DWT decomposition for first and second watermark logos.

A. Algorithm: Watermark Embedding

- 1) Preparing the cover image with the size of (512x512), read the two watermark logos each with the size of (512x512).
- 2) Performing fifth level DWT using Haar wavelets and selecting LL5 sub band, converting it to gray image; then converting it to a binary image to get value position in forms of (0,1).
- 3) Performing fourth level DWT, for first and second watermark logos.
- 4) Examination of LL5 position value; if $LL5(i, j) == 0$, embedding first watermark logo in the host image to (LL3) sub band position.
- 5) Examination of LL5 position value; if $LL5(i, j) == 1$, then embedding second watermark logo in the host image to (LL4, HL4, LH4, HH4) sub bands position.
- 6) Performing third level IDWT, to reconstruct first watermarked image, and fourth level IDWT to reconstitute second watermarked image.

Let $f(i, j)$ be the original cover images, $w(i, j)$ is the first watermark image, and $w'(i, j)$ is the second watermark image. Then, $v(i, j)$ is the first watermarked image, and $v'(i, j)$ is the second watermarked image. Therefore,

DYNAMIC BINARY LOCATION BASED MULTI-WATERMARK EMBEDDING ALGORITHM IN DWT

$f'(i, j)$ is the watermarked image, the embedding is done, according to the following equations:

$$v(i, j) = f(i, j) + w(i, j) \quad (3)$$

$$v'(i, j) = f(i, j) + w'(i, j) \quad (4)$$

$$f'(i, j) = (v(i, j) + v'(i, j)) / 2 \quad (5)$$

B. Watermark Extraction

- 1) Prepare the original host image and the watermarked image.
- 2) Decompose both, host image cover and the watermarked cover with using the fourth level of DWT decomposition. Afterwards, subtract the bands to get the first watermark and four second watermark, the extraction equations are:

$$w(i, j) = f(i, j) - f'(i, j) \quad (6)$$

$$w'(i, j) = f(i, j) - f'(i, j) \quad (7)$$

Fig. 2 (b) shows the extraction process.

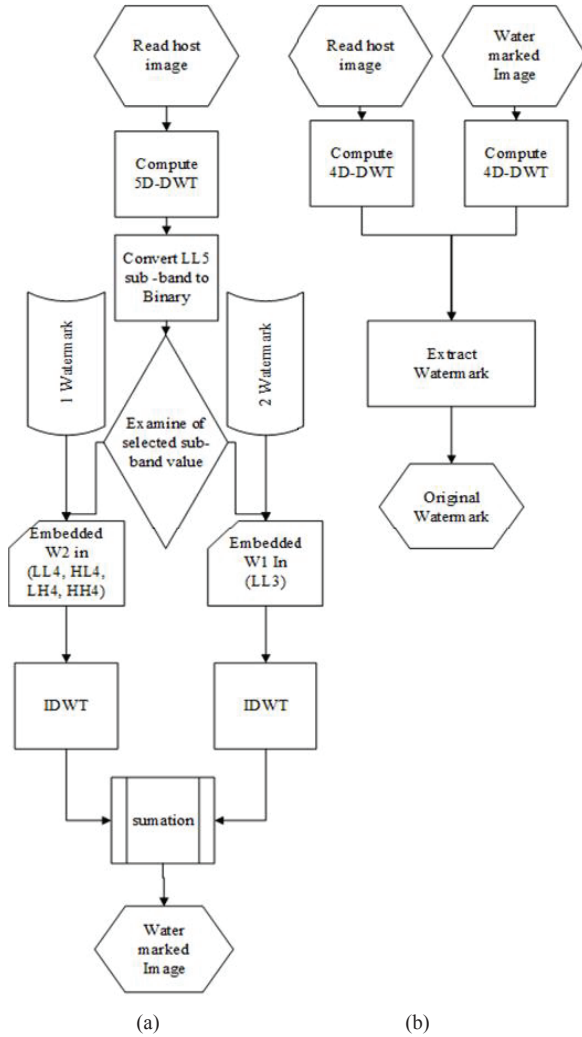


Fig. 2. (a) Embedding scheme

(b) Extraction process

IV. EXPERIMENTAL RESULTS

A number of experiments are performed to evaluate the performance of the proposed watermarking algorithm on different gray scale images of size 512x512 like mandrill, boxer, Boat, Goldhill, Lena and Barbara, using MATLAB platform. The results of two gray scale host images, mandrill and boxer along with used watermarked logo shown in Fig. 3, Fig. 4 and Fig. 5 respectively. Fig. 3 (a) - (b) show comparison between first host image and watermarked image, Fig. 5 (a) - (b) demonstrate comparison between second host image and watermarked image and Fig. 5 (a) - (b) demonstrate comparison between third host image and watermarked image, while Fig. 6 (a) and (b) present first watermark logo and second watermark logo.



Fig. 3 (a) Host Image



(b) Watermarked Image



Fig. 4. (a) Second host Image



(b) Watermarked Image



Fig. 5. (a) Third host Image



(b) Watermarked Image



Fig. 6. (a) First watermark logo



(b) Second watermark logo

A. Attacks

In our experiment, we apply ten types of attacks, which generate a comparison to prove the superiority of recommended scheme. MATLAB is used for all attacks. The chosen attacks are JPEG compression, resizing, adding Gaussian noise, low pass filtering, rotation, histogram

DYNAMIC BINARY LOCATION BASED MULTI-WATERMARK EMBEDDING ALGORITHM IN DWT

equalization, contrast adjustment, gamma correction, and cropping. The attacked images and the attack parameters for mandrill host image by using MATLAB are shown in Table - 1.

TABLE I
ATTACKED IMAGES, AND ATTACKED PARAMETERS

No.	Attacks	Parameters	Result Image
1.	Gaussian noise	(mean = 0, variance = 0.001)	
2.	Low pass filtering	(window size=3x3)	
3.	Cropping	on both sides	
4.	Scaling	512x256	
5.	Rotation	(20°)	
6.	Equalization	automatic	
7.	Adjustment	([l=0 h=0.8],[b=0 t=1])	
8.	Gamma	(1.5)	
9.	Jpeg compression	(Q = 50)	
10.	Noise	(0.02)	

B. Evaluation

The evaluation of watermarked image quality is measured by SNR, PSNR, RMSE, and MAE. In our experiment, we use image J's plugin to evaluate the quality of images [21]. This program calculates the SNR, PSNR, RMSE, and MAE of images or sequences of images depend on the definitions of Gonzalez [22]. The plugin matches a reference image $r(x, y)$ with a test $t(x, y)$. The two images should have the same size $[nx, ny]$, SNR, PSNR, RMSE, and MAE calculated by the given equations:

- 1) Signal-to-noise ratio (SNR) defined by the equation:

$$SNR = 10 \cdot \log_{10} \left[\frac{\sum_{x=0}^{Nx-1} \sum_{y=0}^{Ny-1} [r(x, y)]^2}{\sum_{x=0}^{Nx-1} \sum_{y=0}^{Ny-1} [r(x, y) - t(x, y)]^2} \right] \quad (8)$$

- 2) Peak signal-to-noise ratio (PSNR) defined by the equation:

$$PSNR = 10 \cdot \log_{10} \left[\frac{Max(r(x, y))^2}{\frac{1}{Nx \cdot Ny} \cdot \sum_{x=0}^{Nx-1} \sum_{y=0}^{Ny-1} [r(x, y) - t(x, y)]^2} \right] \quad (9)$$

- 3) Root mean square error (RMSE) defined by the equation:

$$RMSE = \sqrt{\frac{1}{Nx \cdot Ny} \cdot \sum_{x=0}^{Nx-1} \sum_{y=0}^{Ny-1} [r(x, y) - t(x, y)]^2} \quad (10)$$

- 4) Mean absolute error (MAE) defined by the equation:

$$MAE = \frac{1}{Nx \cdot Ny} \cdot \sum_{x=0}^{Nx-1} \sum_{y=0}^{Ny-1} [r(x, y) - t(x, y)] \quad (11)$$

In our experiment, we take many standard host images like mandrill, boxer, boat, Barbara, Lena, and Goldhill to test our watermarked schema along with applying ten type of attacks. After watermarking process, we calculate the SNR, PSNR, RMSE, and MAE shown in Table - 2 (a) (b), Table - 3 (a) (b), and Table - 4 (a) and (b).

TABLE II (A)
MANDRILL HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	47.5	51.76	0.5678	0.285
Gaussia.png	24.4	28.69	8.0891	6.450
Filter.png	26.7	30.94	6.2383	3.733
crop.png	6.11	10.34	66.892	32.88
Resize.png	26.0	30.24	6.7622	4.571
Rotate.png	6.49	10.71	64.060	46.91
Equal.png	10.9	15.18	38.279	34.19
Intensit.png	11.9	16.16	34.201	32.85
Gamma.png	11.9	16.18	34.129	33.85
hostr50.jpg	31.8	36.08	3.4527	2.594
Noise.png	17.1	21.40	18.704	2.808

DYNAMIC BINARY LOCATION BASED MULTI-WATERMARK EMBEDDING ALGORITHM IN DWT

TABLE II (B)
MANDRILL WATERMARKED IMAGE USED AS A REFERENCE
IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	24.5	28.71	8.068	6.432
Filter.png	26.7	30.97	6.217	3.683
crop.png	6.13	10.33	66.89	32.60
Resize.png	26.0	30.28	6.735	4.521
Rotate.png	6.50	10.71	64.08	46.92
Equal.png	10.9	15.20	38.22	34.14
Intensit.png	12.0	16.24	33.90	32.56
Gamma.png	11.9	16.11	34.39	34.14
hostr50.jpg	31.9	36.20	3.406	2.547
Noise.png	17.2	21.41	18.69	2.528

TABLE III (A)
BOXER HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE
Wimage.png	49.36	52.98	0.55
Gaussian.png	26.05	29.67	8.07
Filter.png	28.50	32.12	6.09
crop.png	5.47	9.09	86.37
Resize.png	34.27	37.89	3.13
Rotate.png	4.53	8.15	96.25
Equal.png	14.27	17.89	31.35
Intensity.png	12.78	16.40	37.22
Gamma.png	15.80	19.41	26.30
hostr50.png	37.67	41.29	2.11
Noise.png	17.90	21.52	20.63

TABLE III (B)
BOXER WATERMARKED IMAGE USED AS A REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	26.09	29.73	8.05	6.41
Filter.png	28.54	32.18	6.07	1.51
crop.png	5.48	9.12	86.37	39.85
Resize.png	34.43	38.07	3.08	1.41
Rotate.png	4.54	8.18	96.26	65.99
Equal.png	14.23	17.87	31.55	26.85
Intensit.png	12.85	16.49	36.97	33.87
Gamma.png	15.72	19.36	26.56	25.36
hostr50.png	38.01	41.65	2.04	1.38
Noise.png	17.92	21.56	20.63	2.55

TABLE IV (A)
BOAT HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	49.02	54.3	0.487	0.186
Gaussian.png	24.64	29.9	8.071	6.441
Filter.png	23.50	28.8	9.201	5.521
crop.png	6.154	11.49	67.87	32.33
Resize.png	23.57	28.91	9.136	5.668
Rotate.png	5.815	11.15	70.57	50.57
Equal.png	11.58	16.93	36.30	32.52
Intensity.png	12.14	17.48	34.05	32.16
Gamma.png	12.49	17.84	32.69	32.09
hostr50.png	28.11	33.46	5.414	4.045
Noise.png	17.24	22.58	18.93	2.688

TABLE IV (B)
BOAT WATERMARKED IMAGE USED AS A REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	24.67	30.00	8.062	6.429
Filter.png	23.52	28.85	9.197	5.505

crop.png	6.165	11.49	67.87	32.15
Resize.png	23.59	28.92	9.121	5.648
Rotate.png	5.824	11.15	70.59	50.59
Equal.png	11.60	16.93	36.28	32.52
Intensit.png	12.20	17.53	33.86	31.98
Gamma.png	12.46	17.79	32.87	32.27
hostr50.png	28.16	33.49	5.391	4.025
Noise.png	17.25	22.58	18.93	2.505

C. Extraction after Attacks

In our experiment, we also extract the all embedded (LL3, LL4, HL4, LH4, and HH4) sub bands from watermarked image after and before applying ten types of attacks. MATLAB is used for all extraction process and the visual results for original watermarked image, Gaussian, filter, Gamma, and cropping shown in Table-5.

TABLE V
VISUAL RESULTS AFTER ATTACKS

Test Image	First Watermark Logo	Second Watermark Logo
Original Watermarked Image	LL3 	LL4DWT HL4DWT LH4DWT HH4DWT 
Gaussian (mean = 0, variance = 0.001)	LL3 	LL4DWT HL4DWT LH4DWT HH4DWT 
Filter (0.02)	LL3 	LL4DWT HL4DWT LH4DWT HH4DWT 
Gamma(1.5)	LL3 	LL4DWT HL4DWT LH4DWT HH4DWT 
Crop on both sides	LL3 	LL4DWT HL4DWT LH4DWT HH4DWT 

DYNAMIC BINARY LOCATION BASED MULTI-WATERMARK EMBEDDING ALGORITHM IN DWT

V. CONCLUSION

In this paper, we propose a robust multi-watermark embedding algorithm in DWT based on dynamic binary location by selecting a low frequency sub band from fifth level decomposition using two watermark logos to improve the robustness. We tested with the offered schema by applying ten types of attacks. Experimental results with high PSNR value measure the image quality, optimal SNR values estimate the quality of reconstructed image compared to the original one. We demonstrate that our scheme is robust against set of attacks, and also the extracted watermark logo improves to have good visual feature and image quality. Additionally, this can provide copyright protection for legal ownership. Our experimental results show that working with high level decompositions will lead the embedded watermarking logo to be in smaller part of host image. Thus, this will affect the robustness of proposed algorithm schema in face of the other set of attacks. Future work may focus on this area of study and trying to add extra parameter like "Arnold scrambling algorithm" [23] to improve the security and get better results.

ACKNOWLEDGMENT

A. J. Author thanks Iraqi board of supreme audit Iraq/Baghdad (Government Body) which contributed effectively to give me this opportunity for publishing. We would like to extend our sincere appreciation to Dr. Ersin Elbasi for his support in conducting the survey.

REFERENCES

- [1] C. Pfister, "Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud," O'Reilly Media Inc., 2011.
- [2] P. Ramesh, Dr. V. U. Shree, and Dr. K. Padmapriya "Novel Hybrid Inaudible Audio Watermarking with Binary Image as Watermark using DWT," *International Journal Data & Network Security (IJDNS)*, vol.4, pp. 169-173, 2013.
- [3] G. Langelaar, I. Setyan, and R. Lagendijk, "Watermarking Digital Image And Video Data: A State Of Art Overview," *IEEE Transactions on Signal Processing Magazine*, 2000, pp. 19-47.
- [4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," 2nd ed., *Morgan Kaufmann Publishers, Burlington, MA*, 2007.
- [5] A. Bovik, *The Essential Guide to Image Processing*. Academic Press, 2009.
- [6] P. Singh and R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, pp. 164-168, 2013.
- [7] R. Dugad, K. Ratakonda, and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," *Proc. 1998 International Conference on Image Processing*, vol. 2, pp. 419-423, 1998.
- [8] I. J. Cox, J. Kilian, F.T. Leighton, and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1672-1688, 1997.
- [9] E. Elbasi and A. M. Eskicioglu, "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands," *Proc. SPIE 18th Annual Symposium on Electronic Image Security, Steganography and Watermarking of Multimedia Contents VIII*, vol. 6072, pp. 1-10, 2006.
- [10] P. Kumhom and K. Chamnongthai, "Image Watermarking Based on Wavelet Packet Transform With Best Tree," *ECTI Transactions on Electrical Eng., Electronics, and Communications*, vol. 2, 2004.
- [11] J. Ayubi et. al., "A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain," *International Journal of Computer Science Issues*, vol. 8, pp. 191-198, 2011.
- [12] P. Kumar et al., "Digital Image Watermarking Using Wavelet Technique," *World Journal of Science And Technology*, 2012, pp. 6-9.
- [13] V. Parthiban and R. Ganesan, "Hybrid Watermarking Scheme for Digital Images," *Journal of Computer Applications*, 2012, pp. 85-95.
- [14] H. C. Andrews and C. L. Patterson, "Singular Value Decomposition and Digital Image Processing," *IEEE Trans. On Acoustics, Speech and Signal Processing*, no. 1, pp. 25-53, 1976.
- [15] X. Y. Wang and H. Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT," *IEEE Trans. On Signal Processing*, vol. 12, no. 54, pp. 4834-4841, 2006.
- [16] X. Y. Wang, P. P. Niu, and H. Y. Yang, *A Robust Content Based Image Watermarking Using Local Invariant Histogram*. New York: Springer, 2011, pp. 341-363.
- [17] B.Y. Lei, I. Y. Soon and Zhen Li, "Blind and Robust Audio Watermarking Scheme Based on SVD-DCT," *Signal Processing*, vol. 91, pp. 1972-1985, 2011.
- [18] S. G. Hoggar, "Mathematics of Digital Images Creation, Compression, Restoration, Recognition," Cambridge University Press, 2006.
- [19] R. Mehta and N. Rajpal "A Hybrid Semi-Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model," *Contemporary Computing (IC3), IEEE Sixth International Conference*, 2013.
- [20] B. Furht, "Signal Processing for Image Enhancement and Multimedia Processing," *Multimedia Systems And Applications Series Consulting Editor*, 2008.
- [21] Image plugin to assess the quality of images - Written by Daniel Sage at the Biomedical Image Group, EPFL, Switzerland. Available: <http://bigwww.epfl.ch/>
- [22] R. C. Gonzalez and R.E. Woods, "Digital Image Processing," 3rd ed., Prentice Hall, 2008.
- [23] M. Li, T. Liang, and Y. J. He, "Arnold Transform Based Image Scrambling Method", *3rd International Conference on Multimedia Technology (ICMT 2013)*, pp. 1309-1316.

Ammar Jameel. He is a MS student in the Computer Engineering Department at Çankaya University/Ankara/Turkey. His research areas are the manner, methods, applications and issues in a cloud of virtual sensors. He is also working as a network administrator in Iraqi Board of Supreme Audit. He received B.Sc. and PGD in Computer Engineering at University of Technology/Baghdad/Iraq. He is a member of the Federation of Arab engineers.

Seda Yuksel. She received her B.Sc. degree in Computer Engineering from Çankaya University/Ankara/Turkey in 2011. She is a M.Sc. student in the Department of Computer Engineering at Çankaya University. She is also externally working as a software engineer for Unify since 2012. Her research interests are in the following areas: database management systems, information security, and security vulnerabilities in software testing.

Ersin Elbasi. Associate Prof. Dr. Ersin Elbasi is currently working for the Department of Digital Game Design at İPEK University. He received MS degree in Computer Science at Syracuse University; MPhil and PhD degrees in Computer Science at Graduate Center, The City University of New York. His research interests include multimedia security, event mining in video sequences and biomedical data mining and analysis.

