BİLDİRİLER KİTABI

PROCEEDINGS BOOK

***Editors*/Editörler**

Prof. Dr. Şeref Sağıroğlu

Prof. Dr. Mustafa Alkan

Doç. Dr. Sedat Akleylek

ISBN: **978-605-86904-7-9**

10. ULUSLARARASI
BİLGİ GÜVENLİĞİ
ve **KRİPTOLOJİ**
KONFERANSI

10th INTERNATIONAL CONFERENCE
ON INFORMATION
SECURITY &
CRYPTOLOGY

20 - 21 Ekim - October 2017• ANKARA BTK MERKEZ BİNASI • ICTA HEADQUARTER

BİLGİGÜVENLİĞİ
DERNEĞİ

PROCEEDINGS OF
10th INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY (ISCTURKEY 2017)

10. ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
BİLDİRİ KİTABI

ISC TURKEY 2017
BİLDİRİLER KİTABI
PROCEEDINGS

20-21 Ekim / ***October 2017***
ANKARA BTK MERKEZ BİNASI / ANKARA ICTA HEADQUARTER

Ankara, TÜRKİYE / *TURKEY*

***Editors*/Editörler**
Prof. Dr. Şeref Sağıroğlu
Prof. Dr. Mustafa Alkan
Doç. Dr. Sedat Akleylek

www.iscturkey.org
ISBN 978-605-86904-7-9

ABOUT / HAKKINDA

This book compromises the proceedings of ISCTURKEY 2017. The articles in the proceedings reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by ISCTURKEY 2017 Organising Committee.

Bu bildiriler kitabında yer alan bildirin tam metinleri konferans konu başlıklarına uygun olarak yazarlar tarafından hazırlanmıştır. Bildiri özetleri yazarların kendi fikirlerini yansıtır ve herhangi bir değişiklik yapılmadan aynı şekilde basılmıştır. Bu bildiri kitabında yayımlanan görüşler yazarlara ait olup bu görüşlerinden ISCTURKEY 2017 Düzenleme Kurulu sorumlu tutulamaz.

Contact to / İrtibat:

Bilgi Güvenliği Derneği

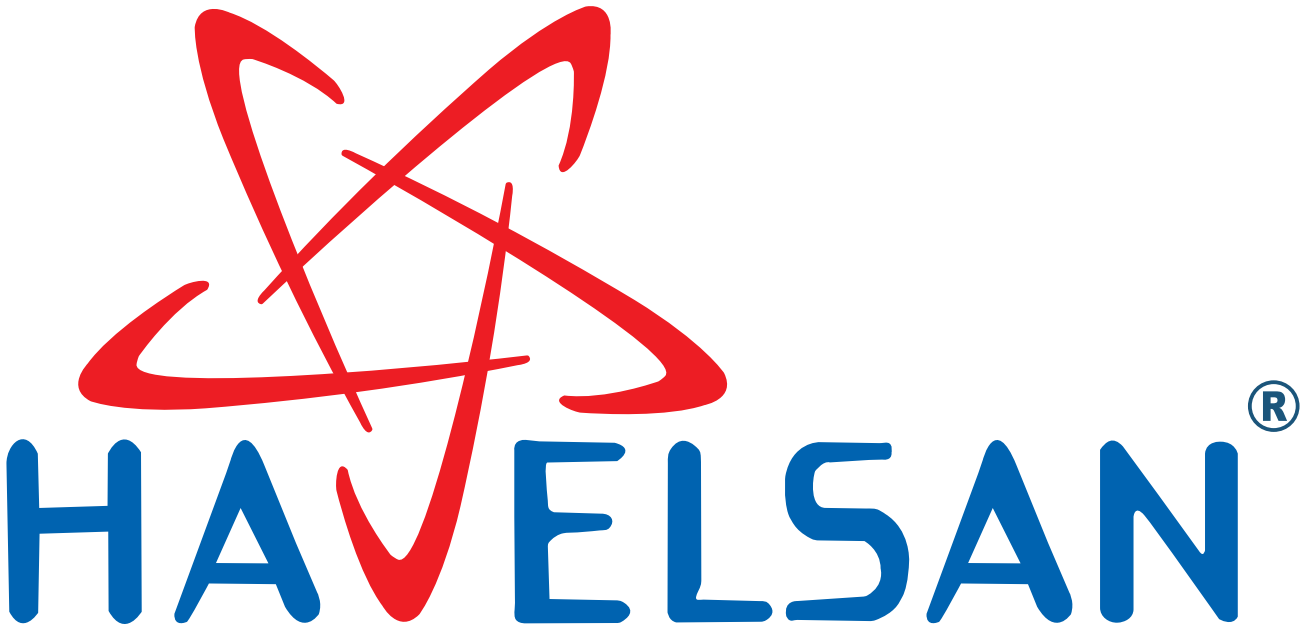
Adres : Maltepe Mahallesi Tuncer Sok. No.4/8 - Çankaya 06570 - Ankara - Türkiye
Tel : +90 312 231 1810
Fax : +90 312 231 1810
Eposta : bilgi@bilgiguvenligi.org.tr

ORGANISERS / ORGANİZASYON

SPONSORS / SPONSORLAR

THANKS TO / TEŞEKKÜR EDERİZ…

MAIN SPONSOR
ANA SPONSOR



SPONSORS / SPONSORLAR

THANKS TO / TEŞEKKÜR EDERİZ…

GOLD SPONSOR
ALTIN SPONSOR

NETAS

SILVER SPONSORS
GÜMÜŞ SPONSORLAR

STM

EMFA

Türk Telekom

TechData

vodafone

TÜRKSAT

aselsan

FORCEPOINT
POWERED BY Raytheon

TURKCELL

SPONSORS / SPONSORLAR

THANKS TO / TEŞEKKÜR EDERİZ…

COFFEE BREAK SPONSORS
KAHVE ARASI SPONSORLARI

ICTERRA

INNOVA

PANEL SPONSORS
PANEL SPONSORLARI

INTELLFOR GLOBAL STRATEGY

atarlabs

SIEMENS Ingenuity for life

BİZNET BİLİŞİM

STANDS SPONSORS
STAND SPONSORLARI

beam://

Verify

360 TEKNOLOJİ

Arge360

Labris NETWORKS

bvk

Bitdefender

net iletişim

atarlabs

BİZNET BİLİŞİM

ATTACK FLOW

bqtek

COSLAT Security Systems

MAY CYBER TECHNOLOGY

EMT ELECTRONICS

BARIKAT

BACKDROP SPONSOR
SAHNE SPONSORU

ayesaş

HUAWEI

NAME BADGE SPONSOR
YAKA KARTI SPONSORU

TURKTRUST

SPONSORS / SPONSORLAR

THANKS TO / TEŞEKKÜR EDERİZ…

MEDIA SPONSORS
MEDYA SPONSORLARI

CyberMag
TÜRKİYE'NİN İLK VE TEK SİBER GÜVENLİK DERGİSİ

faselis

EVENT MANAGEMENT SPONSOR
ETKİNLİK YÖNETİMİ SPONSORU

sencron

DİJİTAL İLİŞKİLER SPONSORU
DIGITAL RELATIONS SPONSOR

DİJİTALMEDYA
Yeni nesil dijital liderlik ajansı

COMMITTEES / KURULLAR

Onur Kurulu / *Honory Committee*

Dr. Ömer Fatih **SAYAN**, *BTK Başkanı*

Prof. Dr. Mehmet **KARACA**, *ITÜ Rektörü*

Prof. Dr. İbrahim **USLAN**, *Gazi Üniversitesi Rektörü*

Prof. Dr. Mustafa Versan **KÖK**, *ODTÜ Rektörü*

Düzenleme Kurulu / *Organising Committee*

Mustafa **ALKAN**, Eş Başkan/ CoChair, *Gazi Üniversitesi /Gazi University*

Ersan **AKYILDIZ**, Eş Başkan/ CoChair, *Orta Doğu Teknik Üniversitesi/Middle East Technical University*

Ertuğrul **KARAÇUHA**, Eş Başkanı/CoChair, *İstanbul Teknik Üniversitesi/İstanbul Technical University*

Şeref **SAĞIROĞLU**, Eş Başkan/CoChair, *Bilgi Güvenliği Derneği /Information Security Association of Turkey*

Ali **YAZICI**, *Bilgi Güvenliği Derneği/Information Security Association*

Abdullah Raşit **GÜLHAN**, *Bilgi Güvenliği Derneği/Information Security Association*

Burhanettin **AL**, *Bilgi Güvenliği Derneği/Information Security Association*

Mehmet **GÜLŞEN**, *Bilgi Güvenliği Derneği/Information Security Association*

Mehmet Ali **İNCEEFE**, *Bilgi Güvenliği Derneği/Information Security Association*

Mustafa **ÜNVER**, *Bilgi Güvenliği Derneği/Information Security Association*

Bilgehan **ARSLAN**, *Gazi Üniversitesi/Gazi University*

Duygu **SİNANÇ**, *Gazi Üniversitesi/Gazi University*

Enver **ÖZDEMIR**, *İstanbul Teknik Üniversitesi/İstanbul Technical University*

Fatih **DEMİRHAN**, *Orta Doğu Teknik Üniversitesi/Middle East Technical University*

Lütfiye **ATA DURAK**, *İstanbul Teknik Üniversitesi/İstanbul Technical University*

Merve Sedef **GÜNDÜZ**, *Gazi Üniversitesi/Gazi University*

Murat **CENK**, *Orta Doğu Teknik Üniversitesi/Middle East Technical University*

Oğuzhan **KÜLEKÇİ**, *İstanbul Teknik Üniversitesi / İstanbul Technical University*

Ramazan **TERZİ**, *Gazi Üniversitesi/Gazi University*

Sebahattin **EKER**, *İstanbul Teknik Üniversitesi / İstanbul Technical University*

Sedat **AKLEYLEK**, *Ondokuz Mayıs Üniversitesi/Ondokuz Mayis University*

Yavuz **CANBAY**, *Gazi Üniversitesi/Gazi University*

Bilim Kurulu / *Program Committee*

A. Naci **ÜNAL**, *Bahçeşehir Üniversitesi, Bahçeşehir University*

A. Nurdan **SARAN**, *Çankaya Üniversitesi/Çankaya University*

Ahmet **KOLTUKSUZ**, *Yaşar Üniversitesi/Yaşar University*

Ahmet **ÖZMEN**, *Sakarya Üniversitesi/Sakarya University*

Akın **MARSAP**, *Aydın Üniversitesi/Aydın University*

Albert **LEVI**, *Sabancı Üniversitesi/Sabancı University*

Ali Aydın **SELÇUK**, *TOBB ETÜ/TOBB University of Economics and Technology*

Ali **DOĞANAKSOY**, *Orta Doğu Teknik Üniversitesi/METU*

Ali **İNAN**, *Adana Bilim ve Teknoloji Üniversitesi*

Ali **ŞENTÜRK**, *Mersin Üniversitesi/Mersin University*

Ali **YAZICI**, *Atılım Üniversitesi/Atılım University*

Ali Ziya **ALKAR**, *Hacettepe Üniversitesi/Hacettepe University*

Alisher **KHOLMATOV**, *Sabancı Üniversitesi/Sabancı University*

Alok **TONGAONKAR**, *Symantec*

Alper **ÖZBİLEN**, *Bilgi Güvenliği Derneği/Information Security Association of Turkey*

Alper **UĞUR**, *Pamukkale Üniversitesi/Pamukkale University*

Alptekin **KÜPCÜ**, *Koç Üniversitesi/Koc University*

Ammar **DAŞKIN**, *İstanbul Medeniyet Üniversitesi/ İstanbul Medeniyet University*

Asaf **VAROL**, *Fırat Üniversitesi, Fırat University*

Atila **BOSTAN**, *Atılım Üniversitesi/Atılım University*

Atilla **ELÇİ**, *Aksaray Üniversitesi/Aksaray University*

Atilla **ÖZGİT**, *Orta Doğu Teknik Üniversitesi/METU*

Aydın **ALATAN**, *Orta Doğu Teknik Üniversitesi/METU*

Ayşe **BAŞAR BENER**, *Boğaziçi Üniversitesi/Boğaziçi University*

Barış Bülent **KIRLAR**, *Süleyman Demirel Üniversitesi/Süleyman Demirel University*

Bedri **ÖZER**, *Fırat Üniversitesi/Fırat University*

Berkant **USTAOĞLU**, *İzmir Teknoloji Enstitüsü/İzmir Institute of Technology*

Berna **ORS YALÇIN**, *İstanbul Teknik Üniversitesi/İstanbul Technical University*

Berrin **YANIKOĞLU**, *Sabancı Üniversitesi/Sabancı University*

Berry **SCHOENMAKERS**, *Eindhoven University of Technology*

Bimal **ROY**, *Indian Statistical Institute*

Bülent **ÖRENCİK**, *İstanbul Teknik Üniversitesi /İstanbul Technical University*

Bülent **TUĞRUL**, *Ankara Üniversitesi/Ankara University*

Cebrail **ÇİFTLİKLİ**, *Erciyes Üniversitesi/Erciyes University*

Cevat **SENER**, *Orta Doğu Teknik Üniversitesi/METU*

Cihangir **TEZCAN**, *Ortadoğu Teknik Üniversitesi/METU*

Cüneyt **BAZLAMAÇCI**, *Orta Doğu Teknik Üniversitesi/METU*

Çağdaş **ÇALIK**, *National Institute of Standards*

Debasis **GIRI**, *Haldia Institute of Technology*

Deniz **TAŞKIN**, *Trakya Üniversitesi/Trakya University*

Derviş **KARABOĞA**, *Erciyes Üniversitesi/Erciyes University*

Ecir Uğur **KÜÇÜKSİLLE**, *Süleyman Demirel Üniversitesi/Süleyman Demirel University*

Eiji **OKAMOTO**, *University of Tsukuba*

Elif **SAYGI**, *Hacettepe Üniversitesi/Hacettepe University*

Emin **ANARIM**, *Boğaziçi Üniversitesi/Boğaziçi University*

Emin İslam **TATLI**, *İstanbul Medipol Üniversitesi/İstanbul Medipol University*

Emir **DİRİK**, *Uludağ Üniversitesi/Uludağ University*

Emrah **ÇAKÇAK**, *Orta Doğu Teknik Üniversitesi/METU*

Engin **AVCI**, *Fırat Üniversitesi/Fırat University*

Engin **KIRDA**, *ISECLAB*

Enis **KARAARSLAN**, *Muğla Üniversitesi/Muğla University*

Ercan **BULUŞ**, *Namık Kemal Üniversitesi/Namık Kemal University*

Erdal **IRMAK**, *Gazi Üniversitesi/Gazi University*

Erdem **ALKIM**, *Ege Üniversitesi/Ege University*

Erdoğan **DOĞDU**, *TOBB Ekonomi ve Teknoloji Üniversitesi/TOBB University of Economics and Technology*

Erkan **AFACAN**, *Gazi Üniversites/Gazi University*

Erkan **BEŞDOK**, *Erciyes Üniversitesi/Erciyes University*

Erkay **SAVAŞ**, *Sabancı Üniversitesi/Sabancı University*

Ersan **AKYILDIZ**, *Orta Doğu Teknik Üniversitesi/METU*

Ersin **ELBAŞI**, *TÜBİTAK/The Scientific and Technological Reseach Council of Turkey*

Esra **YOLAÇAN**, *Osmangazi Üniversitesi/Osmangazi University*

Eşref **ADALI**, *İstanbul Teknik Üniversitesi/ITU*

Ertan **ONUR**, *Orta Doğu Teknik Üniversitesi/METU*

Eyüp Burak **CEYHAN**, *Bartın Üniversitesi/Bartın University*

Faruk **GÖLOĞLU**, *ESAT-COSIC*

Fatih **SULAK**, *TÜBİTAK/The Scientific and Technological Reseach Council of Turkey*

Fatma **BÜYÜKSARAÇOĞLU SAKALLI**, *Trakya Üniversitesi/Trakya University*

Fatoş **YARMAN VURAL**, *Orta Doğu Teknik Üniversitesi/METU*

Ferruh **ÖZBUDAK**, *Orta Doğu Teknik Üniversitesi/METU*

Gökay **SALDAMLI**, *Boğaziçi Üniversitesi/Boğaziçi University*

Gökhan **DALKILIÇ**, *Dokuz Eylül Üniversitesi/Dokuz Eylül University*

Guangzhi **QU**, *Oakland University*

Hacer K**ARACAN**, *Gazi Üniversitesi/Gazi University*

Hakan **TEKEDERE**, *Gazi Üniversitesi/Gazi University*

Halil İbrahim **BÜLBÜL**, *Gazi Üniversitesi/Gazi University*

Hamdi Murat **YILDIRIM**, *Bilkent Üniversitesi/Bilkent University*

Harold **BAIER**, *TU DARMSTADT*

Hayri **SEVER**, *Hacettepe Üniversitesi/Hacettepe University*

Hidayet **TAKÇI**, *Cumhuriyet Üniversitesi/Cumhuriyet University*
Hüseyin **DEMİRCİ**, *TÜBİTAK/The Scientific and Technological Reseach Council of Turkey*
Hüseyin **HIŞIL**, *Yaşar Üniversitesi/Yaşar University*
Hüsrev Taha **SENCAR**, *TOBB ETÜ/TOBB University of Economics and Technology*
Ion **TUTANESCU**, *University of Pitesti*
İbrahim Alper **DOĞRU**, *Gazi Üniversitesi/Gazi University*
İbrahim **SOĞUKPINAR**, *Gebze Yüksek Teknoloji Enstitüsü/Gebze Institute of Technology*
İlhami **ÇOLAK**, *Nişantaşı Üniversitesi/Nisantasi University*
İlkay **ULUSOY**, *Orta Doğu Teknik Üniversitesi/METU*
İsmail **GÜLOĞLU**, *Doğuş Üniversitesi/Doğuş University*
İsmail **SAN**, *Anadolu Üniversitesi/Anadolu University*
İzzet Gökhan **ÖZBİLGİN**, *HAVELSAN Akademi Direktörü - Gazi Üniversitesi*
Jianying **ZHOU**, *ASTAR Institute for Infocomm Research*
John A. **CLARK**, *University of York*
Jongsub **MOON**, *Korea University*
Jorge **NAKAHARA**, *Universite' Libre de Bruxelles (ULB), Belgium*
Kasım **ÖZTOPRAK**, *KTO Karatay Üniversitesi/Karatay University*
Katerina **MITROKOTSA**, *Delft University of Technology*
Kemal **BIÇAKCI**, *TOBB Ekonomi ve Teknoloji Üniversitesi/TOBB University of Economics and Technology*
Kerem **KAŞKALOĞLU**, *Özyeğin Üniversitesi/Özyeğin University*
Kıvanç **DİNÇER**, *Hacettepe Üniversitesi/Hacettepe University*
Kıvanç **MIHÇAK**, *Boğaziçi Üniversitesi/Boğaziçi University*
Koray **KARABINA**, *Florida Atlantic University*
Leyla **BERBER**, *Bilgi Üniversitesi/Bilgi University*
Mehmet **AKTAŞ**, *TÜBİTAK Bilgem, BTE/The Scientific and Technological Reseach Council of Turkey*
Mehmet **DEMİRCİ**, *Gazi Üniversitesi/Gazi University*
Mehmet **KİRAZ**, *TÜBİTAK-UEKAE/The Scientific and Technological Reseach Council of Turkey*
Mehmet **TEKEREK**, *KSU Üniversitesi/KSU University*
Mehmet Emin **DALKILIÇ**, *Ege Üniversitesi/Ege University*
Mehmet Ufuk **ÇAĞLAYAN**, *Boğaziçi Üniversitesi/Boğaziçi University*
Melek D. **YÜCEL**, *Orta Doğu Teknik Üniversitesi/METU*
Melissa **DANFORD**, *California State University*
Meltem **SÖNMEZ TURAN**, *National Institute of Standards and Technology (NIST)*
Mert **ÖZARAR**, *Konya Gıda ve Tarım Üniversitesi*
Mine **AKKAN**, *9 Eylül Üniversitesi/9 Eylül University*
Muhammet Ali **AYDIN**, *İstanbul Üniversitesi/İstanbul University*
Muhammet **ÜNAL**, *Gazi Üniversitesi/Gazi University*

Muhiddin **UĞUZ**, *Ortadoğu Teknik Üniversitesi/METU*

Murat **AK**, *Akdeniz Üniversitesi/Akdeniz University*

Murat **AŞKAR**, *İzmir Ekonomi Üniversitesi/İzmir University of Economics*

Murat **AYDOS**, *Hacettepe Üniversitesi/Hacettepe University*

Murat **CENK**, *Orta Doğu Teknik Üniversitesi/METU*

Murat **KARAKAYA**, *Atılım Üniversitesi/ Atılım University*

Mustafa **ALKAN**, *Gazi Üniversitesi/Gazi University*

Nazife **BAYKAL**, *Orta Doğu Teknik Üniversitesi/METU*

Oğuz **YAYLA**, *Hacettepe Üniversitesi/Hacettepe University*

Orhun **KARA**, *TÜBİTAK-UEKAE/The Scientific and Technological Reseach Council of Turkey*

Osmanbey **UZUNKOL**, *TÜBİTAK/The Scientific and Technological Reseach Council of Turkey*

Ömer Faruk **BAY**, *Gazi Üniversitesi/Gazi University*

Özgür **AKAN**, *Orta Doğu Teknik Üniversitesi/METU*

Peter **COOPER**, *Sam Houston State University*

Qinghan **XIAO**, *Defence Research and Development Canada*

Resul **DAŞ**, *Fırat Üniversitesi/Fırat University*

Sedat **AKLEYLEK**, *Ondokuz Mayıs Üniversitesi/Ondokuz Mayis University*

Selçuk **BAKTIR**, *Bahçeşehir Üniversitesi/Bahçeşehir University*

Selçuk **KAVUT**, *Balıkesir Üniversitesi/Balıkesir University*

Selim **KINACI**, *SSMDB, EGM/Turkish National Police*

Serap **ŞAHİN**, *İYTE/Izmir Institute of Technology*

Serdar **BOZTAŞ**, *RMIT Üniversitesi/RMIT University*

Serdar Süer **ERDEM**, *GYTE/Gebze Institute of Technology*

Sevil **ŞEN**, *Hacettepe Üniversitesi/Hacettepe University*

Shahram **RAHIMI**, *Southern Illinois University*

Suat **ÖZDEMİR**, *Gazi Üniversitesi/Gazi University*

Subhamoy **MAITRA**, *Indian Statistical Institute*

Süleyman **ÖZARSLAN**, *Orta Doğu Teknik Üniversitesi/METU*

Şaban **EREN**, *Maltepe Üniversitesi/Maltepe University*

Şeref **SAĞIROĞLU**, *Gazi Üniversitesi/Gazi University*

Taner **ALTUNOK**, *Türk Hava Kurumu Üniversitesi / Turkish Aviation Association University*

Tarık **YERLİKAYA**, *Trakya Üniversitesi/Trakya University*

Tekin **MEMİŞ**, *Kadir Has Üniversitesi/Kadir Has University*

Tolga **MATARACIOĞLU**, *Tübitak Bilgem Siber Güvenlik Enstitüsü*

Tolga **SAKALLI**, *Trakya Üniversitesi/Trakya University*

Tolga **YALÇIN**, *Konya Gıda ve Tarım Üniversitesi*

Tuğba **TAŞKAYA TEMİZEL**, *Ortadoğu Teknik Üniversitesi/METU*

Tuğkan **TUĞLULAR**, *İzmir Yüksek Teknoloji Enstitüsü/Izmir Institute of Technology*

Tuğrul **YANIK**, *Celal Bayar Üniversitesi/Celal Bayar University*

Türksel Kaya **BENSGHİR**, *TODAİE*

Umut **ULUDAĞ**, *TÜBİTAK UEKAE/The Scientific and Technological Reseach Council of Turkey*

Vasif **NABİYEV**, *Karadeniz Teknik Üniversitesi/Karadeniz Technical University*

Veysel **ASLANTAŞ**, *Erciyes Üniversitesi/Erciyes University*

Volkan **ATALAY**, *Orta Doğu Teknik Üniversitesi/METU*

Yadigar **IMAMVERDIYEV**, *Institute of Information Technology, Azerbaijan National Academy of Sciences*

Yurdahan **GÜLER**, *Ortadoğu Teknik Üniversitesi/METU*

Yusuf **İPEKOĞLU**, *Orta Doğu Teknik Üniversitesi/METU*

Yusuf Murat **ERTEN**, *İzmir Yüksek Teknoloji Enstitüsü/Izmir Institute of Technology*

Yücel **SAYGIN**, *Sabancı Üniversitesi/Sabancı University*

Ziya **AKTAŞ**, *Çankaya Üniversitesi/Çankaya University*

Zülfükar **SAYGI**, *TOBB ETÜ/TOBB University of Economics and Technology*

Danışma Kurulu / *Advisory Board*

A. Neşe **SAYARI**, *Biznet*

Abdullah Raşit **GÜLHAN**, *SİNERJİTÜRK*

Ahmet Hamdi **ATALAY**, *NETAŞ*

Ali **YAZICI**, *ASELSAN*

Batuhan **TOSUN**, *ISSA Türkiye*

Bilal **ÖNAL**, *BGD*

Burak **ÇİFTER**, *BOA TEKNOLOJİ*

Burhanettin **AL**, *Turkcell*

Cem **AKOYMAK**, *Avea*

Cemal **AKYEL**, *Akyel Online*

Doğan Ufuk **GÜNEŞ**, *YASAD*

Emine Yazıcı **ALTINTAŞ**, *UDHB*

Faruk **ECZACIBAŞI**, *TBV*

Ferhat **YEŞİLLİ**, *BİH Grup*

Füsun Sarp **NEBİL**, *TİD*

Gökhan **ÖZBİLGİN**, *Havelsan*

Gürcan **GÜRSÜ**, *ALBERK QA TECHNIC*

Hanzade **SARIÇİÇEK**, *ODTÜ Teknokent*

Huzeyfe **ÖNAL**, *BGA*

İlker **TABAK**, *TBD*

Kadriye Yıldız **BARLAS**, *BGD*

Kemal **CILIZ**, *TÜBİSAD*

Mehmet Ali **İNCEEFE**, *BGD*

Mesut **DEMİRBİLEK**, *Vodafone*

Metin **TARAKÇI**, *ÇMD*

Muhterem **İLHAN**, *Vodafone*

Mustafa **AKGÜL**, *İNETD*

Mustafa **MACAR**, *BGD*

Mustafa **YANARTAŞ**, *TÜBİFED*

Nahit **GÖK**, *SABİDER*

Orhan **TURAN**, *BGD*

Selim **ÜLKÜ**, *BGD*

Tolga **TÜFEKÇİ**, *TürkTrust*

TOPICS / KONULAR

Siber Güvenlik

- Kurumsal Sistem Güvenliği
- Dağıtık ve Yaygın Sistem Güvenliği
- Donanım Tabanlı Güvenlik
- Olay İşleme ve Penetrasyon Testi
- Yasal Sorunlar
- Multimedya ve Belge Güvenliği
- İşletim Sistemleri ve Veritabanı Güvenliği
- Gizlilik sorunları
- SCADA ve Gömülü Sistem Güvenliği
- Güvenli Yazılım Geliştirme
- Bulut Bilişim Güvenliği
- Büyük Veri Güvenliği
- Sosyal Ağlarda Güvenlik
- Web Tabanlı Uygulamalar ve Hizmetlerin Güvenliği
- Güvenlik Protokolleri
- VOIP, Kablosuz ve Telekomünikasyon Ağ Güvenliği

Dijital Adli Bilişim

- Siber Suçlar
- Karşı-Adli Bilişim ve Karşı-Karşı Adli Bilişim Teknikleri
- Veri sızıntısı ve Veri Koruma
- Veritabanında Adli Bilişim
- İçerik Filtreleme
- Dosya Sistemi ve Bellek Analizi
- Sanal ve Bulut Ortamlarında Adli Tıp
- Bilgi Gizleme
- Multimedia Adli Bilişimi
- İçeriden Saldırıların İncelenmesi
- Büyük Ölçekli Araştırmalar
- Malware Adli Bilişimi ve Anti-Malware Teknikleri
- Ağ Adli Bilişimi ve Trafik Analizi
- Donanım Hassasiyeti ve Cihazların Adli Bilişimi
- Yeni Tehditler ve Geleneksel Olmayan Yaklaşımlar

Bilgi Güvencesi ve Güvenlik Yönetimi

- İş Sürekliliği ve Felaket Kurtarma Planlaması
- Kurumsal Yönetim
- Kritik Altyapı Koruma
- Dijital Haklar Yönetimi ve Fikri Mülkiyet Koruması
- Güvenlik Ekonomisi
- Dolandırıcılık Yönetimi
- Kimlik Yönetimi
- Kanun ve Yönetmelikler
- Güvenlik Politikaları ve Güven Yönetimi
- Tehditler, Güvenlik Açıkları ve Risk Yönetimi

Siber Savaş ve Fiziki Güvenlik

- Gözetleme Sistemleri
- Biyometri Uygulamaları
- Siber Savaş Eğilimleri ve Yaklaşımlar
- Elektronik Pasaportlar, Ulusal Kimlik ve Akıllı Kart Güvenliği
- Sosyal Mühendislik
- Kimlik ve Erişim Kontrol Sistemleri
- Biyometri Standartları
- Yeni Teori ve Algoritmalar

IoT Destekli Teknolojiler

- 5G Ağlar ve IoT
- Yazılım Tanımlı Ağ (SDN) ve IoT
- Sensör ve Aktüatör Ağları
- Ultra-düşük güç IoT Teknolojileri ve Gömülü Sistem Mimarileri
- Giyilebilir Cihazlar, Vücut Algılayıcı Ağlar, Akıllı Taşınabilir Aygıtlar
- IoT Cihazlar ve Sistemleri için Tasarım Uzayı Keşif Teknikleri
- Heterojen Ağlar
- IoT Protokolleri (IPv6, 6LoWPAN, RPL, 6TiSCH, W3C)
- Iot için Adlı Veri Ağı (NDN)
- Nano Şeylerin Interneti
- Sensör Veri Yönetimi, IoT Madenciliği ve Analitiği
- Adaptif Sistemler
- Dağıtık Depolama
- Veri Füzyonu

- Yönlendirme ve Kontrol Protokolleri
- Kaynak Yönetimi, Erişim Kontrolü
- Kimlik Yönetimi ve Nesne Tanıma
- Yerini Belirleme Teknolojileri
- Uç Nokta Bilişimi, Sis Bilişimi ve IoT
- Makineler Arası Haberleşme (M2M) ve IoT
- Endüstriyel IoT

IoT Uygulama ve Hizmetleri

- Siber-fiziksel sistemler
- İşbirlikçi Uygulamalar ve Sistemler
- Servis Deneyimleri ve Analizi
- Akıllı Şehirler, Akıllı Kamu Yerleri, Akıllı Ev/Bina
- e-Sağlık, Yaşam Desteği,
- Akıllı Ulaşım
- Akıllı Şebekeler, Enerji Yönetimi
- Tüketici Elektroniği
- Kırsal Hizmetler ve Üretim
- Endüstriyel IoT Servis Oluşturma ve Yönetimi
- Kitle Kaynaklı Algılama, İnsan Merkezli Algılama
- Büyük Veri ve IoT Veri Analitiği
- Semantik Teknolojiler
- Mobil Bulut Bilişim ve IoT
- IoT için Yatay Uygulama Geliştirme
- IoT Uygulama Geliştirme için Tasarım Prensipleri ve En İyi Uygulamalar

IoT Toplumsal Etkileri

- IoT'da İnsan Rolü, Sosyal Hizmetler
- Değer Zinciri Analizi
- IoT için Yeni İnsan-Aygıt Etkileşimleri
- Sosyal Modeller ve Ağlar
- Yeşil IOT: Sürdürülebilir Tasarım ve Teknoloji
- Kent Dinamikleri ve Kitle Kaynaklı Hizmetler
- IoT Sürdürülebilirliği ve ROI için Ölçümler ve Değerlendirmeler

IoT için Güvenlik ve Gizlilik

- IoT Gizlilik ve Güvenlik Endişeleri
- Kimlik Saptama ve Kimlik Doğrulama Sorunları
- IoT Güvenliği için Kablosuz Sensör Ağı
- IoT'da Saldırı Tespiti
- IoT için kriptografi, anahtar yönetimi ve yetkilendirme
- IoT'da Fiziksel / MAC / Ağ Saldırıları
- IoT'da Çapraz Katmanlı Saldırılar
- IoT'da QoS Optimizasyonu ile Güvenlik
- IoT'da Gizlilik Tabanlı Kanal Erişimi
- IoT Adli Bilişimi
- IoT'da Büyük Veri ve Bilgi Bütünlüğü
- IoT'da Haberleşme Güvenliği
- IoT'da Güvenlik Standartları

IoT Deneysel Sonuçlar ve Dağıtım Senaryoları

- Araştırma ve Uygulama Arasındaki Boşluğu Kapama
- Deneysel Prototipler ve Sınama Ortamları
- Çok amaçlı IOT Sistem Modelleme ve Analiz
- IOT Ara Bağlantı Analizi
- Gerçek Vaka Dağıtım Senaryoları ve Sonuçları
- Standardizasyon ve Düzenleme

PREFACE /ÖNSÖZ

Bilgi güvenliği ve siber güvenlik alanında, ulusal ve uluslararası boyutta bilimsel, teknik, sosyal ve kültürel çalışmalar yürüterek kişisel, kurumsal ve ulusal farkındalığın oluşması ve ortak akıl ile çözüm önerilerinin geliştirilmesi amacı ile 2007 yılında kurulan Bilgi Güvenliği Derneği (BGD) her yıl Uluslararası Bilgi Güvenliği ve Kriptoloji (ISCTURKEY) Konferansı düzenlemektedir. Bu konferansın onuncusu, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliğiyle ve T.C. Başbakanlık, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu'nun destekleriyle 20-21 Ekim 2017 tarihlerinde BTK Kongre Merkezinde gerçekleştirilmiştir.

Uluslararası ISCTURKEY Konferansı, düzenlendiği ilk yıldan beri Türkiye'nin bilgi güvenliği alanındaki bilimsel ve sektörel çalışmalarının paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamuoyunun bilgilendirildiği, eğitildiği, ulusal ve uluslararası tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizin bu alandaki en önemli etkinliğidir. Bu etkinlik ile bilgi güvenliği alanında, toplumun her kesiminin farkındalığının arttırılması, bilimsel bilgi birikimine katkı sağlanması, kurumlar ve sektörler arasında işbirliği imkânlarının oluşturulması ve en önemlisi bunu uluslararası boyutta yaparak uluslararası işbirliğinin arttırılması hedeflenmiştir.

ISCTURKEY 2017 Konferansı Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından da desteklenmiş ve Avrupa Birliği'nin her yılın Ekim ayı olarak belirlediği "Avrupa Siber Güvenlik Ayı"etkinlikleri kapsamına alınmıştır.

ISCTURKEY 2017 Konferansının bu yılki ana teması "Siber Güvenlik ve Yapay Zeka" olarak belirlenmiştir. Milli güvenliğin önemli bir parçası olan siber güvenlik konusunda zafiyet gösterilmemesi için hem nitelikli siber güvenlik uzmanları yetiştirilmesi hem de gerek donanım gerek yazılım alanında milli ve yerli çözümler üretilmesinin şart olduğu düşüncesinden hareketle ISCTURKEY 2017 Konferans programı oluşturulmuştur.

ISCTURKEY 2017 Konferansına, bu yıl 1500'ün üzerinde kişi elektronik kayıt yaptırmıştır. Konferans programında; 3 panel, 2 Kurul Toplantısı, 9 akademik oturum, 1 davetli konuşmacı, 4 eğitim, 3 firma ve ürün tanıtım oturumu gerçekleştirilmiştir.

Konferans açılış konuşmalarını; Bilgi Güvenliği Derneği Başkanı SN. Ahmet Hamdi ATALAY, ODTÜ Rektörü Sn. Prof. Dr. Mustafa Verşan KÖK, Gazi Üniversitesi Rektörü Sn. Prof. Dr. İbrahim USLAN, BTK Başkanı Sn. Dr. Fatih SAYAN, UDHB Bakanı Sn. Ahmet ARSLAN, Başbakanımız Sn. Binali YILDIRIM yapmışlardır.

Konferansa sunulmak üzere gönderilen bildiriler, Konferans Bilim Kurulu tarafından incelenmiş ve sunulması önerilen bildiriler, akademik oturumlarda sunulmuş ve bu kitapçıkta basılmıştır.

Bu yıl onuncusunu yaptığımız bu uluslararası konferansın başta ülkemiz ve kurumlarımız olmak üzere tüm katımcılarına faydalı olmasını dileriz.

Saygılarımızla.

Prof. Dr. Şeref **SAĞIROĞLU**, *Konferans Eş-Başkanı*

Prof. Dr. Mustafa **ALKAN**, *Konferans Eş-Başkanı*

Prof. Dr. Ersan **AKYILDIZ**, *Konferans Eş-Başkanı*

Prof. Dr. Ertuğtul **KARAÇUHA**, *Konferans Eş-Başkanı*

20 EKİM 2017, CUMA - *20 OCTOBER 2017, FRIDAY*

08:30 - 09:00	**KAYIT**
09:30 - 11:00	**AÇILIŞ KONUŞMALARI / ANA SALON** • Ahmet Hamdi ATALAY, *Bilgi Güvenliği Derneği YK Başkanı* • Dr. Ömer Fatih SAYAN, *Bilgi Teknolojileri ve İletişim Kurumu Başkanı* • Dr. Faruk ÖZLÜ, *T.C. Bilim Sanayi ve Teknoloji Bakanı* • Ahmet ARSLAN, *T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanı* • Binali YILDIRIM, *T.C. Başbakanı*
11:00 -11:30	**İLETİŞİM ARASI / *BREAK TIME***
11:30-12:30	**Davetli Konuşmacı, Prof. Dr. Erdal Çayırcı, University of Stavanger**
12:30-14:00	**ÖĞLE YEMEĞİ ARASI / *LUNCH BREAK***
14:00 – 15:30	**PANEL - 1 / Ana Salon** *"Kamuda Endüstri 4.0 ve Siber Güvenlik Yaklaşımı"* ***Panel Yöneticisi:*** • Prof. Dr. Ertuğrul Karaçuha, *Konferans Eş Başkanı* ***Panelistler:*** • Doç. Dr. İzzet Gökhan Özbilgin, *HAVELSAN Akademi ve Teknoloji Direktörü* • Eser Ateş, *Biznet Bilişim İş Geliştirme Direktörü* • Dr. Sinan Şenol, *ASELSAN Sistem Mühendisi* • Burak Dayıoğlu, *Atar Labs CEO* • Emre Evren, *EMFA Yazılım Yönetim Kurulu Başkanı*
14:00 – 15:30	**Salon / Hall A - Siber Güvenlik Eğitimi** **Training on Cyber Security** *9-10-11 Sınıflar İçin Eğitim Programı* ***Oturum Başkanları - Session Chairs:*** • Prof. Dr. Şeref Sağıroğlu, *Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı* • Dr. Şahin Bayzan, *BTK Bilişim Uzmanı* ***Oturum Konuları - Session Topics:*** • SİBER ORTAMDA TEHDİTLER • SİBER ORTAMLARIN BİLİNÇLİ VE GÜVENLİK KULLANIMI
14:00 – 15:30	**Salon / Hall B - Siber Güvenlik Eğitimi** **Training on Cyber Security** *5-6-7-8 Sınıflar İçin Eğitim Programı* ***Oturum Başkanları - Session Chairs:*** • Dr. Mustafa Küçükali, *BTK İnternet Dairesi Başkanı* • Ahmet Çubukçu, *BTK Bilişim Uzmanı* ***Oturum Konuları - Session Topics*** • İNTERNETTE TEHDİTLER • İNTERNETİN BİLİNÇLİ VE GÜVENLİ KULLANIMI
15:30 – 16:00	**İLETİŞİM ARASI / *BREAK TIME***

20 EKİM 2017, CUMA – *20 OCTOBER 2017, FRIDAY*

16:00 - 17:30	**PANEL - 2 / ANA SALON**
	"Büyük Veri Analizi ve Veri Merkezleri Güvenliği, Analysis of Big Data, Cyber Security of Data Center"
	Panel Yöneticisi: • Rıdvan Kahveci, *BTK Başkan Yardımcısı*
	Panelistler: • Ahmet Fethi Ayhan, *TÜRK TELEKOM Siber Güvenlik Direktörü* • Utku Sert, *TURKCELL Altyapı Operasyonları Direktörü* • Dr. Hasan Süel, *VODAFONE TÜRKİYE İcra Kurulu Başkan Yardımcısı* • Mustafa Avcı, *Intellfor Global Strategy Başkanı* • Mehmet Ali Ortayatırtmacı, *TÜRKSAT Siber Güvenlik Yönetim Direktörü* • Uğur Çağal, *NETAŞ Siber Güvenlik Teknoloji Geliştirme Direktörü*
17:30 – 18:00	**İLETİŞİM ARASI / *BREAK TIME***
18:00 - 19:00	**YUVARLAK MASA TOPLANTISI /1** **BGD BİLİM KURULU Salon A**
	Oturum Başkanı - Session Chair: • Prof. Dr. Şeref Sağıroğlu, *Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı*
	Oturum Konuları - Session Topics: • BGD tarafından yürütülen etkinliklerde akademik programların oluşturulması ve siber güvenlik ekosisteminde ihtiyaç duyulan teknolojilerin belirlenmesi ve önceliklendirilmesi çalışmalarında yer alacak akademisyenler ile akademik ihtiyaçların belirlenmesine yönelik ortak akıl çalıştayı yapılacaktır.
18:00 - 19:00	**YUVARLAK MASA TOPLANTISI /2** **BGD - Kurumsal Üyeler Salon B**
	Oturum Başkanı - Session Chair: • Taha Yücel, *BGD Başkan Vekili*
	Oturum Konuları - Session Topics: • BGD tarafından yürütülen etkinliklerden sektör beklentilerinin ve isteklerinin belirlenmesi ve bu beklentilerin yürütülecek olan etkinliklere nasıl yansıtılacağına yönelik politikaların oluşturulması amacıyla BGD kurumsal üyelerinin katılımıyla ortak akıl çalıştayı yapılacaktır.

21 EKİM 2017, CUMARTESİ - *21 OCTOBER 2017, SATURDAY*

09:00 - 10:30	**PANEL - 3 / Ana Salon**
	"Siber Güvenlik ve Yapay Zeka, Cyber Security and AI"
	Panel Yöneticisi: • Prof. Dr. Şeref Sağıroğlu, *Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı*
	Panelistler: • Suphi Emre Şahin, *HAVELSAN Ar-Ge ve Mühendislik Grup Müdürü* • Emin İslam Tatlı, *STM Siber Güvenlik ve Büyük Veri Direktörü* • Yılmaz Değirmenci, *Kale İleri Teknoloji Siber Güvenlik Teknolojileri Direktörü* • Oğuz Yılmaz, *Labris Networks Teknoloji Direktörü* • Hasan Ali Pazar, *SIEMENS Türkiye Enerji Yönetimi Satış Grup Müdürü* • Atilla Biler, *TURKTRUST İş Geliştirme Md. / Ar-Ge Merkezi Danışmanı*
09:30 – 10:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon A**
	Oturum - 1 / Session 1
	Oturum Başkanı - Session Chair: • Prof. Dr. Ferruh Özbudak, *ODTÜ*
	Oturum Konuları - Session Topics: • 21- Üç Terimli Polinomlar için Karatsuba Benzeri Çarpma Yöntemlerinin Araştırılması • 46- Efficient Big Integer Multiplication in Cryptography • 58- Quantum Group Proxy Digital Signature based on Quantum Fourier Transform by using blinded and non blinded Trend
10:30 - 11:00	**ÇAY - KAHVE ARASI / COFFEE BREAK**
09:30 – 10:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon B**
	Oturum - 2 / Session 2
	Oturum Başkanı - Session Chair: • Prof. Dr. Halil İbrahim BÜLBÜL, *Gazi Üniversitesi*
	Oturum Konuları - Session Topics • 33- Biometric Verification on e-ID-Card Secure Access Devices: A Case Study on Turkish National e-ID Card Secure Access Device Specifications • 34- Biometric Based Cryptographic Key Generation For Secure Applications • 53- Evaluation of Fingerprint Enhancement Techniques Used by Crime Scene Investigation
09:30 – 12:30	**POSTER (DIALOGUE) SESSION / OTURUMU / Amfi Fuaye**
	Oturum - 1 / Session 1
	Oturum Başkanları - Session Chairs: • Doç. Dr. Murat Cenk, *ODTÜ* • Doç. Dr. Tolga Sakallı, *Trakya Üniversitesi* • Doç. Dr. Zülfükar Saygı, *TOBB ETÜ* • Yrd. Doç. Dr. Enis Karaarslan, *Muğla Sıtkı Koçman Üniversitesi* • Dr. Ahmet Sınak, *ODTÜ*
	Oturum Konuları - Session Topics: • 11 - The Analysis of the Concepts of Informatics, Cyber Crimes and Computer Forensics • 17 - Siber Savunma Tatbikatları: Planlama, Uygulama, Değerlendirme • 32 - Saldırı Tespit Sistemlerinde Ajan Sistemlerin Kullanımı • 35 - Karar Ağacı ile XSS Zararlı Kod Tespiti / Malicious XSS Code Detection with Decision Tree • 38 - Public and Private Sector Cooperation for Cyber Security
10:30 - 11:00	**İLETİŞİM ARASI / *BREAK TIME***

21 EKİM 2017, CUMARTESİ - *21 OCTOBER 2017, SATURDAY*

11:00 – 13:00	**Ana Salon / Main Hall**
	Siber Güvenlik Eğitimi Oturum 1 / Training on Cyber Security Session 1
	Konu Başlığı / Education Topic: • "Mobil Güvenlik ve Zararlı Yazılım Analizi Eğitimi"
	Eğitmenler / Instructors: • Murat Karaöz, Ayşe Selçuk - *HAVELSAN*
11:00 – 12:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon A**
	Oturum - 3 / Session 3
	Oturum Başkanı - Session Chair: • Doç. Dr. Suat Özdemir, *Gazi Üniversitesi*
	Oturum Konuları - Session Topics: • 13- Türkiye'de Siber Saldırılara Karşı Caydırıcılık • 20- Siber Güvenlik Ekosisteminin Geliştirilmesi Modeli: Siber Güvenlik Kümelenmesi • 22 - Siber Savunmada Yapay Zeka • 48- Blok Zinciri Tabanlı Siber Güvenlik Sistemleri
11:00 – 12:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon B**
	Oturum - 4 / Session 4
	Oturum Başkanı - Session Chair: • Doç. Dr. Sevil Şen, *Hacettepe Üniversitesi*
	Oturum Konuları - Session Topics: • 26- Android Kötücül Yazılım Tespiti Yaklaşımları • 40 - Android Uygulama İzinlerinin Analizi ile Kötücül Yazılım Tespiti • 49 - A Survey On Android Malware Detection Techniques Using Static Analysis
13:00 – 14:00	**ÖĞLE YEMEĞİ ARASI / LUNCH BREAK**
14:00 - 17:00	**SİBER GÜVENLİK EĞİTİMLERİ / Ana Salon / Main Hall**
	Siber Güvenlik Eğitimi Oturum 2/ Training on Cyber Security Session 2
	Konu Başlığı / Education Topic: • "Merkezi Kayıt ve Veri Kaybı Önleme Sistemleri Eğitimi"
	Eğitmenler / Instructors: • Cansu Tetik, *HAVELSAN*
14:00 - 15:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon A**
	Oturum - 5 / Session 5
	Oturum Başkanı - Session Chair: • Doç. Dr. Ecir Uğur Küçüksille, *Süleyman Demirel Üniversitesi*
	Oturum Konuları - Session Topics: • 18 - SCADA Sistemleri, Tehdit Ve Güvenlik Açıkları • 28 - Tasarımda Veri Koruma: Kişisel Veri Dostu Yazılımlar İçin Hukuki, İdari ve Teknik Bir Yaklaşım • 31 - Kurumsal Bilgi Güvenliği Üzerinde Yeni Kayıtlı İnternet Sitelerinin Etkisinin Analiz Edilmesi
14:00 - 15:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon B**
	Oturum - 6 / Session 6
	Oturum Başkanı - Session Chair: • Yrd. Doç. Dr. Mehmet DEMİRCİ, *Gazi Üniversitesi*
	Oturum Konuları - Session Topics • 24- Güvenlik Duvarı Etkinlik Ölçümü • 27 - Ağda Anomali Tespiti • 57 - Türkçe İçerikli Web Sayfaları için Zafiyet Tespit ve Önleme Modeli

21 EKİM 2017, CUMARTESİ - *21 OCTOBER 2017, SATURDAY*

15:30 - 16:00	**İLETİŞİM ARASI / *BREAK TIME***
16:00 - 17:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon A**
	Oturum - 7 / Session 7
	Oturum Başkanı - Session Chair: • Yrd. Doç. Dr. Hamdi Murat Yıldırım, *Bilkent Üniversitesi*
	Oturum Konuları - Session Topics: • 23 - A Spam Detection System with Short Link Analysis • 29 - A Review on Social Bot Detection Techniques and Research Directions • 36 - Naïve Bayes Classifier Based Spam Detection on Turkish SMS Messages
16:00 - 17:30	**ORAL PRESENTATION SESSION / SÖZLÜ SUNUM OTURUMU / Salon B**
	Oturum - 8 / Session 8
	Oturum Başkanı - Session Chair: • Yrd. Doç. Dr. İlker Özçelik, *Recep Tayyip Erdoğan Üniversitesi*
	Oturum Konuları - Session Topics: • 12 - Review of Evidence Collection and Evidence Protection Phases in Digital Forensics Process • 41-Implementation and Evaluation of Improved Secure Index Scheme Using Standard and Counting Bloom Filters • 45 - Ev ve Ofis Ağına Katılan Cihazların Güvenliğinin Artırılması için Basit makine Öğrenmesi Yöntemiyle Ağ Geçidi Üzerine Güvenlik Çözümleri Oluşturulması
17:30 - 18:00	**Kapanış Konuşmaları / Closing Remarks: Ana Salon**
	• Prof. Dr. Şeref Sağıroğlu, *ISC TURKEY 2017 Konferansı Eş Başkanı* • Prof. Dr. Mustafa Alkan, *ISC TURKEY 2017 Konferansı Eş Başkanı* • Prof. Dr. Ertuğrul Karaçuha, *ISC TURKEY 2017 Konferansı Eş Başkanı* • Prof. Dr. Ersan Akyıldız, *ISC TURKEY 2017 Konferansı Eş Başkanı*

ARTICLES PRESENTED IN ISCTURKEY 2017

ISCTURKEY 2017'DE SUNULAN BİLDİRİLER

Üç Terimli Polinomlar için Karatsuba Benzeri Çarpma Yöntemlerinin Araştırılması

Searching New Karatsuba-Like Polynomial Multiplication Algorithms for 3-Term Polynomials

Sedat AKLEYLEK
Bilgisayar Mühendisliği Bölümü
Ondokuz Mayıs Üniversitesi
Samsun, Türkiye
sedat.akleylek@bil.omu.edu.tr

Nurşah KAYA
Bilgisayar Mühendisliği Bölümü
Ondokuz Mayıs Üniversitesi
Samsun, Türkiye
nursahkaya93@gmail.com

***Özet*—Bu çalışmada, katsayıları tamsayı olan iki polinomu aritmetik karmaşıklık açısından daha verimli çarpan yöntemlerin araştırılması hedeflenmektedir. Bu yüzden, Böl-ve-Fethet mantığını kullanan, Karatsuba-Ofman Algoritmasından yola çıkarak çarpma işlemlerini daha az maliyetli toplama/çıkarma işlemleriyle değiştiren denklemler bulan bir yazılım gerçeklenmiştir. Geliştirilen uygulamada, üç terimli iki polinomun katsayılarının olası kombinasyonları kullanılarak çarpma işleminden sonra bütün çarpım katsayılarının bulunup bulmadığını test edilmektedir. Üç terimli polinomları çarpmak için 3 farklı yöntem olduğu ve bu yöntemlerin hepsinde 6 çarpma, 13 toplama/çıkarma işlemine ihtiyaç duyulduğu hesaplanmıştır. Bunlara ek olarak, daha fazla terimli polinomların çarpımı için ne tür uygulamalara ihtiyaç duyulduğu konusunda detaylara da yer verilmiştir.**

***Anahtar Kelimeler*—Polinom çarpımı, aritmetik karmaşıklık, sembolik hesaplama, Karatsuba-Ofman, Böl-ve-Fethet.**

***Abstract*—In this paper, new efficient methods are investigated to multiply two polynomials whose coefficients are integer. To achieve this, a software, based on divide-and-conquer idea, is developed with the help of Karatsuba-Ofman algorithm by replacing multiplication operations with addition/subtraction. This software checks all possible combinations of polynomial multiplications of three terms. With experimental results, there are three different methods to multiply 3-term polynomials with integer coefficients that need 6 multiplications and 13 additions. Moreover, the details are provided to extend this application for large dimensions.**

***Index Terms*— Polynomial multiplications, symbolic computation, complexity, Karatsuba-Ofman, divide-and-conquer.** *(key words)*

I. GİRİŞ

Bilgisayarlarda gerçeklenen bütün işlemler, mantıksal ve aritmetik işlemlere indirgenmektedir. Bilgisayar mimarisinde kullanılan temel aritmetik işlemler toplama ve çarpmadır. Sık kullanılmalarının nedeni; bilgisayar mimarisinde yapılan bir çok işlemin temelinde bu işlemlerin yer almasıdır [1]. Toplama işleminin maliyeti, doğrusal karmaşıklığa sahip olduğu için bazı durumlarda göz ardı edilmektedir. Çarpma işleminin maliyeti, toplama işleminin maliyetinden daha fazla olduğu için çarpmayı daha az maliyet ile gerçeklemek önem kazanmaktadır. Bu nedenle, bu çalışma kapsamında çarpma işlemine odaklanılacaktır.

Küçük sayılarda yapılan işlemlerde çalışma zamanı kabul edilebilir büyüklükte olsa da sayılar büyüdükçe işlemler yavaşlamakta hatta sonuca ulaşmak, işlemci gücüne göre farklılık gösterse de, yıllar almaktadır. İşlem gücü artan bilgisayarlara, yüklenen iş gücü de her geçen gün artmaktadır. Doğru orantılı olarak ilerleyen bu artış nedeni ile her zaman aritmetik işlemleri daha az maliyetle yapmanın yolu denenecektir. Bu yüzden çarpma işlemi üzerine olan ilgi sürekli olarak devam etmektedir ve muhtemel olarak devam edecektir [2].

Klasik çarpma işleminin zaman karmaşıklığı $O(n^2)$'dir. Bugüne kadar bu karmaşıklığı azaltmak ve daha az maliyetli bir çarpma algoritması bulmak için çeşitli çalışmalar yapılmış ve yapılmaya da devam edilmektedir. Karatsuba algoritması ile bu alandaki çalışmalar tetiklenmiştir [3]. Böl-ve-Fethet mantığıyla çalışan bu algoritma, klasik çarpma algoritmasından asimptotik olarak daha iyi bir başarım gerçekleştirmektedir. $O(n^2)$ olan karmaşıklığı $O(n^{\log_2 3})$'e indirgemektedir. Karatsuba algoritmasının temelindeki mantık; denklemlerde bulunan bazı özelliklere sahip birden çok çarpma işlemini, daha az çarpma ile yapılmasıdır. Bunu gerçekleştirirken varolan çarpmaları toplama/çıkarma işlemleri ile birleştirilmektedir. Karatsuba'dan sonra bu alana yönelim; kazancının fazla olması ve her alanda kullanılan uygulamaların performansını etkilemesi sebebiyle, gittikçe artmıştır. Karatsuba algoritmasının ortaya çıkmasından sonra farklı bakış açıları da ortaya çıkmıştır. Toom-Cook algoritması, 1963'te Andrei Toom tarafından bulunmuştur. Bu algoritma, Karatsuba algoritması gibi Böl-ve-Fethet mantığıyla çalışmaktadır. Fakat; büyük boyutlardaki iki sayıyı, iki eşit parçaya bölmek yerine, l uzunluğunda k eşit parçaya bölerek; başka bir ifade ile interpolasyon mantığını kullanarak çarpma işlemlerini gerçekleştirmekte ve karmaşıklığı azaltmaktadır. Toom-Cook-3 algoritması, k=3 olduğu durumdur ve karmaşıklığı $O(n^{\log_3 5})$'tir [4]. 1971'de A. Schönhage ve V. Strassen tarafından, sadece herhangi iki büyük sayının veya fazla terimli polinomların çarpımını hesaplamaya yönelik hızlı Fourier dönüşümüne dayalı $O(n \log n \log\log n)$ karmaşıklığında olan Schönhage-Strassen algoritması geliştirilmiştir. Hızlı Fourier dönüşümü, ayrık Fourier dönüşümünü $O(n \log n)$ karmaşıklık ile gerçekleştiren bir tekniktir [5]. Daha sonra 2007 yılında Schönhage-Strassen'den daha hızlı, $log^* x := \min\{k \in N : log^{ok} x \leq 1\}$, $log^{ok} := \log o \ldots_{kx} o\ log$ olmak üzere işlem karmaşıklığını $O(n \log n\, 2^{O(log^* n)})$'e düşüren Fürer algoritması, Martin Fürer tarafından bulunmuştur [6].

Bu çalışmaların temel amacı çarpma işleminin aritmetik karmaşıklığının azaltılmasını sağlamak ve ihtiyaç duyulan küçük boyutlu çarpma sayısını azaltmaktır. Bu çalışma kapsamında; katsayıları tamsayı olan iki polinomu çarpmak için gereken çarpma sayısını azaltarak, polinom çarpmasının

verimliliğini arttırılması amaçlanmaktadır. Katsayıları ifade eden bazı çarpmaları, daha az maliyetli olan toplama ve çıkarma işlemleriyle değiştirerek çarpma sayısını azaltan denklemlerin elde edilmesi hedeflenmektedir. Bu denklemleri elde edilmesi sırasında dikkat edilmesi gereken bir diğer husus ise toplama/çıkarma karmaşıklığıdır. Çarpma sayısı azaltılırken, arttırılan toplama/çıkarma işlemi sayısı, çarpma karmaşıklığını geçmemelidir. Bu yüzden yeni denklemler elde edildikten sonraki hedef aynı çarpma işlemi sayısına sahip, toplama/çıkarma sayısı daha az olan denklem gruplarının bulunmasıdır.

A. Motivasyon ve Katkı

Karatsuba'dan sonra bu alana ilgi artmış fakat Böl-ve-Fethet mantığıyla çalışan Karatsuba'dan farklı denklemler ile çarpma sayısını azaltmaya yönelik çok fazla çalışma yapılmamıştır. 2005 yılında, Montgomery'nin [7] numaralı çalışmasında; 5, 6 ve 7 terimli polinomların çarpımında Karatsuba denklemleri gibi denklemler arama yöntemi ile varolan çarpma sayısı bazı tek değerler için azaltılmıştır. Fakat bu çalışmada denklem arama algoritması açıklanmamıştır. [8] numaralı çalışmada yazarlar, n^2 çarpma ve $(n-1)^2$ toplama/çıkarma işlemi kullanarak polinom çarpımını gerçekleştiren Klasik çarpma yöntemi ile Karatsuba yöntemini karşılaştırmıştır. Bu karşılaştırmanın sonucunda çarpma ve toplama işlemlerinin birbiri türünden maliyetini hesaplanarak, kazanç belirlenmiş ve beş terimli iki polinomun çarpımı için Karatsuba'dan daha verimli bir çarpma yöntemi önerilmiştir. Aynı zamanda farklı bölme boyutlarına göre (örneğin, ikiye parçalama yerine herhangi bir asal sayıya göre parçalama) Karatsuba algoritmasının genelleştirilmesi yapılmıştır.

İşlemci firmaları özellikle kriptografik işlemleri verimli yapabilmek amacıyla polinom çarpımları için özel teknikler kullanmakta ve bunlar için Böl-ve-Fethet yaklaşımı baz alınarak alt işlemciler tasarlamaktadırlar [9]. Bunlar göz önüne alındığında küçük boyutlu polinomların çarpımının, detaylı olarak araştırılması gereken önemli bir konu olduğu ortaya çıkmaktadır.

Bu çalışma, Karatsuba algoritması ile aynı çarpma sayısına ve daha az toplama/çıkarma sayısına sahip çarpma yöntemlerini bulmak üzere yapılmıştır. Sembolik hesaplama tabanlı çalışan arama algoritması için bir veri yapısı tasarlanmış ve uygulanmıştır.

B. Organizasyon

Bölüm 2'de üç terimli iki polinomun çarpımı için çarpma yöntemlerinin bulunmasına ve bu yöntemlerde kullanılan veri yapısına detaylı olarak değinilmiştir. Veri yapısı içerisindeki sembolik hesaplama işlemlerinden ayrıntılı olarak bahsedilmiştir. Bölüm 3'de daha fazla elemana sahip polinomların çarpımı için bazı öneriler ve sonuçlar verilmiştir. Ayrıca, gelecek çalışmalar hakkında açıklamalar detaylandırılmıştır.

II. ÜÇ TERİMLİ İKİ POLİNOMUN VERİMLİ ÇARPMA YÖNTEMLERİNİN BULUNMASI

Bu bölümde, Karatsuba çarpma yöntemi hatırlatılmakta, çalışmanın temelini oluşturan arama algoritması verilmekte ve daha sonra Karatsuba benzeri çarpma yöntemlerini bulabilmek amacıyla oluşturulan yazılımın detayları anlatılmaktadır.

Karatsuba çarpım gruplarında, eşitlik (1)'deki n terimli iki polinomun çarpımındaki katsayıların kombinasyonlarının oluşturduğu denklemlerin toplanması veya çıkarılması ile eşitlik (2)'deki sonuç denklemlerinin katsayıları elde edilmektedir.

$$\begin{aligned} \text{a(x)} &= a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \\ \text{b(x)} &= b_{n-1}x^{n-1} + \ldots + b_1x + b_0 \end{aligned} \tag{1}$$

$$\text{a(x) b(x)} = a_{n-1}b_{n-1}x^{2(n-1)} + \ldots + (a_0b_1 + a_1b_0)\,x + a_0b_0 \tag{2}$$

Karatsuba denklemlerinin bulunma mantığı, çalışmanın gidişini anlamak açısından önemli bulunmaktadır. Bu yüzden, eşitlik (3)'deki üç terimli iki polinomun çarpımında kullanılan Karatsuba denklemleri eşitlik (5)'te detaylandırılmıştır.

$$\begin{aligned} \text{a(x)} &= a_2x^2 + a_1x + a_0 \\ \text{b(x)} &= b_2x^2 + b_1x + b_0 \\ \text{a(x) b(x)} &= a_2b_2x^4 + (a_1b_2 + a_2b_1)\,x^3 + \\ &(a_2b_0 + a_1b_1 + a_0b_2)\,x^2 + (a_0b_1 + a_1b_0)x + a_0b_0 \end{aligned} \tag{3}$$

Üç terimli iki polinomun çarpımında oluşan 5 katsayı eşitlik (4)'de bulunmaktadır:

$$\begin{aligned} \text{Ks[1]} &= a_0b_0 \\ \text{Ks[2]} &= a_2b_2 \\ \text{Ks[3]} &= a_0b_1 + a_1b_0 \\ \text{Ks[4]} &= a_1b_2 + a_2b_1 \\ \text{Ks[5]} &= a_2b_0 + a_1b_1 + a_0b_2 \end{aligned} \tag{4}$$

Bu katsayıları elde etmek için 9 çarpmayı, 6 çarpmaya düşüren Karatsuba çarpımları ve denklemleri eşitlik (5)'te bulunmaktadır:

$$\begin{aligned} &M_0: a_0b_0 \quad M_3: (a_0+a_1)(b_0+b_1) \\ &M_1: a_1b_1 \quad M_4: (a_1+a_2)(b_1+b_2) \\ &M_2: a_2b_2 \quad M_5: (a_2+a_0)(b_2+b_0) \\ &\text{Ks[1]} = M_0, \quad \text{Ks[3]} = M_3 - M_0 - M_1 \\ &\text{Ks[2]} = M_2, \quad \text{Ks[4]} = M_4 - M_1 - M_2 \\ &\text{Ks[5]} = M_5 - M_0 - M_2 \end{aligned} \tag{5}$$

A. Karatsuba Benzeri Çarpma Yöntemlerini Arama Algoritması

Bu çalışmada, üç terimli polinomların çarpımlarını üretirken Karatsuba Algoritması'nın temelde kullandığı mantıkla ilerleyerek, tüm olasılıkları kullanan bir arama algoritması tasarlanmıştır. Bu algoritmanın adımları şu şekildedir:

1. $a_2{*}x^2 + a_1{*}x + a_0$ ve $b_2{*}x^2 + b_1{*}x + b_0$ polinomlarının çarpımındaki katsayıların bütün olası kombinasyonları eşitlik (6)'daki şekilde hesaplanmış ve $0 \leq i \leq 48$ olmak üzere bütün M_i çarpımları kaydedilmiştir. Ek_1'de bütün M çarpımları gösterilmiştir.

$$\left[\binom{3}{1} + \binom{3}{2} + \binom{3}{3}\right]\left[\binom{3}{1} + \binom{3}{2} + \binom{3}{3}\right] = 7 \cdot 7 = 49 \tag{6}$$

2. 49 çarpmadan, istenilen çarpma sayısınca yani 6'sı seçilerek bir çarpma grubu oluşturulmaktadır. Üç terimli iki polinomun çarpımında, $\binom{49}{6}$ olası çarpma grubu bulunmaktadır.

3. Bu çarpmalar, olabilecek bütün toplama/çıkarma işlemlerine tabi tutulmaktadır. Öncelikle seçilen 6 M değerinden biri rastgele alınmakta ve başa getirilmektedir. Daha sonra kalan M değerlerinin toplama ve çıkarmadan oluşan bütün kombinasyonları eşitlik (7)'deki şekilde hesaplanmaktadır.

$$\binom{6}{1}[\,2\binom{5}{1} + 2^2\binom{5}{2} + 2^3\binom{5}{3} + 2^4\binom{5}{4} + 2^5\binom{5}{5}] \qquad (7)$$

Bu işlem sonucunda 1432 tane denklem ortaya çıkmaktadır. Bunlar, M çarpımlarından oluşan k denklemlerini ifade etmektedir. Bu k denklemleri eşitlik (8)'de bulunmaktadır.

$$k_i = M_{40} - M_{21} + M_7 + M_{34} - M_{10} + M_{18} \qquad (8)$$

4. Oluşan her k_i denklemi, sonuç katsayıları ile karşılaştırılmaktadır. 1432 denklem içinde 5 sonuç katsayısını da sağlayan denklemler bulunduğunda, bu denklem grubu sonuç denklem grubuna eklenmektedir. Olası M çarpımlarının hepsi bitene kadar 2. adıma dönülmekte ve yeni M çarpımları seçilerek, sonraki adımlar tekrarlanmaktadır. Olası M çarpımlarının hepsi tarandıktan sonra bir sonraki adıma geçilmektedir.

5. En son bulunan bütün denklem grupları içinden en az çarpma ve toplama/çıkarma işlemiyle bütün katsayıları üreten denklem grubu aranmaktadır. Amaç en az çarpma ile çarpma ve toplama/çıkarma oranını minimize edilmesidir. Sonuç denklemlerinin çarpma ve toplama/çıkarma oranı, eşitlik (9)'da belirtilen yapıya göre kontrol edilmektedir.

Yazarlar, [8] numaralı çalışmada, bu sayıyı kontrol etmek için bir r oranı belirlemiştir. Bunu basit olarak göstermek gerekirse; n terimli iki polinomun çarpımını n^2 çarpma işlemi ve $(n-1)^2$ toplama işlemi ile gerçekleştiren klasik çarpma yöntemi ile, üç terimli iki polinomun çarpımı için daha az maliyetli çalıştığı bilinen Karatsuba algoritmasının karşılaştırılması eşitlik (9) ve eşitlik (10)'da bulunmaktadır.

r = tm / ta
tm: 1 çarpma işleminin maliyeti
ta: 1 toplama işleminin maliyeti

cs (klasik çarpma yöntemi) = 4ta + 9tm
ck (Karatsuba Algoritması) = 13ta + 6tm (9)

ck < cs
13 ta + 6 tm < 4ta + 9 tm (10)
9 ta < 3tm
3 < tm / ta
3 < r

İfade (10)'daki karşılaştırma işleminin sonucunda 3<r oranı elde edilmektedir. Başka bir deyişle bir çarpma, üç toplamadan daha maliyetlidir [8].

B. Veri Yapısı

Bu kısımda, çalışma için yapılan uygulama içerisinde sembolik hesaplama işlemi için kullanılan veri yapısından ve bu veriler üzerindeki sembolik hesaplama işlemlerinden bahsedilmektedir.

Global sınıfı, gerekli değişkenleri ve fonksiyonları diğer sınıflardan soyutlanmış olarak tanımlayarak gerektiğinde bütün sınıflarda kullanılabilmesini sağlamakta ve sınıf kütüphanesi olarak adlandırılmaktadır. Diğer sınıflar içerisinde, her fonksiyondan erişime açık global bir değişken tanımlamak yerine; Global sınıfı içerisinde değişkenler kullanılmıştır.

1) Genel Yapıyı Oluşturan Fonksiyonlar:

Şekil 1. Fonksiyon şeması

Şekil 1.'de sembolik hesaplama için oluşturulan yazılımın fonksiyonel şeması kabaca verilmiştir. Bu kısımdaki fonksiyonların kapsamlı şeması EK-2'de verilmiştir. Kombinasyon işlemlerini hesaplamak için kullanılan bazı fonksiyonları anlatmaya gerek duyulmamıştır.

Main() fonksiyonunda, girilen polinomların katsayıları belirlenmekte ve iki polinomun çarpımındaki katsayıların bütün olası kombinasyonları hesaplanarak eşitlik (11)'deki M ve eşitlik (12)'deki $Toplam$ dizilerine iki farklı şekilde yazdırılmaktadır. Bu iki dizi aslında aynı kavramı ifade etmektedir. Fakat, ayrı yerlerde kullanılmak üzere tasarlanmıştır. M dizisinde, çarpımların dağılmış hali tutulmaktadır.

$$M_i = \text{“}a_0b_0 + a_0b_1 + a_1b_0 + a_1b_1\text{”} \qquad (11)$$

M dizisi, M çarpımları üzerinde sembolik işlemleri uygularken kolaylık sağlanması, her seferinde yapılması gereken çarpma işlemini kaldırmak ve yalnızca sembolik toplama/çıkarma işlemiyle uğraşmak amacıyla tanımlanmıştır. Bundan sonra bütün işlemler M dizisi ile gerçekleştirilecektir. Oluşturulduktan sonra üzerine herhangi bir işlem uygulanmayacaktır. Bu yüzden global sınıfında tanımlanmıştır. $Toplam$ dizisinde ise, çarpımların dağılmamış hali tutulmaktadır.

$$Toplam_i = \text{“}(a_0 + a_1)(b_0 + b_1)\text{”} \qquad (12)$$

Daha sonra yapılması planlanan, sonuç denklemleri üzerinde toplama sayısını hesaplamak için benzer yapıların olup olmadığını kontrol etmek amacıyla oluşturulmuştur. M dizisinde olduğu gibi bütün değişikliklere kapalı bulunmaktadır.

Bundan sonra M_asil_atama() fonksiyonu çağrılmaktadır. Bu fonksiyonda, M dizisinin elemanlarının indislerinin 6'lı kombinasyonları alınarak, eşitlik (13)'deki M_Asil dizisi üretilmektedir. Burada M_Asil dizisinin elemanları;

$$M\_Asil_i = \{\text{“17”, “5”, “42”, “29”, “34”, “16”}\} \quad (13)$$

şeklinde, sayılardan oluşan string değerleridir. Her eleman için iç içe bir for döngüsü açılmaktadır. İlk for döngüsü 0'dan başlamakta ve 49'a kadar gitmektedir. Daha sonraki for döngüleri, bir üstteki for döngüsünün başlangıç değerinin bir fazlasından başlamakta ve 49'a kadar gitmektedir. Sona doğru yaklaştıkça hesaplama sayısı azalmaktadır. Bu kısımda iç içe açılan for'ları parçalara bölerek farklı bilgisayarlarda ya da aynı bilgisayarda paralel olarak çalıştırmak zamandan kazanç sağlamaktadır. Bir işi birden çok iş bölümüne ayırarak eş zamanlı olarak çalıştırmak, işlemlerin daha kısa zamanda yapılmasına olanak sağlamaktadır. Bu çalışmada, for döngülerini eş zamanlı olarak çalıştırarak sonuçlar elde edilmektedir. Her döngüde üretilen M_Asil dizisi, Carpma_Hesaplama() fonksiyonuna parametre olarak gönderilmektedir. Bütün fonksiyonlar çalıştırılmakta ve sonuç değerleri üretilmektedir. En son M_asil_atama() fonksiyonuna geri dönülmekte ve bütün for'lar sonlanana kadar yeni bir M_Asil dizisi üretilmektedir. Fakat yeni bir dizi oluşturulmadan önce gerekli global değişkenler sıfırlanarak yeni dizi için hazır hale getirilmektedir.

Buraya kadar anlatılan kısımda temel amaç, işlemler başlamadan önce kullanılacak ve değişmeyecek bazı global değişkenlerin tanımlanması ve ana yapıdan bahsedilmesidir. Bundan sonraki kısımda M çarpımları üzerindeki sembolik hesaplamanın nasıl yapıldığına değinilecektir.

2) Sembolik İşlemleri Gerçekleştiren Fonksiyonlar:

Carpma_Hesaplama() fonksiyonu, M_Asil dizisinin elemanlarından birini başa koyulmakta ve kalan 5 değerin olası bütün kombinasyonları bulunmaktadır. İfade (14) bu kombinasyonların sayısı verilmektedir.

$$\binom{6}{1}\left[\binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5}\right] = 196 \quad (14)$$

Bütün toplama/çıkarma içeren olasılıkların taranması gerektiği için bu dizinin her elemanı tek tek arti_eksi() fonksyonuna yollanmakta ve toplama/çıkarma işlemi içeren k denklemleri elde edilmektedir. Burada bütün elemanları aynı anda yollamak ve hesaplanan değerleri tek bir dizi içerisinde tutmak, bilgisayarların işlem gücünü ve hafızasını zorladığı için her eleman ayrı olarak yollanmaktadır. Bu sayede hepsinin sonucunu tutan, çok büyük boyutlu bir dizi tanımlanması gerekmemektedir. Elde edilen her bir denklem; sonucu sağlayıp sağlamadığını kontrol edildikten sonra silinmektedir. Bu da bize hafızadan kazanç sağlamaktadır.

Toplama/çıkarma işlemi içeren eşitlik (8)'deki k denklemlerini bulmak için doğruluk tablosu mantığı kullanılmaktadır. Şöyle ki; diziler uzunluğuna bağlı olarak sayısı değişen for döngülerine girmektedirler. İç içe olan bütün for döngüleri iki defa dönmekte ve her dönüşte işaret değiştirilmektedir. Bu işlemler sonucunda bütün olası kombinasyonlar elde edilmektedir. Temel mantık Şekil 2'de uzunluğu 2 olan denklemler için sözde koda dökülmüştür.

Bu kısımda elde edilen işaretli k denklemleri kaydedilmemektedir. Eşitlik (8)'de tanımlı k denklemi sistemde eşitlik (15)'deki şekilde tutulmaktadır.

$$k_i = 40 - 21 + 7 + 34 - 10 + 18 \quad (15)$$

```
for (int i = 0; i < 2; i++){
    for (int j = 0; j < 2; j++){
      if (cikis[0] == "+"){
        m_string = cikis[1] + arr[1] + cikis[0] + arr[0];
        cikis[0] = "-"; }
      else if (cikis[1] == "-"){
        m_string = cikis[1] + arr[1] + cikis[0] +  arr[0];
       cikis[0] = "+";  }
     }
     if (cikis[1] == "+")
      cikis[1] = "-";
     else
        cikis[1] = "+";
}
```

Şekil 2. Uzunluğu 2 Olan Denklemler İçin Algoritma

Burada bulunan sayılar ile M çarpımlarının index değerleri temsil edilmektedir. Unutulmamalıdır ki; burada yer alan sayılar ile standart aritmetik işlemler değil, sembolik hesaplama işlemleri yapılmaktadır. Elde edilen işaretli k denklemi, m_cevir() fonksiyonuna yollanmaktadır. Bu fonksiyon kendisine gelen işaretli k denkleminde eşitlik edilen M çarpımlarının indislerini almakta ve M dizisinde yerlerine koyarak eşitlik (16)'da gösterilen değişimi gerçekleştirmektedir.

Girdi = “0+16-32+20” stringinin ifade ettiği denklem,

$$\text{“0+16-32+20”} = M_0 + M_{16} - M_{32} + M_{20} \quad (16)$$

$$\text{Çıktı} = a_0b_0 + a_2b_2 - a_0b_0 - a_0b_2 - a_2b_0 - a_2b_2 + a_2b_0 + a_2b_1 + a_2b_2$$

$$= a_2b_1 + a_2b_2 + a_0b_2$$

Buradaki çevrim işleminde algoritma şu şekilde çalışmaktadır: String olarak tutulan k denkleminin birinci elemanını almakta ve bir sonraki eleman '+' veya '-' mi diye kontrol etmektedir. Eğer '+' veya '-' ise tek basamaklı bir sayı olduğuna karar vermektedir. İki veya daha fazla basamaklı olma durumunu da aynı şekilde kontrol etmektedir. İfade (7)'de gösterildiği gibi, bu yapıdaki M çarpımlarının sayısı 49 olduğu için üç basamaklı indis değeri bulunmamaktadır. Bu yüzden, basamak değeri ikiye kadar kontrol edilmektedir. Üçten fazla terimli iki polinomun çarpımı için burada bulunan basamak sayısı kontrol edilmeli ve bunun için gerekli olan arttırma yapılmalıdır. Basamak sayısına karar verdikten sonra, string içinden çekilen karakterler integer türüne çevrilmektedir. Daha sonra M dizisinin indisi olarak kullanılmakta ve M dizisinde ifade ettiği çarpım değeri çıktı değişkenine

atanmaktadır. Her indis için bu işlemler tekrar edilmektedir. Burada en önemli nokta: çevrim işleminden sonra M çarpımlarını birleştirirken işarete dikkat edilmesidir. İşaret '-' olduğu zaman çarpımın içindeki bütün '+' işaretleri, '-' işaretlerine çevrilmekte ve denklemin başına '-' işareti koyulmaktadır. Örnek olarak eşitlik (16)'da girdi olarak gelen k denkleminin çevrim işlemini adım adım anlatılmıştır:

1. Bu denklemde ilk eleman 0 olduğu için M dizisinin M_0 elemanına gidilmektedir. M_0 elemanı 'a_0b_0' denk gelmektedir. 'a_0b_0' çıktı değişkenine atanmaktadır. 0'dan sonra gelen eleman '+' veya '-' ise işaret belirlenmekte ve bir sonraki işlemi etkileyeceği için işaret değişkenine atanmaktadır. Bu değişken sayesinde M dizisinin elemanları önlerinde bulunan işarete göre yeniden düzenlenmektedir. Eğer sonradan gelen eleman '+' veya '-' değil ise, '+' veya '-' bulunana kadar her eleman birleştirilmekte daha sonra indis olarak kullanılmaktadır.

çıktı = M_0 şeklinde değiştirilmektedir.

2. "16-" değeri için 1'i ve 6'yı almakta ve '-' karakterini görünce durmaktadır. Daha sonra "16" stringini integer değere dönüştürmektedir. Bir önceki işlemden gelen işaret değişkeni '+' olduğu için; M_{16} denkleminin içi olduğu gibi bırakılmakta ve başına '+' işareti atanmaktadır. Çıkarken bir sonraki eleman '-' karakteri olduğu için işaret değişkeni '-' yapılmaktadır.

çıktı = çıktı + "+" + M_{16} şeklinde değiştirilmektedir.

3. Bir sonraki indis 32'dir. işaret değeri '-' olduğu için M_{32} denkleminin içinde bulunan bütün '+' işaretleri, '-' işaretine dönüştürülmekte ve başına '-' atanmaktadır. Çıkarken bir sonraki eleman '+' karakteri olduğu için işaret değişkeni '+' yapılmaktadır.

çıktı = çıktı + "-" + M_{32}.replace('+','-') şeklinde değiştirilmektedir.

4. Bir sonraki indis 20'dir. İşaret değeri artı olduğu için M_{20} denklemi olduğu gibi çıktı değerine eklenmekte ve başına '+' işareti atanmaktadır.

çıktı = çıktı + "+" + M_{20} şeklinde değiştirilmektedir.

Yukarıda anlatılan 4 adımda yapılan işlemler her k denklemi için yeniden tekrar edilmektedir. Adım sayısı denklemin uzunluğuna bağlı olarak değişmektedir. En son oluşan çıktı değeri Denklem_Sonuc() fonksiyonuna gönderilmektedir.

Bu fonksiyon sembolik toplama ve çıkarma işlemlerini gerçekleştirmekte ve string üzerindeki gerekli sadeleştirmeleri yaparak sonucu döndürmektedir.

Sadeleştirme işlemleri aşağıdaki şekilde gerçekleşmektedir:

1. String değeri, ilk bulunan '+' karakterine göre 2 parçaya bölünmekte ve bir diziye atanmaktadır. Daha sonra aynı string, ilk gelen '-' karakterine göre 2 parçaya bölünmekte ve başka bir diziye atanmaktadır.

2. Bu dizilerin uzunluğuna bakılarak gelen işaret belirlenmektedir. Uzunluğu daha küçük olan dizi, ilk gelen işaretin ne olduğunu belirlemekte ve bu değer işaret değişkenine atanmaktadır. İşaret değişkeni, önünde bulunan denklemi etkilediği için bir sonraki döngüde kullanılmaktadır.

3. İşaret değişkeni belirlendikten sonra işaret, '+' ise bu eleman '+' işaretli çarpımları tutan diziye, '-' ise '-' işaretli çarpımları tutan diziye eklenmektedir.

4. İki dizi karşılaştırılmakta ve aynı eleman bulunduğu durumda iki diziye de 'null' değeri atanmaktadır. Başka bir deyişle; farklı işaretli, aynı elemanlar birbirini sadeleştirmektedir.

5. Son olarak, ayrılan diziler birleştirilerek bir denklem oluşturulmaktadır. İki dizinin elemanları bir dizide birleştirilirken 'null' değeri ile karşılaşıldığında dizi bir kaydırılmaktadır.

Daha sonra bu sonuç, karsilastir_ve_bitir() fonksiyonuna gönderilmektedir. Herhangi bir katsayı ile eşleşip eşleşmediği kontrol edilmektedir. Bu kontrol işlemi, sonuç ifadesinin katsayıdan çıkarılması ile gerçekleştirilmektedir. Eğer bulunan değer 'null' ise katsayı ile eşleşmektedir. Bu yüzden katsayıların kontrol edildiği dizide eşleşen katsayı bir arttırılmaktadır. Daha sonra Carpma_Hesaplama() fonksiyonuna dönülmektedir. Burada M_Asil dizisinden oluşturulan kombinasyonlardan bir diğeri alınmakta ve aynı işlemler tekrar edilmektedir. Bütün kombinasyonlar kontrol edildikten sonra katsayıların hepsi sağlanıyorsa M_Asil dizisi diğer bir deyişle M çarpım grubu istenilen şartları sağlıyor denilmektedir. Daha sonra M_Asil_Atama() fonksiyonuna dönülmekte ve yeni bir M_Asil dizisi oluşturulmaktadır. Bütün M_Asil kombinasyonları tarandığında program sonlanmaktadır.

C. Bulunan Sonuçlar ve Karşılaştırma

Çalışma kapsamında, üç terimli iki polinomun çarpımında ortaya çıkan katsayıları, Karatsuba'dan farklı çarpım grupları ile elde edilmesi sağlanmıştır. Bu çarpım grupları aşağıdaki gösterilmiştir:

1.Grup
1. katsayıya $(a_0b_0) = M_0$
2. katsayıya $(a_2b_2) = M_{16}$
3. katsayıya $(a_0b_1+a_1b_0) = M_{24} - M_8 - M_0$
4. katsayıya $(a_1b_2+a_2b_1) = M_{48} - M_{32} - M_{24} + M_0$ (*)
5. katsayıya $(a_2b_0+ a_1b_1+a_0b_2) = M_8 + M_{32} - M_{16} - M_0$

2.Grup
1. katsayıya $(a_0b_0) = M_0$
2. katsayıya $(a_2b_2) = M_{16}$
3. katsayıya $(a_0b_1+a_1b_0) = M_{48} - M_{32} + M_{16} - M_{40}$ (*)
4. katsayıya $(a_2b_0+ a_1b_1+a_0b_2) = M_{40} - M_8 - M_{16}$
5. katsayıya $(a_2b_0+ a_1b_1+a_0b_2) = M_8 + M_{32} - M_{16} - M_0$

3.Grup (Karatsuba Ofman)
1. katsayıya $(a_0b_0) = M_0$
2. katsayıya $(a_2b_2) = M_{16}$
3. katsayıya $(a_0b_1+a_1b_0) = M_{24} - M_8 - M_0$
4. katsayıya $(a_1b_2+a_2b_1) = M_{40} - M_8 - M_{16}$
5. katsayıya $(a_2b_0+ a_1b_1+a_0b_2) = M_8 + M_{32} - M_{16} - M_0$

(*) Yıldızlı çarpım denklemleri, Karatsuba çarpımlarına farklılık katan çarpım denklemleridir. Bu iki çarpım grubu da üç terimli iki polinomun çarpımını 6 çarpma, 13 toplama/çıkarma işlemiyle gerçekleştirmektedir. Üç terimli polinomların denklem uzayı çok büyük olmadığı için Karatsuba'dan farklı çarpım grubu sayısı az bulunmaktadır.

Çarpım uzayı büyüdükçe bunu sağlayan daha fazla çarpım grubu elde edileceği öngörülmektedir.

Çarpma sayısını hesaplanırken, seçilen M_Asil dizisinin eleman sayısına bakılmakta ve işlem yapılan M çarpımı kadar çarpmaya ihtiyaç duyulmaktadır.

Toplama sayısını hesaplanırken dikkat edilmesi gereken en önemli husus tekrar eden yapıların belirlenmesi ve daha önce hesaplanan bir yapının yeniden hesaplanmamasıdır. Toplama işlemi hesabını daha iyi anlamak için, 1.Grup için toplama/çıkarma sayısının hesaplanışı adım adım gösterilmiştir:

1.Grup M çarpımları:

$M_0 = a_0 b_0$
$M_8 = a_1 b_1$
$M_{16} = a_2 b_2$
$M_{24} = (a_0 + a_1)(b_0 + b_1)$
$M_{32} = (a_0 + a_2)(b_0 + b_2)$
$M_{48} = ((a_0 + a_1) + a_2)((b_0 + b_1) + b_2)$

İlk 3 çarpımda toplama/çıkarma bulunmamaktadır. M_{24} ve M_{32} çarpımlarında 2 tane toplama bulunmaktadır. M_{48} çarpımında toplama sayısı 4 gibi görünse de daha önce hesaplanan parantez içindeki yapılar bir daha hesaplanmayacağı için 2 toplama bulunmaktadır.

1.Grup katsayı denklemleri:

1. katsayıya $(a_0 b_0) = M_0$
2. katsayıya $(a_2 b_2) = M_{16}$
3. katsayıya $(a_0 b_1 + a_1 b_0) = (M_{24} - M_0) - M_8$
4. katsayıya $(a_1 b_2 + a_2 b_1) = M_{48} - M_{32} - (M_{24} - M_0)$
5. katsayıya $(a_2 b_0 + a_1 b_1 + a_0 b_2) = M_8 + M_{32} - M_{16} - M_0$

İlk iki katsayıda toplama/çıkarma bulunmamaktadır. 3. katsayıda 2 çıkarma işlemi bulunmaktadır. 4. katsayıda çıkarma işlemi sayısı 3 gibi görünse de, 3. katsayıda hesaplanan parantez içindeki yapı bir daha hesaplanmamaktadır. Bu yüzden 4. katsayıda 2 çıkarma işlemi bulunmaktadır. 5. katsayıda 4 toplama/çıkarma işlemi bulunmaktadır. Bu işlemde dikkat edilmesi gereken nokta: toplama/çıkarma sayısını azaltmak için paranteze alınan yapıların, başka bir eleman ile paranteze alınanamasıdır.

Sonuç olarak, M çarpımından ve katsayı denklemlerinden gelen toplama/çıkarma işlemi sayıları eşitlik (17)'deki şekilde toplanmaktadır.

$$(2 + 2 + 2) + (2 + 2 + 3) = 13 \text{ toplama/çıkarma} \qquad (17)$$

Tablo 1'de elde edilen sonuçlar özetlenmiştir.

İşlem Sayısı Karşılaştırma		
	İşlemler	
Denklem Grupları	*Çarpma*	*Toplama*
1. Grup	6	13
2. Grup	6	13
Karatsuba Algoritması	6	13

Tablo 1. İşlem Sayısı Karşılaştırması

III. SONUÇLAR VE GELECEK ÇALIŞMALAR

Bu çalışmada, üç terimli iki polinomun çarpımı için gerçeklenen uygulamayı, beş terimli iki polinomun çarpımı için de geliştirilmiş bulunmaktadır. Ancak arama uzayı çok büyük olduğu için detaylı sonuçları burada verilememektedir. Beş terimli iki polinomun çarpımında olası M çarpımlarının sayısı eşitlik (18)'deki şekilde hesaplanmaktadır:

$$\left[\binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5}\right]^2 = 31.31 = 961 \qquad (18)$$

Beklenilen 15 veya daha az çarpma ile polinom çarpımını gerçekleştirmektir. Bu yüzden çarpma sayısını 15 seçilmekte ve beş terimli iki polinomun çarpımındaki olası çarpma sayısı, $\binom{961}{15}$'li kombinasyonu şeklinde hesaplanmaktadır. Bu kombinasyonlar, eşitlik (13)'de gösterilen üç terimli polinomlar için oluşturulan M_Asil dizisini, beş terimli polinomlar için oluşturmaktadır. M_Asil dizisinin elemanlarından oluşturulan olası bütün pozitif denklemlerin sayısı eşitlik (19)'daki şekilde hesaplanmaktadır.

$$\binom{15}{1}\left[\binom{14}{0} + \binom{14}{1} + \cdots + \binom{14}{13} + \binom{14}{14}\right. \qquad (19)$$

Sadece toplama içeren eşitlik (19)'daki denklemlerden, toplama ve çıkarma içeren denklemler elde edilmektedir. Bütün durumları içeren denklemlerin sayısı eşitlik (20)'deki şekilde hesaplanmaktadır.

$$\binom{15}{1}\left[2\binom{14}{1} + 2^2\binom{14}{2} + \cdots + 2^{14}\binom{14}{14}\right] \qquad (20)$$

Bu hesaplama işlemleri, n = terim sayısı olmak üzere aşağıdaki eşitlik için genelleştirilirse eşitlik (21) ve (22)'deki işlemler elde edilmektedir.

$$\begin{aligned} a(x) &= a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ b(x) &= b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \\ a(x)\,b(x) &= a_{n-1}b_{n-1}x^{2(n-1)} + \ldots + (a_0 b_1 + a_1 b_0)\,x + a_0 b_0 \end{aligned}$$

n terimli iki polinomun çarpımdaki M çarpımlarının sayısı:

$$\prod_{i=1}^{2} \sum_{m=0}^{n} \binom{n}{m} \qquad (21)$$

Bütün durumları içeren k denklemlerinin sayısı:

$$\binom{k}{1} \sum_{i=1}^{k} 2^i \binom{k}{i} \qquad (22)$$

Beş terimli iki polinomun çarpımında, yeterli hesaplama gücüne sahip olunmadığı için çarpım sonuçları elde edilememiştir. Uygulama, hesaplama gücü arttırıldığında daha fazla terimli polinom çarpımlarını gerçekleştirebilecek şekilde tasarlanmıştır. İçerisindeki sembolik hesaplama işlemleri çözüme ulaşma süresini arttırmaktadır. Uygun denklemleri bulmak için yapılan hesaplamalar tamamen paralel hale getirilirse, programın çok daha verimli çalışacağı ve daha çok terimli polinom çarpımlarındaki katsayı denklemlerini de bulabileceği öngörülmektedir.

Bu çalışmada, sembolik hesaplama ile üç terimli iki polinomun çarpımı için olası tüm çarpma yöntemlerini elde eden bir arama algoritması tasarlanmış ve bunun uygulaması gerçeklenmiştir. Oluşturulan yazılımın daha fazla elemana sahip polinomlar için de kullanılabileceği belirtilmiş ve bunlar için gerekli olan tüm hesaplamaların nasıl yapılacağı genelleştirilerek açıklanmıştır.

IV. TEŞEKKÜR

Bu çalışma 116E279 proje numarası ile TÜBİTAK tarafından desteklenmiştir.

KAYNAKLAR

[1] J. Von zur Gathen, ve J. Gerhard, Modern Computer Algebra, 3rd ed., Cambridge University Press, 2013.

[2] D. Knuth, The Art of Computer Programming, 3rd ed., vol. 2. Seminumerical Algorithms, 1997.

[3] A. Karatsuba ve Y. Ofman, "Multiplication of Many-Digital Numbers by Automatic Computers", Physics-Doklady, 7, 1963, syf. 595-596.

[4] T. Cook ve A. Stephen, "On the Minimum Computation Time of Functions", Doktora Tezi, Harvard University Department of Mathematics, 1966.

[5] M. Heideman, D. Johnson, C. Burrus, "Gauss and the history of the fast fourier transform", IEEE ASSP Dergisi, Cilt 1(4), 1984, syf. 14-21.

[6] M. Fürer, "Faster Integer Multiplication", Pennsylvania State University, Amerika, 2007.

[7] P. L. Montgomery, "Five, Six, and Seven-Term Karatsuba-Like Formulae", IEEE Transactions On Computers Dergisi, Cilt 54, Numara:3, 2005, syf. 362-369.

[8] C. Paar ve A. Weimerskirch, "Generalizations of the Karatsuba Algorithm for Efficient Implementations", Ruhr-Universty Bochum, Almanya, 2006, http://eprint.iacr.org/2006/224.pdf (Son erişim tarihi: 15 Mart 2017).

[9] K. Jankoqski, P. Laurent ve A. O'Mahony, Intel Polynomial Multiplication Instruction and its Usage for Elliptic Curve Cryptography, Intel White Paper, 2012, http://www.intel.co.kr/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf (Son erişim tarihi: 15 Mart 2017).

Kriptolojide Verimli Büyük Tam Sayı Çarpımı

Efficient Big Integer Multiplication in Cryptography

Murat Burhan İlter
Institute of Applied Mathematics
Middle East Technical University
Ankara, Turkey
Email: milter@metu.edu.tr

Murat Cenk
Institute of Applied Mathematics
Middle East Technical University
Ankara, Turkey
Email: mcenk@metu.edu.tr

***Abstract*—Most of the public key cryptography algorithms require efficient big integer multiplications. In this paper, we show how to develop efficient integer multiplication algorithms for cryptographic applications by combining different methods. Moreover, we determine the complexities by taking into account the cost of single word multiplication, single word addition and double word addition on different platforms.**

***Index Terms*—Integer multiplication, Karatsuba algorithm, Karatsuba-like algorithms, Public Key Cryptography**

***Özet*—Açık anahtarlı kriptosistemlerin bir çoğunda verimli tam sayı çarpımı kullanılmaktadır. Bu makalede, farklı metotların kombinasyonunu kullanarak, kriptografik uygulamalar için verimli tam sayı çarpma algoritmaları geliştirilmiştir. Ek olarak farklı platformlar için, tek kelime çarpımı, tek kelime toplamı, ve çift kelime toplamı dikkate alınarak karmaşıklık hesabı yapılmıştır.**

***Anahtar Kelimeler*—Tam sayı çarpımı, Karatsuba algoritması, Karatsuba-benzeri algoritmalar, Açık Anahtarlı Kriptosistemler**

I. Introduction

Before 1960, the naive multiplication algorithm or the schoolbook method which has complexity $O(n^2)$ had been used to multiply polynomials. In 1962, Karatsuba discovered a new way to multiply polynomials which is called as Karatsuba method [2]. The complexity of Karatsuba algorithm is $O(n^{1.58})$. Following this method, Toom-Cook algorithm where the complexity is $O(n^{1.46})$ was suggested [5], [6]. With these improvements, a variety of scientific analysis has been done in the literature. The following table displays a brief history of studies done regarding on this subject [7].

Table I
Historical overview of integer multiplication algorithms

Date	Algorithm	Time Complexity
$<$ 3000 BC	Schoolbook	$O(n^2)$
1962	Karatsuba	$O(n^{\log_2 3})$
1963	Toom	$O(n2^{5\sqrt{\log_2 n}})$
1966	Schöngage	$O(n2^{\sqrt{2\log_2 n}}(logn)^{\frac{3}{2}})$
1969	Knuth	$O(n2^{\sqrt{2\log_2 n}}(logn)$
1971	Schönage-Strassen	$O(nlognloglogn)$
2007	Fürer	$O(nlogn2^{O(log^* n)})$
2014	Harvey	$O(nlogn8^{log^* n})$

It should be noted that the cost of integer multiplication is reduced; however, these algorithms may not lead to the best results in order to multiply integers for cryptographic applications because of the hidden coefficients in the big$-O$ notation.

In this paper, the main concern is to analyze efficient integer multiplication algorithms to speed-up public key cryptography. The schoolbook and the Karatsuba-like algorithms are analyzed and efficient algorithms are derived by combining these methods. Similar techniques were used in [3] and [1], and the best known complexities were obtained for the polynomial multiplications over the binary field. In this paper, we obtain promising results for the integer multiplications used in cryptographic applications by using the similar methods in [3] and [1]. We first present the well known methods and their optimizations for the polynomial multiplications over the ring of integers, and then we search the best possible selection of algorithms that results in efficient complexities.

The work is structured as follows. Preliminaries on complexity calculation are given in Section 2. We indicate complexity analysis of 2-way and 3-way polynomial multiplication algorithms in Section 3 and Section 4. The combination of these methods is introduced in Section 5. We conclude the paper with Section 6.

II. Preliminaries

In this section, the relation between integer multiplication and polynomial multiplication is given. Throughout the paper, we assume that all polynomials are defined over $\mathbb{Z}$.

A positive integer A can be represented as a polynomial in the following way:

$$A = a_{n-1}\beta^{n-1} + \cdots a_1\beta + a_0$$

where β is an internal base, A is of length n, and a_i's are digits where $0 \leq a_i \leq \beta - 1$.

A polynomial multiplication is analyzed by counting the single and double precision/word addition and the single word multiplication. In this case, we will equally separate polynomials that we want to multiply. In other words, for a polynomial of size n, when we use 2-way multiplication method we have two polynomials of size $\frac{n}{2}$ where n is an even number. If n is an odd number, we can apply padding with dummy coefficient in order to use 2-way multiplication methods.

In order to compute the complexities of multiplication algorithms given as recursive equation, we use the following lemma.

Lemma 2.1: Let a, b, and i be positive integers. Let $n = b^i$, $a \neq b$, and $a \neq 1$. The recursive equation:

$$\begin{aligned} r_1 &= e, \\ r_n &= ar_{n/b} + cn + d, \end{aligned}$$

has the solution

$$r_n = \Big(e + \tfrac{bc}{a-b} + \tfrac{d}{a-1}\Big)n^{log_b(a)} - \Big(\tfrac{bc}{a-b}\Big)n - \tfrac{d}{a-1}.$$

In the complexity calculation A_D and A_S stand for double precision/word addition and single precision/word addition, respectively. In addition, the following notations will be used.

$M(n)$	*The total number of operations required for multiplying degree $n-1$ polynomials.*
$M_{\otimes}(n)$	*The total number of single word multiplications required for multiplying degree $n-1$ polynomials.*
$M_{\oplus_D}(n)$	*The total number of double word additions required for multiplying degree $n-1$ polynomials.*
$M_{\oplus_S}(n)$	*The total number of single word additions required for multiplying degree $n-1$ polynomials.*

Moreover, single word multiplication is denoted by M. Result of the multiplication of two single words is stored in a double word. In 2-way and 3-way multiplication algorithms, we use this procedure to achieve indicated complexities.

III. 2-way Multiplication Algorithms

In this section, 2-way multiplication method is analyzed. In 2-way multiplication algorithms, polynomials are divided into two equal parts. Let $A(x)$ and $B(x)$ be two polynomials of degree $n-1$ such that

$$\begin{aligned} A(x) &= a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}, \\ B(x) &= b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}, \end{aligned}$$

where n is a positive integer.

In 2-way multiplication algorithms, we recursively deploy the following steps: $A(x)$ and $B(x)$ are divided into two equal parts. $A(x) = A_0 + A_1y$ where

$$\begin{aligned} A_0 &= a_0 + a_1x + \cdots + a_{\frac{n}{2}-1}x^{\frac{n}{2}-1}, \\ A_1 &= a_{\frac{n}{2}} + a_{\frac{n}{2}+1}x + \cdots + a_{n-1}x^{\frac{n}{2}-1}. \end{aligned} \tag{1}$$

and $y = x^{\frac{n}{2}}$. Similarly, $B(x) = B_0 + B_1y$ where

$$\begin{aligned} B_0 &= b_0 + b_1x + \cdots + b_{\frac{n}{2}-1}x^{\frac{n}{2}-1}, \\ B_1 &= b_{\frac{n}{2}} + b_{\frac{n}{2}+1}x + \cdots + b_{n-1}x^{\frac{n}{2}-1}. \end{aligned} \tag{2}$$

Then, $(A_0 + A_1y)(B_0 + B_1y)$ is computed. The efficient algorithms for computing this product are the schoolbook algorithm, the Karatsuba 2-way algorithm, the refined Karatsuba 2-way algorithm and the optimized Karatsuba 2-way algorithm.

A. The schoolbook algorithm

The schoolbook algorithm is also known as the naive algorithm in the literature. By using (1) and (2) the multiplication of $A(x)$ and $B(x)$ with the schoolbook method can be performed as:

$$A(x)B(x) = A_0B_0 + y[A_1B_0 + A_0B_1] + y^2A_1B_1.$$

The number of single word multiplications and double word additions should be counted to obtain the cost of schoolbook algorithm. Note that there are four multiplications of polynomials of size $\frac{n}{2}$, A_0B_0, A_1B_0, A_0B_1, and A_1B_1.

Note that A_1B_0 is added to A_0B_1 which requires $(n-1)$ double word additions. In the computation of construction, there exist two overlaps between A_0B_0 and $(A_1B_0 + A_0B_1)$, and $(A_1B_0 + A_0B_1)$ and A_1B_1. Note that the half of A_0B_0 is added to the half of $(A_1B_0 + A_0B_1)$and this requires $\frac{n}{2} - 1$ double word additions. Similarly, this situation is also valid for $(A_1B_0 + A_0B_1)$ and A_1B_1. Therefore, we have totally $2(\frac{n}{2}-1)+n-1 = (2n-3)A_D$ additions. We can separate the total complexity into multiplication, and double word addition.

$$\begin{aligned} M(n) &= 4M(\tfrac{n}{2}) + (2n-3)A_D, M(1) = 1 \\ M_{\otimes}(n) &= 4M(\tfrac{n}{2}), M_{\otimes}(1) = 1, \\ M_{\oplus_D}(n) &= 4M(\tfrac{n}{2}) + (2n-3), M_{\oplus_D}(1) = 0. \end{aligned}$$

By Lemma 2.1, we can compute complexities explicitly as:

$$\begin{aligned} M(n) &= 2n^2 - 2n + 1, \\ M_{\otimes}(n) &= n^2, \\ M_{\oplus_D}(n) &= n^2 - 2n + 1. \end{aligned}$$

B. The Karatsuba 2-way algorithm

In the Karatsuba 2-way method [2], polynomials are divided into two parts as in (1) and (2). This method is applied as:

$$\begin{aligned} A(x)B(x) = \; & A_0B_0 + y[(A_0 + A_1)(B_0 + B_1) \\ & -A_0B_0 - A_1B_1] + y^2A_1B_1. \end{aligned} \tag{3}$$

One can compute the complexities as in the case of the schoolbook algorithm, and the following complexities are obtained.

$$\begin{aligned} M(n) &= 3M(\tfrac{n}{2}) + (3n-4)A_D + (n)A_S, M(1) = 1, \\ M_{\otimes}(n) &= 3M(\tfrac{n}{2}), M_{\otimes}(1) = 1, \\ M_{\oplus_D}(n) &= 3M(\tfrac{n}{2}) + (3n-4), M_{\oplus_D}(1) = 0, \\ M_{\oplus_S}(n) &= 3M(\tfrac{n}{2}) + n, M_{\oplus_S}(1) = 0. \end{aligned}$$

By using Lemma 2.1, we can compute complexities explicitly as:

$$\begin{aligned} M(n) &= 7n^{1.58} - 8n + 2, \\ M_{\otimes}(n) &= n^{1.58}, \\ M_{\oplus_D}(n) &= 4n^{1.58} - 6n + 2, \\ M_{\oplus_S}(n) &= 2n^{1.58} - 2n. \end{aligned}$$

C. The refined Karatsuba 2-way algorithm

In the refined Karatsuba 2-way method [3], we first define P_1, P_2, and P_3 as in (4).

$$\begin{aligned} P_1 &= A_0B_0, \\ P_2 &= (A_0 + A_1)(B_0 + B_1), \\ P_3 &= A_1B_1. \end{aligned} \tag{4}$$

To use this method, we divide our polynomials into two parts as in (1) and (2). We can express the multiplication as:

$$A(x)B(x) = (y-1)(yP_3 - P_1) + yP_2$$

It can be shown that the refined Karatsuba 2-way algorithm has the following complexities.

$$\begin{aligned}
M(n) &= 3M(\tfrac{n}{2}) + (\tfrac{5n}{2} - 3)A_D + (n)A_S, M(1) = 1,\\
M_{\otimes}(n) &= 3M(\tfrac{n}{2}), M_{\otimes}(1) = 1,\\
M_{\oplus D}(n) &= 3M(\tfrac{n}{2}) + (\tfrac{5n}{2} - 3), M_{\oplus D}(1) = 0,\\
M_{\oplus S}(n) &= 3M(\tfrac{n}{2}) + n, M_{\oplus S}(1) = 0.
\end{aligned}$$

By the means of Lemma 2.1, we can compute the complexities as follows:

$$\begin{aligned}
M(n) &= 6.5n^{1.58} - 7n + \tfrac{3}{2},\\
M_{\otimes}(n) &= n^{1.58},\\
M_{\oplus D}(n) &= 3.5n^{1.58} - 5n + \tfrac{3}{2},\\
M_{\oplus S}(n) &= 2n^{1.58} - 2n.
\end{aligned}$$

D. The optimized Karatsuba 2-way algorithm

In the optimized Karatsuba 2-way algorithm [4], we divide the products in (4) into two parts. P_{iL} is the lower part of P_i with $(\frac{n}{2})$ terms where $i = 1, 2, 3$. P_{iH} is the higher part of P_i, for $i = 1, 2, 3$ with $(\frac{n}{2} - 1)$ terms. Substituting these into (3), we can apply the method as follows:

$$\begin{aligned}
A(x)B(x) &= P_{1L} + x^{\frac{n}{2}}[P_{1H} + P_{2L} - P_{1L} - P_{3L}]\\
&\quad + x^n[P_{2H} - P_{1H} - P_{3H} + P_{3L}]\\
&\quad + x^{\frac{3n}{2}}P_{3H}\\
&= P_{1L} + x^{\frac{n}{2}}[(P_{1H} - P_{3L}) + P_{2L} - P_{1L}]\\
&\quad + x^n[-(P_{1H} - P_{3L}) + P_{2H} - P_{3H}]\\
&\quad + x^{\frac{3n}{2}}P_{3H}
\end{aligned}$$

For the optimized Karatsuba 2-way algorithm, the complexities are:

$$\begin{aligned}
M(n) &= 3M(\tfrac{n}{2}) + (\tfrac{5n}{2} - 3)A_D + (n)A_S, M(1) = 1,\\
M_{\otimes}(n) &= 3M(\tfrac{n}{2}), M_{\otimes}(1) = 1,\\
M_{\oplus D}(n) &= 3M(\tfrac{n}{2}) + (\tfrac{5n}{2} - 3), M_{\oplus D}(1) = 0,\\
M_{\oplus S}(n) &= 3M(\tfrac{n}{2}) + n, M_{\oplus S}(1) = 0.
\end{aligned}$$

With the use of Lemma 2.1, we can compute complexities as follows:

$$\begin{aligned}
M(n) &= 6.5n^{1.58} - 7n + \tfrac{3}{2},\\
M_{\otimes}(n) &= n^{1.58},\\
M_{\oplus D}(n) &= 3.5n^{1.58} - 5n + \tfrac{3}{2},\\
M_{\oplus S}(n) &= 2n^{1.58} - 2n.
\end{aligned}$$

IV. 3-way Multiplication Algorithms

In this section, 3-way multiplication algorithms are discussed. There are basically three 3-way multiplication algorithms, namely the schoolbook, the Karatsuba-like algorithm and the optimized Karatsuba-like algorithm. We can calculate $A(x)B(x)$ by using a 3-way algorithm. First, the polynomials $A(x)$ and $B(x)$ are divided into three parts as $A(x) = A_0 + A_1 y + A_2 y^2$ where

$$\begin{aligned}
A_0 &= a_0 + a_1 x + \cdots + a_{\frac{n}{3}-1}x^{\frac{n}{3}-1},\\
A_1 &= a_{\frac{n}{3}} + a_{\frac{n}{3}+1}x + \cdots + a_{\frac{2n}{3}-1}x^{\frac{n}{3}-1},\\
A_2 &= a_{\frac{2n}{3}} + a_{\frac{2n}{3}+1}x + \cdots + a_{n-1}x^{\frac{n}{3}-1},
\end{aligned} \tag{5}$$

and $y = x^{\frac{n}{3}}$. Similarly, $B(x) = B_0 + B_1 y + B_2 y^2$ where

$$\begin{aligned}
B_0 &= b_0 + b_1 x + \cdots + b_{\frac{n}{3}-1}x^{\frac{n}{3}-1},\\
B_1 &= b_{\frac{n}{3}} + b_{\frac{n}{3}+1}x + \cdots + b_{\frac{2n}{3}-1}x^{\frac{n}{3}-1},\\
B_2 &= b_{\frac{2n}{3}} + b_{\frac{2n}{3}+1}x + \cdots + b_{n-1}x^{\frac{n}{3}-1}.
\end{aligned} \tag{6}$$

Then $(A_0 + A_1 y + A_2 y^2)(B_0 + B_1 y + B_2 y^2)$ is calculated.

A. The schoolbook algorithm

In the schoolbook algorithm, we use (5) and (6), and calculate the multiplication of polynomials $A(x)$ and $B(x)$ as follows:

$$\begin{aligned}
A(x)B(x) &= A_0B_0 + y[A_1B_0 + A_0B_1]\\
&\quad + y^2(A_0B_2 + A_1B_1 + A_2B_0)\\
&\quad + y^3(A_1B_2 + A_2B_1) + y^4A_2B_2.
\end{aligned}$$

The complexity of schoolbook algorithm is:

$$\begin{aligned}
M(n) &= 9M(\tfrac{n}{3}) + (4n - 8)A_D, M(1) = 1,\\
M_{\otimes}(n) &= 9M(\tfrac{n}{3}), M_{\otimes}(1) = 1,\\
M_{\oplus D}(n) &= 9M(\tfrac{n}{3}) + 4n - 8, M_{\oplus D}(1) = 0.
\end{aligned}$$

By using Lemma 2.1, we can compute complexities explicitly:

$$\begin{aligned}
M(n) &= 2n^2 - 2n + 1\\
M_{\otimes}(n) &= n^2,\\
M_{\oplus D}(n) &= n^2 - 2n + 1.
\end{aligned}$$

B. The Karatsuba-like 3-way algorithm

In Karatsuba-like 3-way algorithm [8], we can use (5) and (6) and compute the multiplication of polynomials $A(x)$ and $B(x)$ as follows:

$$\begin{aligned}
A(x)B(x) = {} & A_0B_0 + y[(A_0 + A_1)(B_0 + B_1) - A_0B_0\\
& - A_1B_1] + y^2[(A_0 + A_2)(B_0 + B_2) - A_0B_0\\
& - A_2B_2 + A_1B_1] + y^3[(A_1 + A_2)(B_1 + B_2)\\
& - A_1B_1 - A_2B_2] + y^4A_2B_2
\end{aligned}$$

The complexity of Karatsuba-like 3-way algorithm is:

$$\begin{aligned}
M(n) &= 6M(\tfrac{n}{3}) + (6n - 11)A_D + (2n)A_S, M(1) = 1,\\
M_{\otimes}(n) &= 6M(\tfrac{n}{3}), M_{\otimes}(1) = 1,\\
M_{\oplus D}(n) &= 6M(\tfrac{n}{3}) + 6n - 11, M_{\oplus D}(1) = 0,\\
M_{\oplus S}(n) &= 6M(\tfrac{n}{3}) + 2n, M_{\oplus S}(1) = 0.
\end{aligned}$$

By applying Lemma 2.1, we can compute complexities explicitly as:

$$\begin{aligned}
M(n) &= 6.8n^{1.63} - 8n + 2.2\\
M_{\otimes}(n) &= n^{1.63},\\
M_{\oplus D}(n) &= 3.8n^{1.63} - 6n + 2.2,\\
M_{\oplus S}(n) &= 2n^{1.63} - 2n.
\end{aligned}$$

C. The optimized Karatsuba-like 3-way algorithm

In the optimized Karatsuba-like 3-way method, we use (5) and (6), and calculate the multiplication of polynomials. The case over binary fields is in [9]. In order to get the compact formula we define:

$$\begin{aligned}
P_1 &= A_0B_0,\\
P_2 &= (A_0 + A_1)(B_0 + B_1),\\
P_3 &= A_1B_1,\\
P_4 &= (A_0 + A_2)(B_0 + B_2),\\
P_5 &= A_2B_2,\\
P_6 &= (A_1 + A_2)(B_1 + B_2).
\end{aligned}$$

Table II
COMPLEXITY COMPARISON OF 2-WAY AND 3-WAY MULTIPLICATION ALGORITHMS

Algorithm	$M_{\oplus S}(n)$	$M_{\oplus D}(n)$	$M_{\otimes}(n)$	$M(n)$
SB		n^2-2n+1	n^2	$2n^2-2n+1$
KA2	$2n^{1.58}-2n$	$4n^{1.58}-6n+2$	$n^{1.58}$	$7n^{1.58}-8n+2$
RK2	$2n^{1.58}-2n$	$3.5n^{1.58}-5n+1.5$	$n^{1.58}$	$6.5n^{1.58}-7n+1.5$
OPK2	$2n^{1.58}-2n$	$3.5n^{1.58}-5n+1.5$	$n^{1.58}$	$6.5n^{1.58}-7n+1.5$
SB		n^2-2n+1	n^2	$2n^2-2n+1$
KA3	$2n^{1.63}-2n$	$3.8n^{1.63}-6n+2.2$	$n^{1.63}$	$6.8n^{1.63}-8n+2.2$
OPK3	$2n^{1.63}-2n$	$\frac{53}{15}n^{1.63}-\frac{16}{3}n+\frac{9}{5}$	$n^{1.63}$	$\frac{98}{15}n^{1.63}-\frac{22}{3}n+\frac{9}{5}$

P_{iL} is the lower part of P_i with $(\frac{n}{3})$ terms where $i = 1, \cdots, 6$. P_{iH} is the higher part of P_i, for $i = 1, \cdots, 6$ with $(\frac{n}{3}-1)$ terms. Then, the multiplication of $A(x)B(x)$ is expressed as follows:

$$\begin{aligned} A(x)B(x) &= P_{1L} + y[P_{1H} + P_{2L} - P_{1L} - P_{3L}] \\ &\quad + y^2[P_{2H} - P_{1H} - P_{3H} + P_{4L} - P_{1L} \\ &\quad - P_{5L} + P_{3L}] + y^3[P_{4H} - P_{1H} - P_{5H} \\ &\quad + P_{3H} + P_{6L} - P_{3L} - P_{5L}] + y^4[P_{6H} \\ &\quad - P_{3H} - P_{5H} + P_{5L}] + y^5 P_{5H} \\ &= P_{1L} + y(P_{1H} - P_{3L}) + P_{2L} - P_{1L}] \\ &\quad + y^2[-(P_{1H} - P_{3L}) - P_{3H} + P_{2H} + P_{4L} \\ &\quad - P_{1L} + P_{5L}] + y^3[(P_{3H} - P_{5L}) + P_{4H} \\ &\quad - P_{1H} - P_{5H} + P_{6L} - P_{3L}] + y^4[-(P_{3H} \\ &\quad - P_{5L}) + P_{6H} - P_{5H}] + y^5 P_{5H} \end{aligned}$$

The complexity of the optimized Karatsuba-like 3-way algorithm is:

$$\begin{aligned} M(n) &= 6M(\tfrac{n}{3}) + (\tfrac{16}{3}n - 9)A_D + (2n)A_S, M(1) = 1, \\ M_{\otimes}(n) &= 6M(\tfrac{n}{3}), M_{\otimes}(1) = 1, \\ M_{\oplus D}(n) &= 6M(\tfrac{n}{3}) + (\tfrac{16}{3}n - 9), M_{\oplus D}(1) = 0, \\ M_{\oplus S}(n) &= 6M(\tfrac{n}{3}) + 2n, M_{\oplus S}(1) = 0. \end{aligned}$$

By Lemma 2.1, we can compute complexities as follows:

$$\begin{aligned} M(n) &= \tfrac{98}{15}n^{1.63} - \tfrac{22}{3}n + \tfrac{9}{5}, \\ M_{\otimes}(n) &= n^{1.63}, \\ M_{\oplus D}(n) &= \tfrac{53}{15}n^{1.63} - \tfrac{16}{3}n + \tfrac{9}{5}, \\ M_{\oplus S}(n) &= 2n^{1.63} - 2n. \end{aligned}$$

D. Complexity comparison of 2-way and 3-way multiplication algorithms

In this section, we provide complexity results that were calculated in Section III and Section IV.

In 2-way multiplication algorithms, the refined Karatsuba 2-way and the optimized Karatsuba 2-way algorithms lead to the best complexity. In 3-way multiplication algorithms, the optimized Karatsuba-like 3-way algorithm is the best algorithm. The asymptotic complexities are tabulated in Table II. Note that these asymptotic complexities are useful when the input size is very huge. For cryptographic sizes, combination of different algorithms is more efficient than the use of a single algorithm. In next section, we discuss this approach.

V. COMBINED METHODS

It can be observed that the complexity of Karatsuba-like algorithms has better complexities than the schoolbook method. However; in some cases, using combined methods, applying the refined Karatsuba or the optimized Karatsuba algorithm before the schoolbook method yields more desirable results. First, the best complexity for $n = 2$ is searched. Then, we search for $n = 3$ by using the previous results. We continue similarly and when we come to $n = l$, we check all possible cases by using the previous complexities. Since we have limited number of algorithms, this search ends quickly. The following examples use this approach.

Example 5.1: Assume that we have a platform where a single and a double word addition and a single word multiplication have the same complexity. In this platform, we want to multiply two polynomials of degree 5. If we use the schoolbook method, we need 36 word multiplications and 25 double word additions. Therefore, this operation results in 61 operations. However, using the refined Karatsuba 2-way algorithm first, then the schoolbook algorithm, we have

$$\begin{aligned} M(6) &= 3M(3) + (\tfrac{5\cdot 6}{2} - 3)A_D + (6)A_S \\ &= 3(9M + 4A_D) + 12A_D + 6A_S \\ &= 27M + 24A_D + 6A_S, \end{aligned}$$

and since we assume M, A_D, and A_S have equal costs, the complexity reduces to 57.

Example 5.2: Assume that we have same platform as in the Example 5.1, and we want to multiply two polynomials of degree 11. If we use the schoolbook method, we need 144 word multiplications and 121 double word additions, so this operation comes out 265 operations. On the other hand, using the refined Karatsuba 2-way algorithm first, then the best algorithm for multiplying degree 5 polynomials which is denoted by $M(6)$ from Example 5.1, we obtain

$$\begin{aligned} M(12) &= 3M(6) + (\tfrac{5\cdot 12}{2} - 3)A_D + (12)A_S \\ &= 3(27M + 24A_D + 6A_S) + 27A_D + 12A_S \\ &= 81M + 99A_D + 30A_S, \end{aligned}$$

and therefore by the same assumption the complexity is 210 operations.

As it can be seen from Example 5.1 and 5.2, computation of the minimum number of operations can be computed with a hybrid method where one single word addition, one double word addition, and one single word multiplication have the same cost. The list of this operations for multiplying two

polynomials up to size 20 is given in Table III where SB is used for the schoolbook algorithm, and RK2 is used for the refined Karatsuba 2-way algorithm. The last column in Table III shows the name of the algorithm used to obtain the indicated complexities. If there are two algorithm names, it means that first apply the leftmost algorithm following apply the rightmost one. On the condition that having two algorithm names, and the last term in these ones, we again first apply the leftmost algorithm, and then we use naive multiplication method for degree one polynomial term by term.

Table III
MINIMUM NUMBER OF OPERATIONS 1 SINGLE WORD ADDITION=1 WORD DOUBLE ADDITION = 1 WORD MULTIPLICATION

n	Mult.	A_S	A_D	Tot. Operation	Algorithm
1	1			1	SB
2	4		1	5	SB
3	9		4	13	SB
4	16		9	25	SB
5	25		16	41	SB
6	27	6	24	57	RK2, M(3)
7	40	6	35	81	M(6), last term
8	48	8	44	100	RK2, M(4)
9	65	8	59	132	M(8), last term
10	75	10	70	155	RK2, M(5)
11	96	10	89	195	M(10), last term
12	81	30	99	210	RK2,M(6)
13	106	30	122	258	M(12), last term
14	120	32	137	289	RK2, M(7)
15	149	32	164	345	M(14), last term
16	144	40	169	353	RK2, M(8)
17	177	40	200	417	M(16), last term
18	195	42	219	456	RK2, M(9)
19	232	42	254	528	M(18), last term
20	225	50	257	532	RK2, M(10)

Example 5.3: Suppose that in a given platform, we have one single word addition and one single word multiplication having the same cost; however, one double word addition is twice as costly as one single word addition and one single word multiplication. We want to multiply two polynomials of degree 11. If we use schoolbook method, then we get 144 single word multiplication and 121 double word additions where the total complexity is 386 operations. As a second option, by using the optimized Karatsuba-like 3-way algorithm first, then the best way to multiply degree 4 polynomials in this platform, we get

$$\begin{aligned} M(15) &= 6M(5) + (\tfrac{16\cdot 15}{3} - 9)A_D + (30)A_S \\ &= 6(25M + 16A_D) + 71A_D + 30A_S \\ &= 150M + 167A_D + 30A_S, \end{aligned}$$

which costs 514 operations. Finally if we use best way to multiply degree 13 polynomials first, then term by term multiplication we have

$$\begin{aligned} M(15) &= M(14) + (29)M + (27)A_D \\ &= (120 + 29)M + (137 + 27)A_D + (32)A_S \\ &= 149M + 164A_D + 32A_S. \end{aligned}$$

Under our assumption, it corresponds to 509 operations.

In Table IV, the best algorithms for this platform are presented. It should be noted that the choice of the best algorithm for multiplication might change for different platforms. On the other hand, as it can be seen from Tables III and IV, even though the operation costs are different, the best multiplication algorithms can be the same.

Table IV
MINIMUM NUMBER OF OPERATIONS 1 WORD SINGLE ADDITION=2 WORD DOUBLE ADDITION = 1 WORD MULTIPLICATION

n	Mult.	A_S	A_D	Tot. Operation	Algorithm
1	1			1	SB
2	4		1	6	SB
3	9		4	17	SB
4	16		9	34	SB
5	25		16	57	SB
6	27	6	24	81	RK2, M(3)
7	40	6	35	116	M(6), last term
8	48	8	44	144	RK2, M(4)
9	65	8	59	191	M(8), last term
10	75	10	70	225	RK2, M(5)
11	96	10	89	284	M(10), last term
12	81	30	99	309	RK2, M(6)
13	106	30	122	380	M(12), last term
14	120	32	137	426	RK2, M(7)
15	149	32	164	509	M(14), last term
16	144	40	169	522	RK2, M(8)
17	177	40	200	617	M(16), last term
18	195	42	219	655	RK2, M(9)
19	232	42	254	782	M(18), last term
20	225	50	257	789	RK2, M(10)

VI. CONCLUSION

In this paper, we show how to develop efficient algorithms in polynomial multiplication over the ring of integers used in cryptographic applications by searching the best possible multiplication algorithm in each recursion level. These algorithms are analyzed according to their arithmetic complexities. It is revealed that the selection of the multiplication algorithms varies on each different platform since the cost calculation depends on the implementation platform.

ACKNOWLEDGMENT

This work is supported in part by TÜBİTAK under grant number 115R289.

REFERENCES

[1] Cenk, M., & Hasan, M. A. (2015). Some new results on binary polynomial multiplication. Journal of Cryptographic Engineering, 5(4), 289-303. 1345-1361.

[2] Karatsuba, A. (1963). Multiplication of multidigit numbers on automata. In Sov. Phys. Dokl. (Vol. 7, No. 7, pp. 595-596).

[3] Bernstein, D. (2009). Batch binary Edwards. In: Advances in Cryptology CRYPTO 2009, LNCS, (vol. 5677, pp. 317336).

[4] Zhou, G., & Michalik, H. (2010). Comments on" A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Field". IEEE Transactions on Computers, 59(7), 1007-1008.

[5] Toom, A. L. (1963). The complexity of a scheme of functional elements realizing the multiplication of integers. In Soviet Mathematics Doklady (Vol. 3, No. 4, pp. 714-716).

[6] Cook, S. A., & Aanderaa, S. O. (1969). On the minimum computation time of functions. Transactions of the American Mathematical Society, 142, 291-314.

[7] Harvey, D., Van Der Hoeven, J., & Lecerf, G. (2016). Even faster integer multiplication. Journal of Complexity, 36, 1-30.

[8] Weimerskirch, A., & Paar, C. (2006). Generalizations of the Karatsuba Algorithm for Efficient Implementations. IACR Cryptology ePrint Archive, 2006, 224.

[9] Cenk, M., Hasan, M. A., & Negre, C. (2014). Efficient subquadratic space complexity binary polynomial multipliers based on block recombination. IEEE Transactions on Computers, 63(9), 2273-2287.

Quantum Group Proxy Digital Signature based on Quantum Fourier Transform by Using Blinded and Non Blinded Trent

Ihsan YILMAZ
Canakkale Onsekiz Mart University,
Computer Engineering Department
Email: iyilmaz@comu.edu.tr

***Abstract*—In this study, quantum proxy group signature protocol based on the Quantum Fourier Transformation(QFT) is suggested. In this protocol, QFT is used to share signature with group members. So all proxy group members know only their part of the signature information which are encrypted output of the QFT. This improves the security of the protocol. In addition, the security of the quantum proxy group signature is provided by using reorder QFT output qubits with permutation of the Trent,blinded and nonblinded . The security analysis expresses higher efficiency, effective secret key usage and security of the proposed protocol.**

I. Introduction

Classical cryptography techniques use some assumptions about mathematically hard problems to obtain security and create some communication protocols. However, these hard problems can be easily solved with the quantum computer and quantum algorithms [1], [2], [3].

The aspects of the quantum mechanics were adopted to improve the security of the cryptography. So, quantum cryptography research area has been developing. Especially, secure communication based on quantum cryptography is extremely important in quantum cryptography.

Quantum key distribution(QKD) has been developed instead of the classical version [4]. Ekert [5] also designed QKD based on the Bell's theorem. Gao [6] proposed quantum key distribution protocol based on entanglement swapping. Mayers [7] described unconditional security of the QKD.

Quantum Secret Sharing(QSS) is another concept and it is used to share data between participants in securely way. Cleve et. al. [8] defined (k, n) threshold scheme to share a quantum secret. Hillery et al. [9] defined a quantum sharing mechanism based on GHZ-states. Chen et. al [10] presented a three-party quantum secret-sharing by using GHZ-states. Huang et. al. [11] used Quantum Fourier Transform(QFT) to share secret.

Besides these developments, quantum cryptography techniques are also applied in the digital signatures. Gottesman and Chuang [12] were firstly presented quantum digital signature protocol. Buhrman et. al. [13] defined quantum finger prints to compare string which is very useful in the quantum digital signatures. Zeng and Keitel [14] suggested an arbitrated quantum signature scheme which uses symmetrical quantum keys, GHZ-states and quantum one-time pads [15]. Lee et. al. [16] also proposed an arbitrated quantum digital signature scheme with message recovery. Li et. al. [17] proposed Bell-states version of the protocol of Zeng and Keitel [18].

Chaum [19] has firstly defined the concept of the group signatures. In these signatures, some members of the group can sign the messages. Membership authentication schemes such as E-payment systems [20] can be generalized as group signatures.

Yang [21], [22] proposed threshold proxy group signature scheme. Shi et al.[23] analyzed Yang and Wen's quantum proxy group signature [24] and proposed some methods to improve the security of the protocol.

Wen et. al. [25] presented a group signature protocol based on the quantum teleportation. Then Wen [26] also defined a e-payment system which uses proposed group signature scheme [27].

Shi et. al. [26] proposed multi-party quantum proxy group signature based on QFT transform. The group members cooperate to sign the message with QFT with authorization of the owner. These group members use QFT^{-1} to restore the message with authorization of the receiver. All participants use quantum circuits to perform all operations.

In this study, quantum proxy group signature protocol based on the QFT is suggested. In this protocol, QFT is used to share signature with group members. The paper can be outlined as follows; in Sect.II,basic concepts of QFT are explained; In Sect.III, base stages of the protocol are introduced. In Sect.IV, the blinded version of the group signature protocol is defined. In Sect.V, the security analysis of the protocol based on forgery and disavowal concepts are given. In the conclusion, some results are discussed.

II. Quantum Fourier Transform

Quantum Fourier transform is a quantum version of classical discrete Fourier transform [21]. The QFT transform of an orthonormal basis set $|0\rangle, |1\rangle, ..., |N-1\rangle$ can be defined as follows [21]:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle \tag{1}$$

If we define QFT of n qubits, then $N = 2^n$ and orthonormal basis set is $|0\rangle, |1\rangle, ..., |2^n - 1\rangle$. The $|x\rangle$ state can be written in binary form as $x = x_0 x_1 ... x_{N-1}$. The circuit of Quantum

Fourier Transform for x can be seen in Fig.1. The $|x\rangle$ state is transformed into the phase of qubits which are results of the QFT transform.

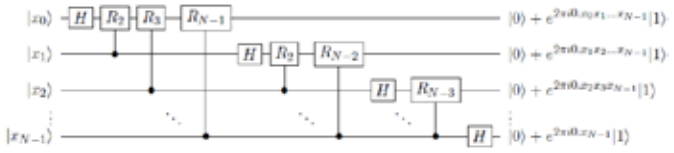


Fig. 1. Quantum Fourier Transform Circuit QFT

III. Group Signature Protocol with QFT

The participants of the protocol are Alice, Bob, Trent and proxy group members $\{G_1, G_2, ..., G_N\}$. Alice would like to send data $m = \{m_0 m_1 ... m_{N-1}\}$,$m_i \in \{0, 1\}$ with her signature of m to Bob. Alice can cooperate some group members $G_i \in \{G_1, G_2, ..., G_N\}$ to create her signature. Trent is assumed as a group manager of the protocol and he is trusted. Trent manages some communication to provide security of the protocol. Bob can obtained data m and verify the signature of the data with the help of these group members and Trent. The protocol can be described with following phases.

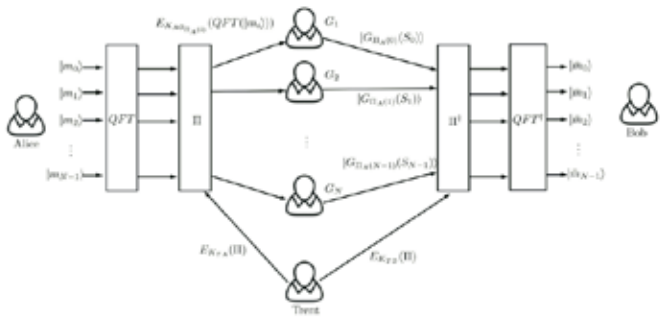


Fig. 2. Proxy Group Signature With QFT

A. Initialization Phase

1) Alice shares secret keys $K_{AG_i}, i = 1..N$ with group members G_i and K_{AB} with Bob. Bob shares secret keys $K_{G_iB}, i = 1..N$ with group members G_i. Also Trent shares secret key K_{TA} with Alice and secret key K_{TB} with Bob. Participant's secret keys $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ are obtained by using quantum key distribution(QKD) protocol [3]-[5]. Mayers [7] howed unconditionally security of the QKD protocol. The secret keys are used to encrypt quantum data to prevent any attackers.The encryption algorithm is given in Eq. 9. The length of the all keys are $|K| = 4N$. The method of using secret keys can be defined as follows.
   The length of the all data to be sent may be larger than N. In this case, the data can be divided into N length parts. Each part can send in different sessions. Every participant of the protocol uses 4-bits of the owned secret key to encrypt quantum data.
   a) $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ secret keys are only once created. Then the secret keys can be divided into 4-bit pieces. These different pieces of the secret keys can be used in encryption respectively for consecutive sessions by participants.
   b) Different $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ secret keys are created for every different sessions. Every created secret keys can be divided into 4-bit pieces. The piece corresponding to the session number can be used in encryption by participants.
2) Alice expresses her data m with quantum computational bases as $\{0 \to |0\rangle, 1 \to |1\rangle\}$. We assume that the length of the m is $|m| = N$.

$$|m\rangle = \otimes_{i=0}^{N-1} |m_i\rangle \tag{2}$$

   Where $|m_i\rangle \in \{|0\rangle, |1\rangle\}$.
3) Trent creates a permutation $\Pi : \{1, 2, ..., N\} \to \{1, 2, ..., N\}$ as follows:

$$\Pi = \begin{bmatrix} 1 & 2 & ... & N \\ \Pi(1) & \Pi(2) & ... & \Pi(N) \end{bmatrix} \tag{3}$$

   Trent creates encrypted versions of that permutation as follows:

$$\Pi S_A = E_{K_{TA}}(\Pi) \tag{4}$$
$$\Pi S_B = E_{K_{TB}}(\Pi) \tag{5}$$

   Then, Trent sends ΠS_A to Alice by using authenticated classical channel or quantum channel.
4) Alice decrypts ΠS_A and obtains Π_A.
5) Alice applies QFT to her data ($\otimes_{i=0}^{N-1} |m_i\rangle$) and obtains following state:

$$\begin{aligned} |m_0 m_1 m_2 ... m_{N-1}\rangle = \frac{1}{\sqrt{2^{N-1}}} \left(|0\rangle + e^{2\pi 0.m_{N-1}}|1\rangle\right) \otimes \\ \left(|0\rangle + e^{2\pi 0.m_{N-2}m_{N-1}}|1\rangle\right) \otimes \\ ... \otimes \left(|0\rangle + e^{2\pi 0.m_0 m_1 ... m_{N-1}}|1\rangle\right) \end{aligned} \tag{6}$$

$$|m_0 m_1 m_2 ... m_{N-1}\rangle = \frac{1}{\sqrt{2^{N-1}}} \otimes_{i=0}^{N-1} QFT(|m_i\rangle) \tag{7}$$

B. Signing Phase

1) Alice encrypts all qubits of Eq. 7 with secret keys which are shared with group members.

$$|A(S_i)\rangle = E_{K_{AG_{\Pi_A(i)}}}(QFT(|m_i\rangle)), i = 0..N-1 \tag{8}$$

   Here, $E_K(.)$ is a quantum one-time pad encryption algorithm which is firstly defined by Kim et al [26] and used by Zhang et al. [27] to improve security

of the protocol against forgery attacks. That quantum encryption algorithm can be defined as follows [27]:

$$E_K(|m\rangle) = \otimes_{i=0}^{N-1} {\sigma_x}^{K_{4i}} {\sigma_z}^{K_{4i-1}} T {\sigma_x}^{K_{4i-2}} {\sigma_z}^{K_{4i-3}} |m_i\rangle \quad (9)$$

$$T = \frac{i}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z) \quad (10)$$

Due to using T, encrypted message cannot be forged [24]. Where the key length is $|K| = 4n$.

2) Alice sends $|A(S_i)\rangle$ to proxy group member $G_{\Pi_A(i)}$ by using permutation of Trent.
3) Alice encrypts $|m\rangle$ with secret key $K_T A$ with above encryption algorithm and send to Trent via quantum channel.
$$|AT(S_i)\rangle = E_{K_{TA}}(|m_i\rangle) \quad (11)$$
4) Trent decrypts the $|AT(S_i)\rangle$ with secret key K_{TA} and obtains $\tilde{m}$. Trent saves $\tilde{m}$.
5) After receiving $|A(S_i)\rangle$, proxy group member $G_{\Pi_A(i)}$ decrypt $|A(S_i)\rangle$ and obtains $|QFT(m_i)\rangle$. But any proxy group member does not know the order of $|QFT(m_i)\rangle$. Then $G_{\Pi_A(i)}$ encrypt $|QFT(m_i)\rangle$ with secret $K_{G_{\Pi_A(i)}B}$.
$$\left|G_{\Pi_A(i)}(S_i)\right\rangle = E_{K_{G_{\Pi(i)}B}}(QFT(|m_i\rangle)) \quad (12)$$
6) $G_{\Pi_A(i)}$ sends $\left|G_{\Pi_A(i)}(S_i)\right\rangle$ to Bob.

C. Verification Phase

1) Bob decrypts all $\left|G_{\Pi_A(i)}(S_i)\right\rangle$ by using secret key $K_{G_{\Pi_A(i)}B}$ and obtains $QFT(|m_i\rangle)$.
2) Bob asks Trent for permutation and m of Alice.
3) Trent sends ΠS_B to Bob by using authenticated classical channel or quantum channel.
4) Bob decrypt the ΠS_B and obtains Π_B permutation.
5) Bob reorder $QFT(|m_i\rangle)$ states with permutation of Trent and then applies $QFT^{-}1$ and gets $|\bar{m}_0\bar{m}_1\bar{m}_2...\bar{m}_{N-1}\rangle$. Then makes computational basis measurement onto that states and obtains $\bar{m}$.
6) Trent encrypts $|\tilde{m}\rangle$ with secret key $K_T B$ with above encryption algorithm and send to Bob via authenticated quantum channel.
$$|TB(S_i)\rangle = E_{K_{TB}}(|\tilde{m}_i\rangle) \quad (13)$$
7) Bob decrypts the $|TB(S_i)\rangle$ with secret key K_{TB} and obtains $|\tilde{m}\rangle$. Bob measures $|\tilde{m}\rangle$ with computational basis and saves $\tilde{m}$.
8) Bob checks equality of $\tilde{m}$ and $\bar{m}$. If $\tilde{m} = \bar{m}$, Bob will announce that the signature is valid, otherwise the signature is rejected and the protocol aborted.
9) If the signature is valid, then the Trent stores the message m with Alice's and proxy group participants identifications for later traceability.

IV. Group Signature Protocol with QFT and Blinded Signature

In the first protocol, trusted participant Trent can see the message m in the step-3 of the signing phase. To blind the message the participants can forward following steps instead of the above protocol.

A. Signing Phase

The first two steps are the same as in the signing phase of Sect.III.

3) Alice encrypts $|m\rangle$ with secret key $K_A B$ with the encryption algorithm and send to Trent via quantum channel.
$$|AT(S_i)\rangle = E_{K_{AB}}(|m_i\rangle) \quad (14)$$
4) Trent encrypts the $|AT(S_i)\rangle$ with the secret key K_{TB}.
$$|TB(S_i)\rangle = E_{K_{TB}}(|AT(S_i)\rangle) \quad (15)$$
Then, Trent sends the above encrypted state to Bob via quantum channel.
5) Bob decrypts $|TB(S_i)\rangle$ with the secret key K_{BT} and gets $|AT(S_i)\rangle$. Then, Bob decrypts the states $|AT(S_i)\rangle$ and gets $|m_i\rangle$ states. Bob measures the $|m_i\rangle$ states with computational basis and saves the results as $\tilde{m}$.

The other steps are the same as in the signing phase of Sect.III.

B. Verification Phase

The first step is the same as in the verification phase of Sect.III.

2) Bob asks Trent for permutation.
3) Trent sends ΠS_B to Bob by using authenticated classical channel or quantum channel.
4) Bob decrypt the ΠS_B and obtains Π_B permutation.
5) Bob reorder $QFT(|m_i\rangle)$ states with permutation of Trent and then applies $QFT^{-}1$. So Bob gets $|\bar{m}_0\bar{m}_1\bar{m}_2...\bar{m}_{N-1}\rangle$. Then Bob makes computational basis measurement onto that states and obtains $\bar{m}$.
6) Bob checks equality of $\tilde{m}$ and $\bar{m}$. If $\tilde{m} = \bar{m}$, Bob will announce that the signature is valid, otherwise the signature is rejected and the protocol aborted.
7) If the message is valid, then Bob encrypt the valid message m with encryption algorithm.
$$|BT(S_i)\rangle = E_{K_{BT}}(|m_i\rangle) \quad (16)$$
Then Bob sends $|BT(S_i)\rangle$ to Trent.
8) Trent decrypts $|BT(S_i)\rangle$ with secret key K_{BT} and measures the states with computational basis and obtains $\bar{m}$.
9) Trent also asks Alice for sending m to him.
10) Alice encrypt the valid message m with encryption algorithm.
$$|AT(S_i)\rangle = E_{K_{AT}}(|m_i\rangle) \quad (17)$$
Then Alice sends $|AT(S_i)\rangle$ to Trent.
11) Trent decrypts $|AT(S_i)\rangle$ with secret key K_{AT} and measures the states with computational basis and obtains $\tilde{m}$.
12) Trent checks the equality of the $\tilde{m}$ and $\bar{m}$. If they are equal then stores the message $\tilde{m}$ with Alice's and proxy group participants identifications for later traceability.

V. Security Analysis

Main requirements of the quantum digital signature protocols to provide unconditionally security are that the signature should not be disavowed by the signatory, and any attacker cannot forgery signatory's signature.

A. Impossibility of Forgery

Firstly, we consider insider attacker. We assume that Bob is illegal participant and wants to create a signature of Alice. Even if Bob knows the details of the signature protocol he cannot create Alice's signature because of trusted group manager Trent. Bob cannot create Alice's signature without knowledge of Trent. After the end of the legal signature protocol , Bob may change correct data m to $\bar{m}$. Because of the knowledge about correct m of Trent, Bob cannot achieve forgery.

Secondly, any proxy group member $\{G_1, G_2, ..., G_N\}$ may try to forge Alice's signature. Any individual proxy group member G_i cannot achieve forgery because of he/she can only contribute the part of the full signature. Suppose dishonest $N-1$ group of participants want to create a correct signature of Alice. But they cannot achieve that. Because, all of the $QFT(|m_i\rangle)$ state must be reordered with Trent's permutation to produce a correct signature of Alice. Even if any attacker can get the permutation, the permutation will be changed by Trent for every signature session. Trent must be part of the protocol. So any $N-1$ participant of proxy group cannot achieve collective forgery. Further, one of the proxy group member G_i may change $QFT(|m_i\rangle)$ state by applying unitary transformation. Then, Bob and Trent can decide who changed the state by comparing m and $\bar{m}$.

$$\Pi S_{AB} = E_{K_{AB}}(\Pi_A) \tag{18}$$

$$\Pi S_{BA} = E_{K_{AB}}(\Pi_B) \tag{19}$$

Thus, Alice and Bob decrypt $\Pi S_{AB}, \Pi S_{BA}$ with secret key K_{AB}. They checks equality of Π_A, Π_B.

B. Impossibility of Disavowal

In this protocol, all the members of the proxy group must cooperate to create a signature. Bob must get the data of the signature from the all group members to obtain valid signature. So any member of the group proxy can not disavow the signature.

Alice and Bob cannot disavow the signature because of the management of protocol by trusted Trent. Trent controls some communication steps of the protocol. If Alice can send different $|\tilde{m}\rangle$ to the Trent and claim that the signature is not mine. Trent can check the equality of the $|\tilde{m}\rangle$ from Alice and $|\bar{m}\rangle$ from Bob. Trent can decide whether the signature protocol is valid or not.

VI. Conclusion

It is well known that ring signature related to group signature. However group and ring signature have advantages and disadvantaged with respect to each other. For example , in many ring signature, it is assumed honest users and honestly generated public keys of ring . There is no security in the case of users sign with respect to a ring containing even one adversarial generated public key. However ring signature is flexible. But , in group signature, the signer can be traced by a designed group manager like our scheme. Also, in our scheme, amplitudes of quantum states is transfered to the phase space due to application of quantum Fourier transformation. So, it is very hard for attachers to get right quantum state. Furthermore, in our case like other quantum scheme , it is instantly possible to become aware of thief by quantum decoy state.

In this study, a new multi-partied quantum proxy group signature protocol based on QFT is proposed. All of the proxy group members are part of the signature creation. Alice expresses the message m into phase-space by using QFT. So the message m is expressed in phases of the output qubits of QFT. This improves the message security.Because, every member of the proxy group takes only one part of the message and thus knows only their part of the message. Alice sends every part of the message to the proxy group members to be signed. But Alice changes order of the output qubits of the QFT according to permutation information which is sent by trusted Trent. So any member of the proxy group does not know order of the qubits and also they cannot create a valid signature.

Any information(classical or quantum) in the protocol is sent by using encryption algorithm which is robust against forgery by insider/outsider attacker. Furthermore, decoy states can be used to be aware of Eve.

Bob can verify validity of the signature by the help of the trusted Trent and proxy group members. Trent must send the order of the qubits to the Bob to obtain real message m by using $QFT^{-}1$.

The above security analysis implies that given group proxy signature protocol based on QFT provides unconditionally security. In addition, our protocol provides higher efficiency, effective secret key usage and security.

Acknowledgments

I would like to thank referee for valuable suggestions and new insight.

References

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," 1997 SIAM J. Comput. 26 14841509

[2] L.K. Grover, "A fast quantum mechanical algorithm for database search," 1996 Annual Acm Symposium on Theory of Computing (ACM) pp 212219

[3] L. K. Grover," A framework for fast quantum mechanical algorithms," 1998 Proceedings of the Thirtieth Annual ACM Symposium on Theory of Com-puting STOC '98 (New York, NY, USA: ACM) pp 5362 ISBN 0-89791-962-9

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distiriubition and coin tossing," 1984 Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (India) p 175

[5] A. K. Ekert, " Quantum cryptography based on Bell's theorem," 1991 Phys. Rev. Lett. 67(6) 661663

[6] F. Gao, F. Z. Guo, Q. Y. Wen and F. C. Zhu, " Quantum key distribution without alternative measurements and rotations," 2006 Physics Letters A 349 53 58 ISSN 0375-9601

[7] D. Mayers," Unconditional security in quantum cryptography," 2001 J. ACM 48 351406 ISSN 0004-5411
[8] R. Cleve, D. Gottesman and H. K. Lo, " How to Share a Quantum Secret," 1999 Phys. Rev. Lett. 83(3) 648651
[9] M. Hillery, V. Buzzek and A. Berthiaume, " Quantum secret sharing," 1999 Phys. Rev. A 59(3) 1829-1834
[10] X. B. Chen, X. X. Niu, X. J. Zhou and Y. X. Yang, " Multi-party quantum secret sharing with the single-particle quantum state to encode the information," 2013 Quantum Information Processing 12 365380 ISSN 1573-1332
[11] H. Da-Zu, C. Zhi-Gang and G. Ying, " Multiparty Quantum Secret Sharing Using Quantum Fourier Transform," 2009 Communications in Theoretical Physics 51 221
[12] D. Gottesman and I. Chuang, " Quantum Digital Signatures," 2001 eprint arXiv:quant-ph/0105032
[13] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf," Quantum fingerprinting," 2001 Phys. Rev. Lett. 87(16) 167902
[14] G. Zeng and C. H. Keitel, " An arbitrated quantum signature scheme," 2002 Phys. Rev. A 65(4) 042312
[15] P. O. Boykin and V. Roychowdhury, " Optimal encryption of quantum bits," 2003 Phys. Rev. A 67(4) 042317
[16] H. Lee, C. Hong, H. Kim, J. Lim J and H. J. Yang, " Arbitrated quantum signature scheme with message recovery," 2004 Physics Letters A 321 295 300 ISSN 0375-9601
[17] Q. Li, W. H. Chan and D. Y. Long, " Arbitrated quantum signature scheme using Bell states," 2009 Phys. Rev. A 79(5) 054307
[18] D. Chaum and E. van Heyst 1991 Group Signatures (Berlin, Heidelberg: Springer Berlin Heidelberg) pp 257265 ISBN 978-3-540-46416-7
[19] X. Wen, Y. Tian, L. Ji and X. Niu, " A group signature scheme based on quantum teleportation," 2010 Physica Scripta 81 055001
[20] W. Xiaojun, " An E-payment system based on quantum group signature," 2010 Physica Scripta 82 065403
[21] Y. Yang, " Multi-proxy quantum group signature scheme with threshold shared verification," 2008 Chinese Physics B 17 415418
[22] Y. Yang and Q. Wen, " Threshold proxy quantum signature scheme with threshold shared verification," 2008 Science in China Series G: Physics, Mechanics and Astronomy 51 10791088 ISSN 1862¬2844
[23] J. Shi, S. Zhang and Z. Chang, " The security analysis of a threshold proxy quantum signature scheme," 2013 Science China Physics, Mechanics and Astronomy 56 519523 ISSN 1869¬1927
[24] J. Shi J, R. Shi, Y. Tang and M. H. Lee, " A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform," 2011 Quantum Information Processing 10 653670 ISSN 1573-1332
[25] M. A. Nielsen and I. L. Chuang 2011 Quantum Computation and Quantum Information: 10th Anniversary Edition 10th ed (New York, NY, USA: Cambridge University Press) ISBN 1107002176, 9781107002173
[26] T. Kim, J. W. Choi, N. S. Jho and S. Lee, " Quantum messages with signatures forgeable in arbitrated quantum signature schemes," 2015 Physica Scripta 90 025101
[27] W. Zhang, D. Qiu and X. Zou, " Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation," 2016 Quantum Information Processing 15 24992519 ISSN 1570-0755

Biometric Verification on e-ID-Card Secure Access Devices: A Case Study on Turkish National e-ID Card Secure Access Device Specifications

Atila Bostan
Computer Engineering Department
Atılım University
Ankara, Turkey
atila.bostan@atilim.edu.tr

Gökhan Şengül
Computer Engineering Department
Atılım University
Ankara, Turkey
gokhan.sengul@atilim.edu.tr

K. Murat Karakaya
Computer Engineering Department
Atılım University
Ankara, Turkey
murat.karakaya@atilim.edu.tr

Abstract

Biometric verification on e-ID cards requires clear procedures and standards be defined, especially when the access devices are anticipated to be produced commercial companies. Turkish national e-ID card project has reached the dissemination step. Now the commercial companies are expected to produce and market e-ID card access devices which will conduct secure electronic identity verification functions. However, published standards specifying e-ID card-access-device requirements are ambiguous on biometric verification procedures. In this study, we intended to attract scientific interest to the problems identified in the current design of biometric verification on Turkish national e-ID cards and proposed several verification alternatives which enables the production of e-ID card access devices in a commercial-competition environment.

Index Terms

e-ID cards, biometric verification, Turkish national e-ID cards.

I. INTRODUCTION

Electronic Identification Cards (e-ID) are getting prevalent in most of the countries worldwide. Especially EU member countries are speeding up on the transition to e-ID, since the recognition of e-IDs in EU member counties will be mandatory as of 29 September 2018 [1]. Turkey has started handling of national e-ID cards to citizens in early 2017 and plans to complete initial distribution until 2018 [2].

The motivations behind Turkish transition to e-ID cards are listed as; [2]

- providing means for secure identity verification
- preventing citizens from unjust-treatment as a result of identity fraud
- easing the access to e-government services
- be used for travel document (for the destinations exempt from visa)
- be used in e-signature process
- increasing the citizen satisfaction and service quality in community services
- reducing the amount of financial loss due to the personal incompetency in identity

Turkish e-ID cards support three discrete identity verification alternatives, namely visual, electronic and biometric verification methods. Hence, they should have secure and enough number of evidences in order to assure these verification alternatives.

On the other hand, secure card access devices needs to be developed and produced, in order to have functional and widespread usage of e-ID cards. Card access devices should guarantee certain level of security and should support different methods for identity verification. Additionally, for some financial, maintenance and commercial reasons, they are preferred to be produced by the companies in the industry. So that there is a strong requirement for descriptive, functional and measurable standard specifications, since these devices are expected to use e-ID cards which is developed and produced by the General Directorate of Civil Registration Services and should guarantee certain security levels. In order to design and produce a compatible e-ID card access device, companies need to know supported communication alternatives by the e-ID card and the structure of the data which can be accessed. Furthermore, companies should know the security requirements to support the demanded security levels. With the intention to meet these industry requirements, Turkish Standards Institute published four standards explaining the specifications for secure e-ID card access devices in 2013 and updated in in 2017 [3,4,5,6]. Although, the physical and electronic specifications of the smart cards which are referred by e-ID card access device standards are specified in another series of standards [7,8,9], they are not scrutinized in this study.

In secure e-ID access device specification standard series, there are 11 identity verification alternatives listed [10]. Depending on the assurance requirements of the application, the choice in between these verification alternatives is expected to be made by the verifier or be imposed by verification-policy server. Biometric data on e-ID is to be used in 3 out of 11 identification verification alternatives. Even though a passport-size photograph of the card holder is stored in the e-ID card content, it is not referred as biometrics in the standard series, since it is planned to be used only for visual verification alternatives. These 3 biometric verification methods are named and listed as follows in the standard series.

- Method 5: Verification on secure access device by using biometrics.
- Method 10: Verification on secure access device by using PIN and biometrics.
- Method 11: Verification on secure access device by using PIN, biometrics and photograph of the card holder.

However 3 identity verification methods are defined in the standards, the structure for the biometric data in the e-ID card is not mentioned. Hence the device developers face a compatibility problem in design.

In this study, we propose solution alternatives with a comparison on advantages and disadvantages for biometric information storage and retrieval in e-ID cards. Because no rationale is published on the effective policy requirements in designing and in texting the standards, we interpret our predictions as the reasoning.

II. PRIVACY AND SECURITY CONSIDERATIONS

The design of Turkish national e-ID cards was conducted by The Scientific and Technological Research Council of Turkey (TÜBİTAK). Following the technological feasibility, functionality, pilot usage and security studies, actual production and dissemination of e-ID cards were commenced. Published standards are one of several outcomes of these studies as well. So that, the definitions, methods and specifications in standards were assumed to be well studied and tested.

Apparently, e-ID cards are instruments with high privacy and security requirements. The content of the card is strongly private and sensible to exploitation. It goes without saying, security and privacy considerations should take precedence in e-ID card specifications.

In line with the specifications in current secure e-ID card-access-device standards, we consider the rationale in not specifying the biometrics data structure and feature sets which are used in Turkish national e-ID cards is the secrecy. Since keeping these parameters secret, would bring significant level of a support for the security of the biometric information, without doubt, until those are discovered. Furthermore, if biometric feature data are accessed then it is possible to use them for malicious or fraudulent purposes either as feature data or by reproducing the biometric input from them.

Nevertheless, the most important security risk in biometrics is their unsuitability for revocation and cancellation. In all of the identification instruments used in security domain, biometrics has the hardest problem in cancellation and revocation. It is typically easy to cancel or revoke passwords, tokens or digital-certificates when needed. But it is not the case for the biometrics. It is impractical for one to revoke his finger-print and change to a new alternative. This characteristics increases the privacy and security requirements for the biometrics. Anyhow, people have limited number but static biometric information. One can change his password, token or digital-certificate to any one he chooses from a theoretically infinite alternative pool. But for the biometrics, options are limited especially for hand and retina vein maps.

III. PROBLEMS WITH THE CURRENT DESIGN

Turkish national e-ID card access devices should meet a set of security requirements, such as blocking the remote access, keeping specific event/user logs and being temper resistant etc. In order to certify whether the devices meet these requirements, they are obliged to Common Criteria (CC) tests with a predefined protection profile [11]. In short, e-ID card access devices should be secure and resistant to a set of predefined security attacks. By their specification, they are bind to use an embedded cryptographic smart card (referred as Secure Access Module-GEM) to store security sensitive data such as private keys, signature certificates and perform several security operations such as authentication, signing etc. Secure Access Modules are planned to be provided by TÜBİTAK following the CC certification.

In all 3 identity verification methods that are specified by the standards, biometric verification is planned to be conducted either on e-ID access device or in biometric sensor. Although implementing one way of the verification is adequate for meeting the standards, both ways are supported. However, these biometric verification alternatives are problematic from the point of card access device production.

If the producer opts for on-device verification alternative then the data structure and feature notation of the biometrics should be known by the designer. Since, with the purpose of verifying the identity, the device is supposed to compare the scanned biometrics with the biometric data which is read from e-ID card, assuming proper access rights such as PIN and/or certificates are provided. Nevertheless, the data structure and the feature notation used in e-ID card for biometrics is not published. This means e-ID card access device producers will not be able to develop a verification system running on the device.

On the other hand, if the producer opts for verification on biometric sensor, then acquiring a sensor which can process biometric-data with the structure used in e-ID cards will be needed. As it is with the previous option, without the knowledge of the data structure used in e-ID cards, acquiring a proper sensor is problematic.

Moreover, cancellation or revocation of biometric data is not supported with the current verification and usage. Even though biometric data is problematic in cancellation and revocation processes, there can be several algorithmic alternatives to support these procedures as well.

IV. PROPOSED ALTERNATIVES TO BIOMETRICS STORAGE AND PROCESSING

We are quite aware of the fact that finding a solution that would solve all the listed problems without bringing about new ones is not realistic. However, in this study, we wanted to list several alternatives that can be commercially implemented and produced by no additional security risks but with some functionality and processing degradation. In brief, we focused on commercially productivity of e-ID card access devices. Below the alternatives for biometric verification of e-ID card-holder are listed with some basic explanations on each of them. In the next section, advantages and disadvantages (additional requirements) are given to help in comparison and decision making.

A.Alternative 1: Verification on a remote server

In this alternative, biometric verification will be conducted on a government-controlled server. E-ID access devices will transmit citizen (or card identity) along with the scanned biometrics without processing (as a digital image) to a secure biometrics-verification server and receive the verification result. No biometrics will be stored on e-ID card. Access device and the sensor do not need to process biometrics.

B.Alternative 2: Encrypted storage of biometrics

This alternative requires the knowledge of biometric data structure. However getting access to the biometrics will necessitate another security step other than PIN. For the encryption a symmetric key which is encrypted by card-holder's public-key may be utilized for computation convenience, otherwise encrypting biometrics by the public-key can be an option. This encryption will enable an indirect cancellation and revocation of biometrics when public-private keys are updated.

C. Alternative 3: Provision of a dynamic library

A dynamic library code can be provided by the government agency (namely TÜBİTAK) to process the biometrics and run verification algorithm to the access device producers. In this alternative, biometric data structure used in e-ID cards does not need to be known by the access device producers and several types of sensor data formats and biometric features can be supported. Biometrics storage structure and verification details will be hidden to access device producers. The dynamic library can be stored and run on the Secure Access Module (GEM) card or otherwise on access device itself.

D.Alternative 4: Biometric hash usage

A combination of alternative 1 and 2 with some modifications can be used in e-ID biometric verification process. In this alternative biometric data structure is publicly shared with the access device producers, so that access devices can verify the scanned biometrics. But a central validity check is introduced to the process steps with a minimum network and communication overhead. For central verification a hash of the biometric data on e-ID card is to be transmitted to a government controlled validation server and validity result is received. This mode of operation enable the cancellation and revocation of biometrics.

V. COMPARISON OF THE ALTERNATIVES

As we have mention in the previous section each biometric verification algorithm has its own advantages and disadvantages. In this section we list the advantages and disadvantages of the current and proposed mode of operations in biometrics verification by using e-ID cards.

A.Current running mode

Advantages;

- Local verification of biometrics
- No need for a network connection
- No need for a central service
- Biometric data storage structure s hidden from access devices

Disadvantages

- Access devices cannot be produced by commercial companies without sharing the biometric data and verification algorithm specifications
- Biometrics cannot be cancelled or revoked
- Parameters for sensor acquisition is not set. Suitable sensors cannot be acquired.
- Commercial competition is not supported among access device producers

B.Alternative 1

Advantages

- No need to sore biometrics on e-ID cards
- No need to share biometrics storage structure
- No need to share the verification algorithm specifications
- Sensor specifications can be shared with a minimum set of requirements
- Cancellation and revocation of the biometrics are enabled
- Access devices can be produced by commercial companies
- Supports commercial competition among access device producers

Disadvantages

- No local biometric verification
- Requires a secure central high performance service
- Requires a network connection

C.Alternative 2

Advantages

- Biometric storage structure can be shared
- Getting access to biometrics requires an additional security procedure
- Fraudulent usage risk of biometrics is reduced, especially without existence e-ID card
- Local biometric verification
- No need for a network connection
- No need for a central service
- Sensor specifications can be shared with a minimum set of requirements
- Cancellation and revocation of the biometrics are enabled by the change of encryption key
- Access devices can be produced by commercial companies

• Supports commercial competition among access device producers

Disadvantages

• Requires a decryption step in biometric verification process

• Biometric storage structure will be revealed

• Verification algorithm specifications should be published

D.Alternative 3

Advantages

• Biometric storage structure is hidden

• Verification algorithm specifications is hidden

• Local biometric verification

• No need for a network connection

• No need for a central service

• Sensor specifications can be shared with a minimum set of requirements

• Access devices can be produced by commercial companies

• Supports commercial competition among access device producers

Disadvantages

• Requires a dynamic library and communication parameters be developed

• Requires secure and reliable distribution of dynamic library

• Additional measures are needed to enable cancellation and revocation of biometric data

E.Alternative 4

Advantages

• Cancellation and revocation of the biometrics are enabled by the usage of central verification server

Disadvantages

• Biometric data structure will be revealed

• Verification algorithm specifications should be published

• Requires a secure central verification service

• No local verification

• Requires a network connection

VI. CONCLUSIONS

Developing secure e-ID card is not always a simple process. It necessitates a series of critical decisions to be made, tests to be conducted and production to be coordinated. Turkey is about the end of her transition to national e-ID card usage. Distribution of e-ID cards to citizens started in 2017 aside from some previous and local pilot studies. At the current step, commercial production of e-ID card access devices are anticipated, following the standards publication. But this step is not problematic with the current design of usage which is specified in the standards.

The most important problem in the current specifications is in the biometric verification process, since the ambiguity in this process blocs the production of secure e-ID access devices. In this study, we proposed 4 alternatives for the biometric verification process on e-ID cards. Our focus is to enable the production of access devices while enabling commercial competition. We have listed our proposed mode of operations with their respective advantages and disadvantages.

We fairly admire the existence of several administrative, financial and technical constraints. In this kind and size of a projects firm constrains are generally inevitable. However, the current running mode as it is depicted in the standard series does not enable commercial development of the Turkish national e-ID card secure access devices. With the intention to attract focus on the problem and provide several plausible solutions we have conducted this research. Excluding the other possible considerations, from a technical perspective, our evaluation points to alternative 3 for a plausible solution.

REFERENCES

[1] European Commission, Digital single market - e-Identification, accessed online from https://ec.europa.eu/digital-single-market/en/e-identification, on 12.08.2017

[2] Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Yeni Kimlik Kartları, accessed online from http://www.ekds.org/, on 12.08.2017

[3] Turkish Standards Institute, TS 13582 Secure card access devices for Turkısh national identity cards- overview.

[4] Turkish Standards Institute, TS 13583 Secure card access devices for Turkish national identity cards- interfaces and their characteristics.

[5] Turkish Standards Institute, TS 13584 Secure card access devices for Turkish national identity cards- security specifications.

[6] Turkish Standards Institute, TS 13585 Secure card access devices for Turkish national identity cards KEC application software specifications.

[7] Turkish Standards Institute, TS 7246 EN ISO IEC 7810 Identification cards- Physical characteristics.

[8] Turkish Standards Institute, TS ISO/IEC 14443-1 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics.

[9] Turkish Standards Institute, TS ISO/IEC 14443-2 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface.

[10] Turkish Standards Institute, TS 13678 Electronic identity verification system - Part 1: Overview.

[11] National Research Center of Electronics and Cryptography, eID Applications Unit, Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System.

Biometric Based Cryptographic Key Generation For Secure Applications

Samet Öztoprak
Science Institute
Istanbul University, Istanbul, Turkey
sametoztoprak@hotmail.com

Muhammed Ali Aydın
Science Institute
Istanbul University, Istanbul, Turkey
aydinali@istanbul.edu.tr

Ahmet Sertbaş
Science Institute
Istanbul University, Istanbul, Turkey
asertbas@istanbul.edu.tr

Abstract

More and more people are exposed to internet fraud every day because of the increasing use of the internet. The passwords defined by the users are generally weak, fragile and predictable. The best way to overcome this situation is to use biometric encryption systems. The biometric parameter based encryption systems basically suggest solutions for two main issues. One of these problems is the possibility of forgetting or losing the password, which is not the nature of biometric systems. Secondly, the uniqueness of the key generated by the biometric parameter. For this purpose, the fingerprint is transformed into a matrix, and a unique key is obtained from this matrix. The public key is generated by helping of this unique key. On our study, an algorithm is proposed which is based on the biometric parameter, thus generating a public key, which makes the RSA algorithm stronger. Because of the simplicity of the mathematical approach used in our work, the proposed method is a very effective and rapid way to generate a unique key from a biometric parameter. Cryptoanalysis methods on RSA show that this new method is safer.

Keywords-component

Asymmetric cryptography, Biometric cryptography, Fingerprint, Biometric parameters.

I.INTRODUCTION

Our main goal on our study is to increase the security for all bank transactions, bill payments and other everyday purchases on internet. It is so obvious that the need for transaction security on the network requires to take more serious security measures. As well known, it has occurred millions of internet fraud cases every day in the world. New solutions and approaches are proposed to overcome this problem. Biometric parameters appear as the best solution to this issue, because they are both persistent and not easy changing, that makes them a strong security feature. In our internet security model, the public key is selected by using the unique key generated from the biometric parameters.

In this work, we tried to bring a simple and reliable solution to this security issue. For this purpose, we use a simple mathematical method which can be applied to other biometric parameters that can be transformed into matrices. This superior feature increases the usability of our mathematical method. In section 2, the related work in the literature is summarized in order. In section 3, the basic RSA algorithm is described briefly. In Section 4, the biometric based unique key is generated after the fingerprint image has been subjected to filtering and mathematical operations; also the general scheme of our encryption system developed on our study is given. In Section 5, the algorithm we developed is described step by step. In the last section the results of our work are given.

II.RELATED WORK

In [1], Mohammed worked on the 2-step fingerprint identification system has been studied using the basic methods used for fingerprint identification. The server has increased the verification rate of fingerprint data using these 2-step fingerprint data. Much of the work expenditure on fingerprinting, as on our study and other articles examined, has led us to use fingerprints in our work. In [2], Guo, Susilo and Mu introduced a new concept of biometric encryption. They used fingerprints, eyes, faces and hands as encryption parameters. In making this verification, he verified these biometric parameters using the Euclidean distance parameter. This approach controls the accuracy rate with a specified threshold value. Values above this specified threshold value will be considered correct. Our work is a similar one because on our study key production was tried to be done on biometric parameters. In [3], Chakraborty and Bandyopadhyay studied biometric parameter-based encryption algorithms are becoming popular increasingly. Iris, fingerprints, palms, sound, etc. The use of biometric parameters in encryption algorithms in terms of performance and usability has been investigated. Detailed data and graphics are given on our study. It gives us information about which biometric parameter should be used on out study. In [4], Murakami, Ohki and Takahashi have attempted to produce a solution by using mathematical calculations to reduce the most of the offensive attacks used in biometric encryption. This study inspired us in our study of cryptanalysis. In [5], O. Joymala and N. Khare studied the security of smart home systems has been developed with the sound biometrics parameter. The concept of the internet of things is getting more and more every day, and this requires more security precautions on communication with our de-

vices. We can see how secure communication is provided with voice parameters. In [6], T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma are trying to create a biometric-based protocol in the study. In this protocol, fingerprint biometric parameters are also used in public encryption. It has been found that a more secure public encryption algorithm has emerged. In [7], A. Ramesh worked to encrypt the biometric parameters to keep them encrypted and not to pass on someone else. In our work, we went on to cryptographically store biometric parameters in the database and on the network in encrypted form. In [8], K. Ankit and J. Rekha studied a matrix was created using the minutiae information from the fingerprint and then this matrix was used in the production of public keys. In fact, this study can be shown as the base of work.

In [9], Y. Kumar, R. Munjal and J. Rekha compare symmetric and asymmetric cryptography methods. In doing so, we compare strengths and weaknesses by comparing DES for symmetric cryptography and the RSA algorithm for asymmetric cryptography. In [10], A. K. Jain, J. Feng and K. Nandakumar, A Study on the Identification of the Fingerprint Biometric Parameter. In [11], P. Mahajan and A. Sacheva model points the performance of RSA, DES and AES algorithms is compared and the results are shown. In [12], M. Manoria, A. K. Shrivastava, S. S. Thakur and D. Sinha studied the reliability of the cryptographic system is increased by applying the biometric parameter to the RSA encryption algorithm. Progress in performance is shown graphically. In [13], F. Hao, R. Anderson and J. Daugman have attempted to integrate the iris biometric parameter into the AES encryption algorithm in the essay. During this process, the iris provides information on how to manage bit errors during identification. In [14], S. Chandra, S. Paul, B. Saha and S. Mitra claimed that the keys used in everyday life cannot be the unique key, so it is necessary to combine the biometric parameters to avoid key conflict between persons and to produce a unique individual key for each person. In [15], C. Rathgeb and A. Uhl conducted a study on the identification of biometric parameters. It is demonstrated the identification rates by comparing biometric parameters iris and fingerprints etc. In [16], Z. Jin, A. B. J. Teoh, B. Goi, and Y. Tay. main goal to produce a single key with minutiae information. In [17], D. Boneh has demonstrated cryptanalysis methods on RSA for 20 years. Our algorithm with these cryptanalysis methods has been put to the test for safety. In [18], U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain discussed the superiority of biometric parameter-based encryption systems over traditional encryption systems. The advantages of a new biometric-based encryption method are described. In [19], Y. Kumar, R. Munjal and H. Sharma discuss the difficulties and security vulnerabilities of symmetric and public cryptographic systems. It helps us to go on what kind of cryptographic system. In [20], L. Ogiela, M. R. Ogiela and U. Ogiela address the study of biometric parameters with security measures, especially linguistic cryptography approach. In [21], G. Panchal and D. Samanta have tried to produce a constant single key from the fingerprint every time. The accuracy rate was found to be 97.25% on users. In [22], P.Balakumar and R. Venkatesan work on the creation of encryption keys over biometric parameters. In this work, a production scheme has been created to hide the key.

III.BASIC RSA CRYPTOGRAPHY

As it is well known, RSA is the best example of asymmetric cryptography. As shown in Fig. 1, during communication between Begüm and Ali, Ali receives a public key with n number to encrypt his data. After he encrypts his data by public key and n number pair, Ali sends his encrypted data. Then Begüm can open it with her own private key and n number pair which is kept by herself.

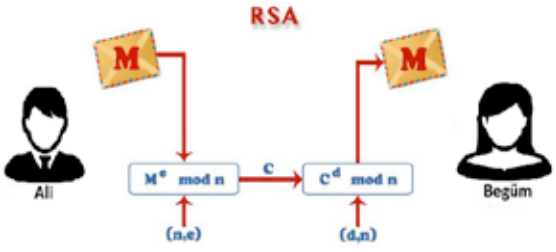


Fig. 1. The working principle of RSA cryptosystem.

A.Asymmetric cryptography principles are as follows:

1.Begüm wants the cryptosystem to generate a key pair which is consisted a public key and a private key. N and public key pair is sent to Ali to encrypt his data

2.Ali will encrypt the data by using a public key and n pair when sharing data between them.

3.When Begüm received encrypted data. It is used private key and n value to unlock encrypted data.

B.Also, RSA key generation steps are given at bottom;

1.Two prime number is chosen p and q.

2.Calculate n = pq

3.Totient calculate Φ = (p-1)(q-1).

4.1<e< Φ gcd(e, Φ)=1.

5.d private key de =1 mod Φ.

6.(e,n) public key.

The above RSA algorithm belongs to the public-cryptography system. In the next section, this algorithm will be modified by some mathematical approaches that empower RSA algorithm against cryptanalyze methods. This mathematical approach will be based on biometric parameters.

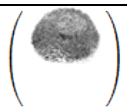
IV.BIOMETRIC BASED UNIQUE KEY GENERATION

As known, personal information sharing in any kind of platform creates a serious security problem. Personal information should not be stored in the database or sent to the network directly. The personal biometric parameters such as fingerprints, iris, and palm are kept in the database in a kind of masking format due to drawbacks of keeping personal parameters. One of the drawbacks of keeping personal

information in database is against the law of personal data retention. The other drawback is that person's data is used in fraud events.

Table I shows the steps of turning from matrix to the unique key. Firstly, fingerprint is represented as a matrix form afterwards it is found the average value in matrix. According to this average value, the matrix is reduced to a matrix which consists of only 1 and 0 values. This process can be called as filter process. The values of N and M are the matrix sizes which are obtained from fingerprint picture. Each value in the row is summed and then it is written at the beginning of the line and thus obtained N size array. The values in each column of the matrix are summed and then obtained M size array. These two arrays are merged. The last array which consists of merging 2 array is the unique key. This unique key is used to public key generation. New RSA algorithm based on biometric parameter indicate a strong defense against cryptanalyze methods through the unique.

TABLE I. CREATE UNIQUE KEY FROM A FINGERPRINT

Fingerprint picture.	
Resize picture.	$\begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ z_{n,1} & \cdots & z_{n,m} \end{bmatrix}_{nxm}$
Find average value of picture.	$avg = \sum_{k=1,l=1}^{m,n} a_{k,l} / 2$
Filter picture take into consideration average.	$a_{m,n} = \begin{cases} 1, & avg < a_{m,n} \\ 0, & avg \geq a_{m,n} \end{cases}$
Open as a matrix and get unique key.	$\begin{bmatrix} \sum_{k=0}^{m} a_{1,k} * 2^k \\ \vdots \\ \sum_{k=0}^{m} a_{n,k} * 2^k \end{bmatrix} \begin{bmatrix} a_{0,0} & \cdots & a_{0,m} \\ \vdots & \ddots & \vdots \\ a_{n,0} & \cdots & a_{n,m} \end{bmatrix}_{nxm} \begin{bmatrix} \sum_{k=0}^{m} a_{k,1} * 2^k & \cdots & \sum_{k=0}^{m} a_{k,n} * 2^k \end{bmatrix}$
Unique Key.	$\begin{bmatrix} \sum_{k=1}^{m} a_{1,k} & \cdots & \sum_{k=1}^{m} a_{n,k} & \sum_{k=1}^{m} a_{k,1} & \cdots & \sum_{k=1}^{m} a_{k,n} \end{bmatrix}$

V.UNIQUE KEY - CHARACTER SET CONVERSION

A character table is generated to store the values in a single key. By matching the characters through this table, these values are stored both as a character array and as secret in the database. The characters used here can be selected by the person developed the system. The number of characters must be width and height of matrix. The reason for this is that it must be enough number that can store every value of a single key array.

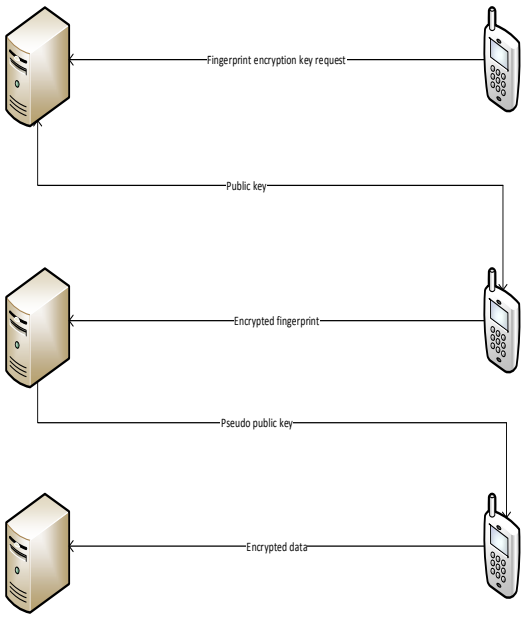


Fig. 2. The operational schema of RSA based on biometric parameters algoritm.

Figure 2 shows the biometric RSA encryption algorithm. Here, the user creates the fingerprint's unique key from the server. The reason for this is that the generated individual key will be used to generate the public key, and privacy will be ensured by keeping this data in the database rather than the fingerprint. A public key is sent in order to prevent freely roaming fingerprint on the network. The fingerprint is encrypted with this key. Encrypted fingerprint form is opened to produce a unique key. After this step, the public key is sent to the user based on the generated single key. This public key is in a certain frame structure so that it cannot be seen on the network. The complexity is increased by giving time and encrypted public key together in this frame structure. A frame in the format (ddmMyyyyhhmm + encrypted public key) is delivered to the user. The reason for this is that it is ensured to prevent the various methods used to reach the private key from the public key. The public key is multiplied by a time-based formula to make it a very large number. On this count, it becomes more difficult for fake receivers to make sense of this number. The key to being sent is personally different because it is produced from the fingerprint image object. This allows us to create a different public key at every time. This is an important security measure as well.

VI. PROPOSED BIOMETRIC BASED RSA ALGORITHM

The following algorithm belongs to the new biometric-based RSA encryption algorithm. The public key is used to encrypt a text, while the private key is used to open the encrypted text.

The steps of proposed biometric based RSA algorithm are as follow:

1.Two prime numbers are chosen p and q.

2.Calculate n = pq.

3.Totient calculate Φ = (p-1)(q-1).

4.publicKeyvalue(date) < e < Φ and gcd(e,Φ)=1.

5.d private key de =1 mod Φ.

6.epseudo = e * getNumber(date).

As seen above, two prime numbers are selected like in the basic RSA encryption algorithm. These are multiplied by each other. Totient (Φ) is also calculated as the product of these two numbers by subtracting one from the selected prime numbers like in the basic RSA. Here, as the first place where it differs from the basic RSA, the selected public key is generated via a single key generated with the aid of the biometric parameter. Later on, this open key will generate an appropriate secret key. getNumber is a function that generates a selected public key time-based number, multiplies the public key by the value generated by this function, and generates a large number to prevent the public key from being sent explicitly.

A. publicKey Function

This function takes the date as a parameter. It uses the hour and minute of date to choose a reference point from the unique key so that a different key is produced each time.

publicKey(hhmm) = (hh + mm)*5 % (lenght) (1)

Where the length is the size of unique key. The number turning from this formula will be index number over unique key.

B. getNumber Function

This function takes the date as a parameter as well. Unlike publicKey function, it uses the year, month and day of date to make public key complicated.

getNumber(ddMMyyyy) = yyyy3 + mm2 + dd (2)

The formula given in (2) produces a number to multiply with public key. The frame which is sent to receiver will be in format (date + publicKey* getNumber(date)). The receiver uses the date to obtain the public key as encrypted data.

VII. PERFORMANCE EVALUATION

For our performance evaluations, all measurements were made using a computer with an Intel Core (TM) i7-4710MQ CPU @ 2.50GHz processor, 8.00 GB RAM capacity and a 64-bit operating system. Performance evaluation graphics are shapes based on this computer.

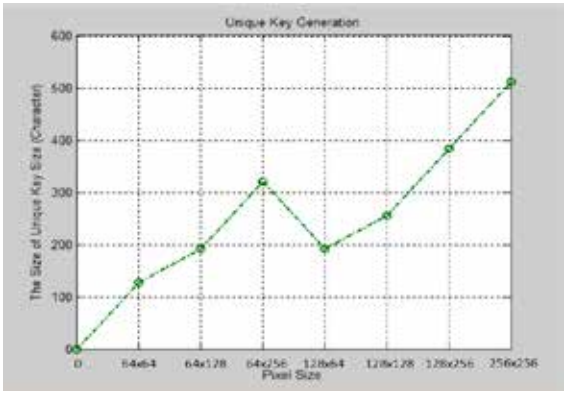


Fig. 3. Unique key production according to image size.

Figure 3 shows how the size of the individual key generated in the work changes according to the number of pixels in the image when a single key is obtained. As seen in Fig. 3, the size of the key will be h+w, which is expressed in height and width, respectively. This will have a performance effect.

In our approach, the key length depends on the fingerprint image sizes. Let assume that the fingerprint image has 64x128 pixels, so the uniqe key consists of 192 (64+128) characters. In Minutia Approach known in the literature, the unique key length depends on the number of minutia used in fingerprint image. So it is generated by the minutiae extracted from the image matrix. In the mentioned approach [10], the detail information on each finger varies from 20 to 70, as in Fig.4. The average number of characters for the coordinate values is calculated and the unique key value is determined from these values.

Blue : Minutia Approach *Green : Matrix approach(our work)*

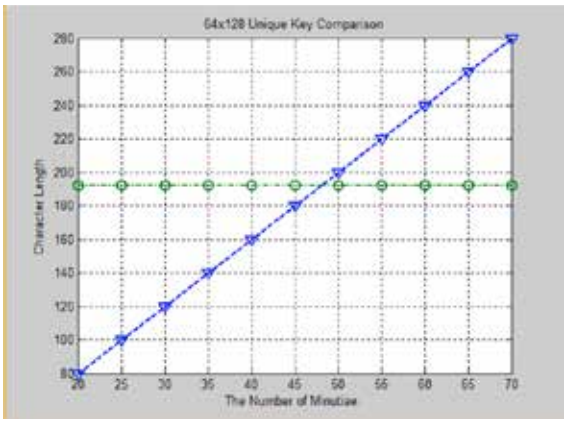


Fig. 4. Key size comparison.

Table II shows difference of both methods, our method and Minutia Approach, algorithmically. In order to compare both methods with each other, we counted each assignment in the algorithm as one operation, like the calculation (O) notation. So, in our work, cost evaluation as a performance metric is calculated by assignment count. The assignment count (cost) is measured as the computation time (seconds) as seen in Fig. 5.

TABLE II. ALGORITHM PERFORMANCE COMPARISON

Minutia Approach	Matrix Approach

for(h=0; h>H; h++)
for(w=0; w>W; w++)
for(p=0; p<12;p++)
if(minutiae(w,h,p))
registerKey(w,h)
	for(h=0; h>H; h++){
	x = 0;
	for(w=0; w>W; w++){
	x = x + matrix(h,w)
	}
	registerKey(x);
	}
	
	for(w=0; w>W; w++){
	x = 0;
	for(h=0; h>H; h++){
	x = x + matrix(w,h);
	}
	registerKey(x);
	}

As the fingerprint image size increases, the cost of the Minutia Approach increases sharply (seen in Fig.5), but the cost of our method increases slowly. On the other hand, as the number of minutia for selected fingerprint image increases, the key length also grows rapidly, but in our methods key length remains constant.

Blue : Minutia Approach *Green : Matrix approach(our work)*

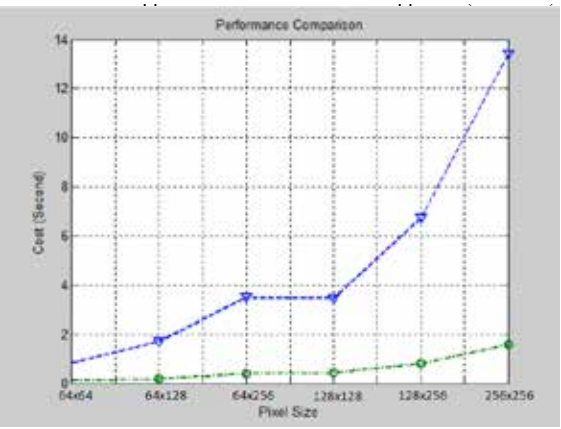


Fig. 5. Cost (Performance) evaluation

VIII.CONCLUSION

Biometric parameters, which are now being used more for identification, are being used to strengthen encryption algorithms. Our study shows how to make the RSA algorithm stronger with the biometric parameter. The mathematical method we used on our study shows that a more efficient unique key is generated and the public keys generated from this unique key increases the security level of the RSA.

As the future work, it will be investigated in the DNA of each individual, is the more powerful biometric parameter than a fingerprint, iris, palm and other biometric parameters. Because all these biometric parameters are changed by injuring and aging but DNA never changes throughout life [24]. We need a parameter that never changes from cradle to grave and available in all of the human cells, like the DNA biometric parameter for the future work. On the other hand, the biggest obstacle in the DNA parameter is the inability to resolve the large helical structure in an effective time scale, and today's processors will not solve the DNA helix effectively [24]. This situation is thought to be possible with the introduction of quantum computers. Nevertheless, it seems that DNA will play a crucial role in secure communication and identification in the future.

REFERENCES

[1] A. F. Mohammed, "Biometric Based Authentication Using Two-Stage Fingerprint Privacy Protection for File Storage on Serandr" International Journal of Computer Science and Mobile Computing, (IJCSMC 2016), vol. 5, Issue. 3, pp. 377 – 387, Mar. 2016, ISSN 2320–088X.

[2] F. Guo, Willy Susilo and Yi Mu, "Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption" ieee transactions on information forensics and security, (IEEE 2016), vol. 11, no. 2, feb. 2016, pp. 247 – 257, ISSN 1556-6013.

[3] S. Chakraborty and S. K. Bandyopadhyay "Emerging Biometric Technology-A Review" International Journal of Advances in Computer Science and Technology, Volume 5 No.1, Jan. 2016, pp. 8-22, ISSN 2320 – 2602.

[4] T. Murakami, T. Ohki and K. Takahashi "Optimal sequential fusion for multibiometric cryptosystems" National Institute of Advanced Industrial Science and Technology, vol. 11 No.3, Feb. 2016, pp. 1-16, ISSN 135-0064.

[5] O. Joymala and N. Khare "Securing a Smart Home Network using Voice Biometric" International Journal of Application or Innovation in Engineering & Management (IJAIEM 2016) vol. 5, issue. 2, Feb. 2016, pp. 113 – 118, ISSN 2319 - 4847.

[6] T. Zhao, Q. Ran, L. Yuan, Y. Chi and J. Ma "Image encryptionusing finger print as key based on phase retrieval algorithm and public keycryptography" State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin 150001, China, vol. No. , Mar. 2015, pp. 12-17, ISSN 150001.

[7] A. Ramesh and S. P. Setty "Analysis on biometric encryption using RSA Algoritm" International Journal of Multidisciplinary Educational Research, vol. 2, issue. 11(2), Oct. 2013, pp. 303 – 307, ISSN 2277-7881.

[8] K. Ankit and J. Rekha "Biometrics as a Cryptographic Method for Network Security" Indian Journal of Science and Technology, vol. 9, issue. 22, Jun. 2016, pp. 2 – 6, ISSN 0974-6846.

[9] Y. Kumar, R. Munjal and J. Rekha "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, vol. 11, issue. 03, Oct. 2011, pp. 2 – 6, ISSN 0974-6846.

[10] A. K. Jain, J. Feng and K. Nandakumar, "Fingerprint Matching" IEEE Computer Society http://biometrics.cse.msu.edu/Publications/Fingerprint/JainFpMatching_IEEEComp10.pdf

[11] P. Mahajan and A. Sacheva "A Study of Encryption Algorithms AES, DES and RSA for Security" Global Journal of Computer Science and Technology Network, Web & Security vol. 13, issue 15, 2013, pp. 14 – 22, ISSN 0975-4350.

[12] M. Manoria, A. K. Shrivastava, S. S. Thakur and D. Sinha "Secure Biometric Cryptosystem for Distributed System" International Journal Communication & Network Security, http://www.idc-online.com/technical_references/pdfs/information_technology/Secure%20Biometric.pdf

[13] F. Hao, R. Anderson and J. Daugman "Combining cryptography with biometrics effectively" http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-640.pdf, Jul. 2005, ISSN 1476-2986.

[14] S. Chandra, S. Paul, B. Saha and S. Mitra "Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data oandr a Network" IOSR Journal of Computer Engineering, vol. 12, issue. 01, May. 2013, pp. 16 – 22, e-ISSN 2278-0661.

[15] C. Rathgeb and A. Uhl "A surandy on biometric cryptosystems and cancelable biometrics" EURASIP Journal on Information Security http://jis.eurasipjournals.springeropen.com/articles/10.1186/1687-417X-2011-3.

[16] Z. Jin, A. B. J. Teoh, B. Goi and Y. Tay "A new biometric key binding and its implementation for finger print minutiae-based representation" Feb. 2016 ISSN 0031-3203. http://www.sciencedirect.com/science/article/pii/S0031320316000959.

[17] D. Boneh "Twenty years of attacks on the RSA Cryptosystem" https://crypto.stanford.edu/~dabo/papers/RSA-surandy.pdf

[18] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain "Biometric Cryptosystems: Issues and Challenges" Proceedings of the IEEE, Security vol. 92, issue 06, Jun. 2004, pp. 14 – 22, ISSN 0018-9219.

[19] Y. Kumar, R. Munjal and H. Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, vol. 11, issue. 03, Oct. 2011, pp. 60 – 63, e-ISSN 2231-5268.

[20] L. Ogiela, M. R. Ogiela and U. Ogiela "Comparison of Biometric and Linguistic Secret Sharing Protocols" Lecture Notes on Data Engineering and Communications Technologies (LNDECT), vol. 02, issue. 03, Oct. 2011, pp. 501-505, e-ISSN 978-3-319-49106-6.

[21] G. Panchal and D. Samanta "Comparable features and same cryptography key generation using biometric fingerprint image" Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Feb. 2016, pp. 50-55, e-ISSN 978-1-4673-9745-2.

[22] P.Balakumar and R.Andnkatesan "A Surandy on Biometrics based Cryptographic Key Generation Schemes" International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 02, issue. 01, Oct. 2012, pp. 80-85, ISSN 2249-9555.

[23] P. Srivastava Drug "Metabolism and Individualized Medicine" Division of Pharmacokinetics and Drug Metabolism Central Drug Research Institute, vol. 04, issue. 01, Apr. 2003, pp. 33-44, ISSN 1389-2002.

[24] M Yang, T Aung, R Husain, Y-H Chan, L S Lim, S K L Seah, G Gazzard "Choroidal expansion as a mechanism for acute primary angle closure: an investigation into the change of biometric parameters in the first 2 weeks" Scientific Report, Mar. 2005, pp. 288-300, ISSN 288–290.

Evaluation of Fingerprint Enhancement Techniques Used by Crime Scene Investigation

Mehtap ÜLKER
Department of Computer Engineering
Gazi University
Ankara, Turkey
mehtapulker@gazi.edu.tr

Bilgehan ARSLAN
Department of Computer Engineering
Gazi University
Ankara, Turkey
bilgehanarslan@gazi.edu.tr

Şeref SAĞIROĞLU
Department of Computer Engineering
Gazi University
Ankara, Turkey
ss@gazi.edu.tr

Ozet

Bu çalışmada, olay yeri inceleme sürecinde toplanan maddi delillerden olan parmak izi incelenmiş, özellikle olay yerindeki parmak izinin toplanma süreci değerlendirilmiş, parmakizi analizi ve iyileştirilmesinde kullanılan teknik ve yöntemler detaylı olarak araştırılmıştır, 2007-2017 yılları arasında yapılan akademik çalışmalar ve elde edilen başarı oranları ile geliştirilen tekniklerin kıyaslanmaları yapılarak, elde edilen sonuçlar değerlendirilmiş ve bazı önerilerde bulunulmuştur.

Anahtar Kelimeler

Olay yeri, biyometrik doğrulama, parmak izi, iyileştirme, ön işleme, son işleme, uyarlama.

Abstract

This study focuses on fingerprint, which might be material evidence, gathered during the crime scene investigation. The process of collecting fingerprints at the crime scene has been examined. Improvement techniques and methods used in fingerprint analysis have been investigated in detail. The studies conducted between 2007-2017 have compared according to success rates with development techniques. The results have been obtained and some recommendations have been made.

Index Terms

Crime Scene, biometric identification, fingerprint, enhancement, pre-processing, post processing, adjusting

I. INTRODUCTION

Crime scene expresses the dynamic region where the process of the event is analyzed, criminal suspect and victim can be identified. Any material obtained during the crime scene investigation in order to reveal the crime scene-victim- wrongdoer is called the finding. Crime scene investigation is a research to help clarify the crime of the incident, to find material evidence for the identification and evaluation of murderer or crime process [1,2].

Material evidence collected from the crime scene has certain characteristics [1]. These are:

- It is used to revive the committed crime.
- It is used to find the identity of the victim or to determine the relationship between the crime scene-victim-wrongdoer.
- It can be used as evidence in the court at the time of investigation, after being processed in laboratories.
- It has a material structure and can be alive or inanimate.

The main purpose of the crime scene investigation is to collect data, audio recordings, witness statements that point to the offense etc. without any change and deterioration. If the material evidence gathered from the crime scene is to be grouped [2]:

- Biological evidence; usually composed of body parts and body fluids such as blood, hair, semen, saliva, urine, feces, tissue fragments and bone, skin rashes and dandruff, nasal fluids and sweat
- Biometric evidence that characterizes the body such as fingerprint, footprint, palm print, tooth print, sound, image, data evidence, hand writing
- Inanimate evidence such as wheel trace, tool trace, traces of firearms, explosives, flammable and combustible substances, drugs, medicines, paints, shooting residues

Biological and biometric data collected from the crime scene are definitive proofs in determining the offender. DNA analysis is performed using biological evidence. It is briefly a person-specific descriptive code and is found throughout the body tissues. In addition, biometric evidence is also person-specific [3].

Biometry is used for two main aims: verification and identification. Verification is used in order to access to high security areas and access control such as airports, laboratories, hospitals, banks etc. In the identification process; system compares the biometric properties of the person with the other biometric properties of the previously stored databases and tries to find out who he/or she is. As a result, either the person is identified or the person being compared is not registered in the current database. For this reason, identification is usually used for the analysis of collected data in criminal proceedings [4].

Fingerprints taken as a result of criminal analysis cannot be processed like fingerprints used in other biometric applications, so biometric data are not used directly. Due to environmental conditions, the fingerprint data may not be enough capacity to provide the necessary properties, collected data may be just fingerprint's small part instead of the entire fingerprint or the fingerprint may not have sufficient quality

due to noise in the environment. For this reason, before the characteristic features of the fingerprint are collected [5]:

- Normalization, reinforcement, thinning, orientation calculations
- Finding the core point
- Extraction of minutiae points and determination of faulty minutiae points
- Finding reference points and matching procedures

Examination of the literature studies show that these stages have been carried out for identification process. As a result; some operations such as noise removal from fingerprint data, fingerprint separation from the crime scene background, deleting incorrect values from the fingerprint etc. directly affect the end result of who the fingerprint belongs to. For this reason, it is necessary to carry out all or some of these steps mentioned above. In Figure 1, the steps applied for a fingerprint from crime scene are visualized.

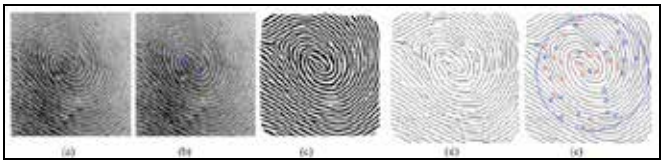


Fig. 1. Fingerprint analysis steps (a) introduction image, (b) reference points, (c) binarization, (d) thinning and enhancing, (e) finding minutiae points and identifying faulty minutiae points

Sequence of operations as mentioned above is expressed fingerprint image enhancement. In this study; collection and analysis of the fingerprint from the crime scene is investigated. In section 2, it is emphasized how fingerprints are used as identifiers. In section 3, preprocessing, adjusting and post processing, which are image enhancement steps, are mentioned and the techniques and methods used in these steps are analyzed according to the obtained success rates. In the last section; the results and suggestions obtained at the end of the study are shared.

II. FINGERPRINTS COLLECTED FROM THE CRIME SCENE AS IDENTIFIERS

All of qualifications used to identify someone and distinguish him or her from others are called identity. Putting forward these properties to know the person who is dead or alive is called as identification. Criminal investigations are very important for illuminating the event, punishing of the criminal, determining of victim or criminal who is dead and alive and people's life in peace and security. To illuminate the criminal events, it can be utilized factors such as age, gender, height, body weights, skin, hair, eye color, fingerprints, teeth trace, footprints, palm prints, etc. of the person for identification. Some characteristics such as age, gender, body weight, hair, and eye color among these elements are not determinants when it is difficult to recognize someone. For this reason, it should be used the biometric data to get more accurate result in recognition. There are lots of biometric data types that are common in the crime scene. Some of them are [1,2]:

- The reliability of recognition systems is quite high for DNA, which is obtained by utilizing the hair, saliva, blood, hair, teeth and bones collected by the scene investigation teams. Despite the fact that identification with DNA is fairly reliable, the collection and analysis of these data is very long and troublesome [1].
- The palm prints and footprints are obtained on the same conditions at crime the scene. These traces are similar to each other. So, while these traces are analyzed, it is difficult to distinguish from each other. In this respect, it is not useful for identification [1].
- When the criminals do not use any hand covering such as gloves, they leave the trace on the crime scene. These traces occur when sweat or skin oil comes into contact with the surface. These traces can be obtained easily by the crime scene teams at places like doors, locks, glass, window tops and edges, cups, plates, forks, knives, pillars, switches, fuses, light bulbs thought to have been loosened with the aim of being extinguished, clothes, shirt catches in case of strangulation, safe locks, drawers, glass, tiles and so on. The fingerprints in crime scene are made visible to the current methods and transferred to digital platform. Then fingerprint enhancement methods are applied [1].

The fingerprints obtained from crime scene are divided to three classes according to surface texture and whether they are visible or not [6,7]. These fingerprints types are explained in below:

- Plastic fingerprints are three-dimensional traces formed by touching finger of criminal or victim on soft surface such as soap, candle and wet paint [6,7].
- Visible fingerprints are traces formed by touching finger contaminating with a substance such as paint, blood, dust, flour, etc. These traces are investigated either naked eye or using alternative light sources. It is ensured that use of various chemical powders is more pronounced in case fingerprint appears. After the trace is made clear, photographing and transparent tape method is used to get it from where it is [6,7].
- Latent fingerprints are the invisible traces left by finger, which is not on the soft surface, and not contaminate with colorant. These traces transmit from the finger to the surface, thanks to the fluid released from the pores. Investigations are conducted on possible surfaces by assessing the nature of the event, the crime shape and the behavior of criminal at the crime scene. So it is tried to find a trace on these surfaces. To obtain such fingerprints clearly, it is necessary to use chemical methods, fingerprint powder, and alternative light sources [6,7].

The Methods of fingerprint acquisition on surfaces by the crime scene teams requires expertise. It is very important for the recognition process to be performed by experts and using the correct techniques while collecting traces. In the first

stage, they investigate the fingerprint on the visible surface. No matter how visible it is visible, they try to obtain smoother images. So, it is necessary to techniques providing image quality increase such as chemical methods and alternative light sources [7].

One of the most important methods used to find and collect latent fingerprints is to use chemical in movable or unmovable places. The obtaining clear fingerprints vary according to the environment, chemical methods, the skill of the experts, sensor limitations, intrinsic aging, factors like cuts, wrinkles, injuries and intrinsic aging. If the chemical methods to be used are not correctly selected, the traces may be distorted or disappear completely. For this reason, before the powers are used, alternative light source and cyanoacrylate should be used on movable or immovable surface. After fingerprinting becomes apparent with these methods in order to transfer digital media, photographing and transparent tape method is used to get it from where it is. However, the degradations based on sensor limitations are resolution, signal to noise ratio and cleanliness causes a reduction in image quality. Along with that, although the crime scene investigation team works meticulously, low quality images are obtained from the crime scene due to factors such as aging, cutting, injury, etc. For these reasons, the recognition system gives incorrect results. In order to clarify the event, identify the victim or criminal, punish the criminal, the fingerprint must be subjected to the enhancement process before matching operations. So, it is primarily necessary to know fingerprint structure and its properties in order to apply enhancement techniques correctly [7].

Fingerprints begin to form when baby's fingers touch mother's uterus. Fingerprints are unique patterns produced by ridges and valley appearing on the surfaces of fingers. The ridges are defined as the dark area in a fingerprint, while the valleys are defined as white area whose region is between two contiguous ridges [4].

Fingerprints are separated into two classes, local and global, depending on the flow of the ridges or the shape and relationship of the ridges. While local characteristics are used to match and verify, global characterizations are used to match, verify and classification [4]. In Figure 3 the local and global characteristics are shown and explained in bellow.

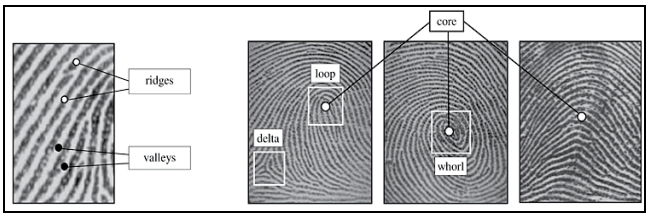


Fig. 2. Global and local characteristic in fingerprint

Global characteristics: Global characteristics formed by depending on ridges or the shape and relationship of the ridges are separated to four class including delta, loop, whorl and arc.

Fig 3. Global characteristics (loop, whorl and ark)

Local characteristics, which are known as a minutiae are local discontinuities in the ridge pattern and provide features to make a personal identification. Although there are many characteristics to be identified, the most of these characteristics are not commonly used to make a personal identification. Only two local characteristics of them, which are ridge ending and ridge bifurcation, are sufficient for identification. Ridge ending is abruptly the ending of ridge on finger. A ridge bifurcation knows as a ridge forks or diverges into branch ridges [8]. Automatic fingerprint matching is compare these minutiaes and their relationships to make personal identification [4,8]

As can be seen, fingerprints can be analyzed according to global characteristic such as loop, whorl and arc, and local characteristic such as bridge, island, line and bifurcation. Then identification is performed according to these characteristics

III. FINGERPRINT ENHANCEMENT TECHNIQUES

While fingerprints are obtained on the crime scene, environmental changes, chemical methods, surface, sensor limitation, age, cuts, and injuries causes the deterioration of image quality image [7]. All of the degradation makes difficult to extract feature. The ridges, which are in fingerprint pattern, contain information of characteristic features for minutiae extraction. The degradation affects these structures. So, the ridges may not strictly continuous due to small breaks (gaps) and contiguous ridges may not well be separated due to the presence of noise. Thus enhancing the fingerprint images are often employed to reduce the noise and become the ridge structures more apparent. The aim of image enhancement techniques improves the clarity of ridge structure in input fingerprint image [4,8,9-31]

In literature, many methods have been proposed to enhance images. However, there is not standard approach used to completely improve fingerprint images. In this works, techniques used in the literature are divided into three categories consist of preprocessing, adjusting and post-processing respectively and techniques in literature and shown in figure 1. In bellow, the methods used in each step are explained and their advantages *and disadvantages are discussed.*

A. Pre Processing Techniques

Pre-processing step can be defined as conversion operations on the data to remove the systematic errors in the aggre-

gated data. This step is performed before applying direction, frequency and filtering techniques in fingerprint images. [8-30]. Correction of errors in data and elimination of redundant data directly affects the recognition process. There are many different approaches for pre-process. One or more of these approaches may be used in this phase. The studies show that; the preprocessing step ensures that the ridges are more pronounced when extracting features and combinations of different techniques have different success rates. When the examined studies are summarized the following headings have been obtained. These are [9-31]:

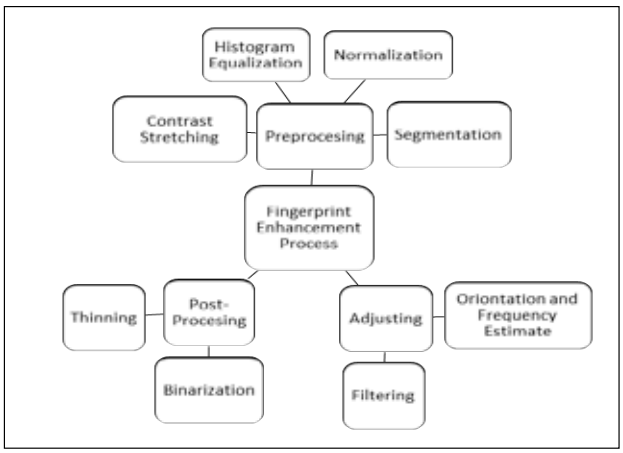


Fig. 4. Enhancement techniques in fingerprint image

Contrast Stretching: Contrast is an important factor in the process of evaluating image quality. Contrast is defined as the difference between visual objects that allow the object to be distinguished from other objects and from the background. Contrast stretching is general phase and linear and nonlinear transform functions such as image negatives, logarithmic transforms, power law transformations and piecewise linear transformations usually are used [16,30].

In study of Hari et al. [30] they have used unsharp masking which is a contrast-stretching scheme and they offer more enhancements in contrast but yielded broken ridges, especially in areas where the ridges are lost in noise. Draa et al. have proposed a new Artificial Bee Colony (ABC) algorithm for image contrast enhancement and have been improved for color image enhancement and their test results are promising [32].

Histogram equalization: Histogram is a graphic, which shows each color value in a numerical image. The brightness and tones in the picture can be determined by using this chart. Histogram Equalization is a method that improves the contrast in an image, in order to stretch out the intensity range. The main purpose of histogram equalization is trying to maximize the image contrast by applying a gray level transform. Histogram Equalization and contrast stretching can be considered as intertwined. While contrast stretching is interested with increasing the difference between the maximum-minimum intensity values, histogram equalization is interested about modifying the intensity values of pixels in image to ensure that the histogram flattened [9,29,31].

In study of Tang et al. proposed Adaptive Image Enhancement based on Bi-Histogram Equalization (AIEBHE) which divides the histogram into subgroups to preserve average brightness and their technique outperforms other histogram-equalization-based enhancement techniques in terms of preservation average brightness [33]. In proposed of Lai et al. MSHE method, textured regions in image should be highlighted and impact of smoother regions should be suppressed. Their experimental results show that; their method is quite competitive if any comparison to other method is made such as HE, BBHE [34].

Normalization: It is commonly used in the image enhancement process and can be thought of as one of the basic steps for image processing. Normalization is a phase in the process that can directly affect the success rate according to the way it is applied. If the mean and variance are calculated based on the entire image, successful normalization operation cannot be performed because of average mean and variance values are used in low-quality region. When local optimization is examined; image is divided into regions and the average and variance of each region are calculated. Since these values are used in the relevant sections, the results of the other section cannot be affected. Thus, the success of the normalization process increases [9,15,16,18,20,22,28,30].

In study of Saravanan et al. local histogram equalization and local normalization is used and normalization is performed in order to reduce the variation in gray level and obtain an image with a pre-specified mean and variance [9]. In study of Khan et al. they have proposed a method, which comprises of normalization, ridge orientation estimation, ridge frequency estimation and filtering stages. Their normalization step has provided avoiding imperfections in the fingerprint capture [35].

Segmentation: The techniques used to extract the fingerprint images from its background are called the segmentations. Since undesired background processing takes more time in enhancement, it is not useful. The aim of it is to reduce size of data, the time consumption of the image enhancement, facilitate the extraction of the minutiae Eliminating the region ends in minimization of number of operations in fingerprint image [16,17,20-22,28,31].

Balti et al. used to the K-means segmentation and Fuzzy c-means which are an unsupervised clustering technique. So it has been observed that it can reliably segment the fingerprint image other techniques [17]. In study of Gupta et al. proposed a slap fingerprint segmentation, which can accurately segment the fingerprints. This approach is used to eliminate several non-fingerprint components, improve its performance. It has been observed that it can correctly segment the fingerprints from the slap-images with an accuracy of 99.40% [36].

B. Adjusting Techniques

Adjusting step is defined as the extraction of intrinsic image and filtered image to extract correct feature extraction. İn this processing, firstly intrinsic information including direction and frequency is obtained and then according to intrinsic information filtering is applied. There are many dif-

ferent approaches for post-process. One or more of these approaches may be used in this phase. The studies show that; this process is the most important step in enhancement. Obtained correct orientation and frequency is improved the success of filter. The previous process defined as preprocessing does not enhance depend on orientation and frequency. So it cannot guarantee getting correct feature. For this reason, pre adjusting is required. When the examined studies are summarized the following headings have been obtained. These are [9,31].

Estimation of Orientation Field: Orientation field is described as the basic structure used in enhancement, which represents the ridge flow of fingerprint. It is important role in enhancement, feature extraction and as a consequence the accuracy of the recognition. The aim of estimating orientation field is to aid to extract correct feature extraction. İt has been realized that defining orientation field at the block level is better than at the pixel level in terms of reducing computational and storage complexity. By filtering along the ridge orientation, quality of fingerprint is improved. However, orientation estimate in latent fingerprint that is obtained from the surfaces of object at crime scenes is too hard since it is poor quality. In this situation reduces the accuracy of fingerprint identification [9-12,14,15,18-21,23,25-27].

In study of Bian et al. they proposed fingerprint orientation field extraction method based on quality grading scheme. In this approaches firstly they have computed the orientations of the higher quality blocks and then are computed the blocks with the lower quality. In other words, after the quality priority of the blocks has been determined, block orientation is estimated orientation. The aims of them spread the higher-quality block an orientation into the neighbouring lower-quality blocks. It has been realized that it cannot guarantee the accuracy of the assessments exactly [37]. In study of Luping Ji they used to projective distance variance of ridge in order to estimate block direction. So, they estimated block direction without using all block. This method is applied to binary image. It has been released that it is better result in terms of performance improvements in compare to other methods. But, the increase in noise intensity is caused to decrease estimation accuracy of orientation field and prolong the processing time [38]. In study of Chikkerur et al. in order to estimate orientation, they proposed a probabilistic approximation of the ridge orientation using short time Fourier analysis. Orientation and frequency information of images is obtained simultaneously. The estimation of orientation can be wrong due to a crease in the fingerprints that spans several analysis frames. However, if there is a crease in the fingerprints that spans several analysis frames, the orientation estimation will still be wrong. To overcome this problem, the orientation of its immediate neighborhood is used. Also, it approach does not regard to local discontinuities [23].

Estimation of Frequency: Frequency in fingerprint image is defined as average distances of inter ridges. As is in orientation field, frequency map cannot extract in the background region. Before estimation of frequency, by applying pre-processing consists of contrast stretching, histogram equalization, normalization and segmentation, the quality of poor region can be enhanced as much as it can be cured or during the segmentation phase of these processes in poor quality image is defined background. So extraction of feature does not occur. Since frequency map is used with contextual filter, it is important that frequency is obtained after preprocessing is applied. Obtaining frequency map in this direction is improved the success of enhancement. The frequency of image is used for extracting reliability minutiae in enhancement [9-12,15,18,21,23-26].

In study of Saravanan et al. in order to obtain frequency, they used to the 2-D Fourier Transform domain approach. This approach makes the process forceful. Also, it reduces the cost of calculation thanks to simultaneous computation of orientation and frequency. Through extraction the frequency of image with this approach, high achievement is obtained in enhancement. A pseudo-spectral fusion approach to fingerprint matching was proposed in [9]. A pseudo-spectral fusion approach depends on orientation and frequency. They developed to two methods in spatial and frequency domain in order to get frequency.in spatial domain methods, before obtaining frequency of image they performed median filter. The aim of using median filter is to eliminate values corresponding to pits and holes and normalizes the curve to have zero-mean They proposed 2-D Fourier Transform to estimate the frequency of image in frequency domain.it has been realized that proposed approach is the most efficient compare to other methods [39]. In study of Chikkerur et al. in order to estimate frequency, they proposed algorithm using short time Fourier analysis. Unlike most algorithms, frequency does not depend on orientation information. Orientation and frequency information of images is obtained simultaneously [23].

Filtering techniques: Filtering is a technique used to eliminate distortions occurring during the image formation. The aim of filters is to emphasize the gray values of pixels or prevent appear. The aim purpose of applying the filtering process in fingerprint images is to remove the noises by maintaining the continuity of the ridge and joint the breaks. So, it has been come to the forefront that filters must be applied it depends on direction. In this way, the feature extraction is performed correctly. In literature, there are the filters applied in the spatial field frequency domain for fingerprint enhancement. Despite the fact that the direction-dependent filters implement in both areas, the filters in the spatial domain cause computation complexity. So, filters in the frequency domain are more useful [9,16,18-28,20,31].

Table 1. Fingerprint Image Enhancement Techniques, Used Methods, Success Rate and Used Dataset

Ref. No	Purposed	Used Techniques	Success Rate	Data Set
9	Extracting and compressing the fingerprint feature	Local Histogram Equalization/ Local Normalization/ O-F Estimate/ Binarization	Compression Rate: 85%	FBI database
10	Estimating the parameters in an effective way/ Enhance the fingerprint	O-F Estimate/ Gabor Filter	EER: 11.5½	FVC2004: DB1_A
11	Improving the clarity of ridge structures in recoverable regions	O-F Estimate/ 2D Low pass Wiener Filter/ Second Derivative of Gaussian Filter	True Core Points: 74%	FVC-2004: DB1-A
12	Extracting the fingerprint characteristics better/ Improving the percentage of fingerprint identification/ Assessing the enhancement alg.	Gray Level Equalization/ O-F Estimate/ Gabor Filter	-	FVC2002 DB3
13	Enhancing the fingerprint	PCA Filter/ Thinning	-	-
14	Improving the clarity of the ridge structures in the recoverable regions/ Marking the unrecoverable regions for further processing	Orientation Estimate/ Gabor Filter/ Gaussian Filter/ Binarization/ Thinning	Orientation Extraction: 0.022s Enhancement Method Based On Gabor: 0.033	FVC2004 Databases/ live-scan database
15	Enhancing the fingerprint	Normalization/ O-F Estimate/ Gabor Filter	Better Perfor. Comp. to Prev.Works/ Hardware Cost 63.8k Gate	-
16	Enhancing the feature of sharpened image/ Reduces processing time	Normalization/ Segmentation/ Sharping Filter/ Gabor Wavelet Filter/ Binarization/ Thinning	Accurately Enhanced 97.14%	FVC2004
17	Extracting the ROI foreground/ Excluding the background regions/ Reducing the time of subsequent processing/ Avoiding the detecting false features	Contrast Enhancement/ Segmentation	K- Means Class. 75.97% / Fuzzy C- Means Class. 76.67%	100 images taken from database FVC2004
18	Enhancing curved structures in noisy images	Normalization/O-F Estimation/ Curved Gabor Filter	EER: %11.88	FVC2004
19	Obtaining a reliable ridge orientation field/ overcoming some limits of the existing enhancement algorithm	Orientation Estimation/ Median Filter/ Morphological Filtering	AR: 85.32%	FVC2004:DB2
20	Connecting broken ridges/ Remove smears and scars /Separating falsely conglutinated ridges/ Removing the true minutiae/ Improving the contrast of low-quality fingerprint images	Normalization/ Segmentation/ Anisotropic Diffusion Filter/ Compensation Filter/ Angular Filter	Complexity Performance: 24.95s/ Objective Qualıty Measurement: 0.0065	FVC2004:DB4
21	Improving the performance of fingerprint and the accuracy of the estimation	Binarization/ Segmentation/ Gaussian Filter/ O-F Estimation/ Curved Gabor Filter	FAR Reduce 0.25% / FRR Increase 0.5%.	FVC2004
22	Enhancing the image with less computation time	Segmentation/Normalization/ Gaussian Band-Pass Filter	PSNR: 26.48db / Comp.Time: 0.8644 Secs	138 Fingerprint from 46 hetero. population
23	Enhancing fingerprint/ estimating the intrinsic properties of the fingerprint	O-F Estimate/ Contextual/ Non-Stationary Filtering	EER: %7.8 Relative Improvement : %24.6	FVC2002 DB3, NIST
24	Enhancing the true minutiae point/ Remove the wrong minutiae	Frequency Estimate/ Gabor Filter/ Gaussian Filter/ Thinning	Better Perfor. Comp. to Prev.Works	FVC2004/ FVC2002:DB1
25	Overcoming the limitations of traditional gabor filter/ Promote fingerprint enhancement Performance/ Reduce the comp. cost/ Extract the frequency spectrum for each block	O-F Estimate/ Log-Gabor Filter	Total Error Rate Is Less Than 5.3% in FVC2004 DB2/ Total Error Rate Is Less Than 4.8 % in FVC2004 DB4	FVC2004:DB2/ FVC2004:DB4
26	Extracting five feature from fingerprint/ Analyzes image quality with clustering method using ward's algorithm	O-F Estimation/ Adaptive Filter/ Thinning	Exec. Time:0.553 s/ Genuine Accept Rate 96% at in 10% FAR	NIST DB4/ Collected dataset at India University
27	Overcome unwanted defects fingerprint recognition system	Orientation Estimate/ Directional Low pass Filter/ Binarization	Executive Times: 0,540 s	FVC2000
28	Propagating good spectra of enhanced ridges to lower-quality regions.	Segmentation/ Normalization/ Gaussian-Matched Filter/ Binarization	Average Equal Error Rate In 8 Out Of 15	FVC2000-2002-2004-2006
29	Enhancing feature extraction for low-quality fingerprint images by adding noise to the original signal	-	EER with no Enhancement: 6.55%/ Histogram Equal.: 6.15 %/ SR Enhancement: 5.03%	FVC2004 DB2
30	Enhancement fingerprints in a dark and noisy background	Normalization/ Quadratic Filter	SNR: 2-4 Db	100 test fingerprints
31	Patching of pore holes in the ridges/ Joining discontinuous ridges	Contrast Stretching/ Histogram Equalization/ Binarization/ Segmentation/ FFT/ Averaging Filter	Coloration: 0.5510/ PSNR: 52.8905	VeriFinger Database

In study of Hu et al used the Gabor Filter and STFT together. So they have been observed that it is powerful in improving the low quality fingerprints, creating a more clearly, increasing the accuracy of minutiae extraction and matching [10]. In study of Choomchuay et al. used directional filter including the second derivative of a Gaussian filter and the pyramid technique. It has been observed that it is smoothed the image with this approaches and increased success of true core point detection [11].

In study of Yuanyuan proposed an elliptical Shape Gabor Filter, which is completed successfully via estimating the degree of curvature and the frequency of fingerprint ridge in local areas. Thereby, it has been observed that it is avoided the block effect, achieved the high accuracy rate, get correct and more precise enhancement [40]. In study of Kabir et al used the anisotropic diffusion filter, the compensation filter and the angular filter. It has been observed that it can connect broken ridges, remove smears and scars, separate falsely conglutinated ridges, recover the true minutiae and improve the contrast of low-quality fingerprint images [20].

C.Post Processing Techniques

Post-processing step used to extract the minutiae more easily and quickly can be defined as conversion operation on enhanced image. This process is also defined as the final stage of the improvement of the fingerprint images and is performed after applying pre-processing and pre-adjusting. There are many different approaches for post-process. One or more of these approaches may be used in this phase. The studies show that; even if it has been cleaned and improved, processing of a gray level fingerprint image is very difficult to find minutiae. To be able to perform image analysis more easily and quickly, it is necessary to apply post processing. Thereby performance of minutiae extraction is improved. When the examined studies are summarized the following headings have been obtained. These are [9-31]:

Binarization: Binarization is a procedure that converts gray scale images into binary images. After binarization, each pixel of the gray scale images is assigned to be either black or white, which are expressed, by ridge and valleys. While a fingerprint image is obtained, the image can be obtained at a binary level or a gray level. If images are scanned at the binary image and then extracted minutiae, it may have a loss of data since gray level images have more information than binary images. This causes spurious minutiae to be extraction and the system performance to be decreased. If the correct threshold which is adapts value to the average local intensity is used, applying binarization can be improved the system performance and be extracted the correct minutiae. However, the processing time in gray ones is longer than that in binary ones [9,14,16,21,27,28,31]

Yun et al. have been applied binarization in preprocessing. They offer more effective in terms of the processing time since gray level image have more information than binary image. However, converting binary image without enhancement causes many spurious minutiae and also removes many important features [26]. In study of Saeed et al. they have performed binarization by using a threshold close to the whitish gray color. Their experimental results show that; their approaches quite competitive according to other method, which is, consist of binarization [16]

Thinning: Thinning is defined as reduction the width of ridges to one pixel in order to obtain the skeletons of fingerprint ridges. The aims of the process are to maintain the connectivity of the original shape including the position, direction and length of lines, to make more easily the extraction of minutiae and to increase the reliability of minutiae. It is important to develop thinning algorithm without generating spurious. The basic components to be considered at this stage; it should not generate spurious minutiae, ridge connectivity should be ensured, pixel should be convergences to unit width, computational cost should be reduced [13,14,16,24,26,32].

In study of Ahmed et al. it has been proposed rule-based approaches for thinning. This approaches guarantees symmetrical thinning with high speed however, it does not give a good result for 2-pixel line [41]. Guo et. al have developed an iterative algorithm known as Zhang-Suen's Algorithm. While preserving to belong to the skeleton, it removes all the contour points of the image. However it is ineffective in terms of preserving patterns that have been reduced to 2x2 and after thinning operation cannot guarantee curve [42].In study of Chen et al. They improved to Zhang-Suen's Algorithm. Their experimental results show that; they have overcome problems of Zhang-Suen thinning algorithm. But this algorithm cannot remove to the acute Angle at the line produced by redundancy line [43]. In literature, it is noted that Zhang-Suen's algorithm is the most preferred thinning algorithm compared to other thinning algorithms. But using this algorithm alone does not give the desired result. Thus it is important that modified and improved of this algorithm is used.

IV. CONCLUSION

In this study, use of fingerprints for identification, collection and analysis of fingerprints at the crime scene, techniques and methods of fingerprint enhancement and the steps used in enhancement process were reviewed. Regarding the results obtained in the reviewed studies:

- Three different types of material evidence are collected from the crime scene. These are biological evidence, biometric evidence and inanimate evidence.
- Fingerprint is biometric evidence and has five basic features. These are universality, distinctiveness, permanence, collectability, and performance. By taking advantage of these features, fingerprint is analyzed whether the fingerprint belongs to the person.
- Fingerprints obtained from crime scene are divided to three classes. These fingerprints types are; plastic finger-

prints, visible fingerprints and latent fingerprints.

- Each type of fingerprint is collected from crime scene with different techniques and methods, after that it is transferred to digital media.

- Fingerprints collected from crime scene are evaluated by image enhancement techniques for use in recognition process.

- Image enhancement techniques are performed in three steps. These are preprocessing, post processing and adjusting. All of these steps do not have to be applied, some of them can be applied alone or some of them can be applied in different combinations.

- The studies conducted between 2007-2017 have been examined and it is seen that; image enhancement techniques are divided into sub-steps themselves. During the pre-processing period, normalization, histogram equalization, contrast stretching and segmentation operations can be applied. In the adjusting process; filtering, orientation and frequency estimate operations can be applied. Finally; during post processing; thinning and binarization operations can be applied.

- It has been observed that the data sets used in the studies performed are generally the same. This situation can lead to the similarity of the results. In the studies to be developed, success rates obtained in different data sets should be emphasized.

- There is no obligation to use all the techniques and methods used to improve the image. It is seen in the studies examined that some of these methods have been used in different combinations.

- Every technique in examined studies has been used to achieve a different purpose. Table 1 shows that; the success criterion obtained from studies does not have a single standard. In order to define success rate achieved in the studies; some terms are used such as compression rate, EER, true core points, orientation extraction, complexity performance, objectıve quality measurement, FAR, FRR, executive times, SNR etc.

- There have been available a few studies interested in image enhancement. Because fingerprints detection mechanism is really one of the most difficult and important process for crime scene investigation.

The contribution of this paper is to review the most recent image enhancement techniques and some solutions according to the literature. This study also contributes the authors who want to study image enhancement methods by providing them a comprehensive analysis of used methods. System and application developers can also benefit from our conclusions while developing new software.

REFERENCES

[1] Dutelle, A. W. (2016). "An introduction to crime scene investigation". Jones & Bartlett Publishers.

[2] Gruijter, M., Poot, C. J., & Elffers, H. (2016). "The influence of new technologies on the visual attention of CSIs performing a crime scene investigation." Journal of forensic sciences, 61(1), 43-51.

[3] Fisher, B. A.. "Techniques of crime scene investigation." http://index-of.co.uk/Tutorials 2/Techniques% 20of%20Crime %20Scene%20Investigation.pdf, accessed July 2, 2017..

[4] Jain, A. K., Nandakumar, K., & Ross, A. (2016). "50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters", 79, 80-105.

[5] Öznur Sinem Sönmez, S. Ö. (2008). "Computer-Aided Fingerprint Recognition System" Master thesis, Istanbul University Graduate School of Science, Istanbul.

[6] Anonymous "A Simplified Guide to Crime Scene Investigation",http://www.forensicsciencesimplified.org/csi/CrimeSceneInvestigation.pdf, accessed July 2, 2017..

[7] Wyatt, D. (2014). "Practising crime scene investigation: trace and contamination in routine work". Policing and Society, 24(4), 443-458.

[8] Sağıroğlu, Ş, & Özkaya, N. (2006). "New Approaches For Pre-Processıng Operatıons Of Automatıc Fıngerprınt Identıfıcatıon And Verıfıcatıon Systems" Journal of The Faculty of Engineering and Architecture of Gazi University, 21(1),11-19.

[9] Saravanan, C., Malalur, S. S., & Manry, M. T. (2009, December). "Fingerprint Feature Compression Using Statistical Coding Techniques". In India Conference (INDICON), 2009 Annual IEEE (pp. 1-4). IEEE.

[10] Hu, Y., Jing, X., Zhang, B., & Zhu, X. (2010, March)." Low quality fingerprint image enhancement based on Gabor filter". In Advanced Computer Control (ICACC), 2010 2nd International Conference on (Vol. 2, pp. 195-199). IEEE.

[11] Choomchuay, S., & Sihalath, K. (2010, June). "An application of second derivative of Gaussian filters in fingerprint image enhancement". In Bioinformatics and Biomedical Engineering (iCBBE), 2010 4th International Conference on (pp. 1-4). IEEE.

[12] Wang, J., & Sun, X. (2010, July)." Fingerprint image enhancement using a fast Gabor filter". In Intelligent Control and Automation (WCICA), 2010 8th World Congress on (pp. 6347-6350). IEEE.

[13] Khan, M. A., Khan, A., Mahmood, T., Abbas, M., & Muhammad, N. (2010, June). "Fingerprint image enhancement using Principal Component Analysis (PCA) filters". In Information and Emerging Technologies (ICIET), 2010 International Conference on (pp. 1-6). IEEE.

[14] Zhang, X., Gong, X. C., Sun, Z. X., & Sun, L. M. (2010, October). "A novel algorithm for fingerprint orientation extraction and image enhancement based on Gabor filters". In Image and Signal Processing (CISP), 2010 3rd International Congress on (Vol. 4, pp.

[15] Liu, J. B., Wang, S., Li, Y., Han, J., & Zeng, X. Y. (2010, November). "Configurable pipelined Gabor filter implementation for fingerprint image enhancement". In Solid-State and Integrated Circuit Technology (ICSICT), 2010 10th IEEE International Conference.

[16] Saeed, A., Tariq, A., & Jawaid, U. (2011, July). "Automated system for fingerprint image enhancement using improved segmentation and Gabor wavelets". In Information and Communication Technologies (ICICT), 2011 International Conference on (pp. 1-6). IEEE.

[17] Balti, A., Sayadi, M., & Fnaiech, F. (2011, March). "Segmentation and enhancement of fingerprint images using K-means, fuzzy C-mean algorithm and statistical features. In Communications", Computing and Control Applications (CCCA), 2011 International Conference.

[18] Gottschlich, C. (2012). "Curved-region-based ridge frequency estimation and curved Gabor filters for fingerprint image enhancement". IEEE Transactions on Image Processing, 21(4), 2220-2227.

[19] Wang, Y., Yu, J. P., Liu, H. W., & Zhang, P. (2011, October). "Fingerprint image enhancement based on morphological filter." In Computational and Information Sciences (ICCIS), 2011 International Conference on (pp. 34-37). IEEE.

[20] Kabir, W., Ahmad, M. O., & Swamy, M. N. S. (2013, August). "Enhancement of low-quality fingerprint images by a three-stage filtering scheme". In Circuits and Systems (MWSCAS), 2013 IEEE 56th International Midwest Symposium on (pp. 1306-1309). IEEE.

[21] Rajan, R. A., Sudha, N., & Kumar, P. A. (2013, December). "OF estimation based on curved Gabor Filter for fingerprint image enhancement." In Advanced Computing (ICoAC), 2013 Fifth International Conference on (pp. 405-412). IEEE.

[22] Dyre, S., & Sumathi, C. P. (2014, December)." Hybrid approach to enhancing fingerprint images using filters in the frequency domain". In Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on (pp. 1-6). IEEE.

[23] Chikkerur, S., Cartwright, A. N., & Govindaraju, V. (2007). "Fingerprint enhancement using STFT analysis." Pattern recognition, 40(1), 198-211.

[24] Khan, T. M., Khan, M. A., & Kong, Y. (2014)." Fingerprint image enhancement using multi-scale DDFB based diffusion filters and modified Hong filters". Optik-International Journal for Light and Electron Optics, 125(16), 4206-4214.

[25] Wang, W., Li, J., Huang, F., & Feng, H. (2008). "Design and implementation of Log-Gabor filter in fingerprint image enhancement". Pattern Recognition Letters, 29(3), 301-308.

[26] Yun, E. K., & Cho, S. B. (2006). "Adaptive fingerprint image enhancement with fingerprint image quality analysis." Image and Vision Computing, 24(1), 101-110.

[27] Çavuşoğlu, A., & Görgünoğlu, S. (2008)." A fast fingerprint image enhancement algorithm using a parabolic mask." Computers & Electrical Engineering, 34(3), 250-256.

[28] Sutthiwichaiporn, P., & Areekul, V. (2013). "Adaptive boosted spectral filtering for progressive fingerprint enhancement." Pattern Recognition, 46(9), 2465-2486.

[29] Ryu, C., Kong, S. G., & Kim, H. (2011). "Enhancement of feature extraction for low-quality fingerprint images using stochastic resonance." Pattern Recognition Letters, 32(2), 107-113.

[30] Hari, V. S., Raj, V. J., & Gopikakumari, R. (2013)." Unsharp masking using quadratic filter for the enhancement of fingerprints in noisy background." Pattern Recognition, 46(12), 3198-3207.

[31] Neethu, S., Sreelakshmi, S., & Sankar, D. (2015). "Enhancement of Fingerprint using FFT×| FFT| n Filter. "Procedia Computer Science, 46, 1561-1568.

[32] Draa, A., & Bouaziz, A. (2014). "An artificial bee colony algorithm for image contrast enhancement". Swarm and Evolutionary computation, 16, 69-84.

[33] Tang, J. R., & Isa, N. A. M. (2014). "Adaptive image enhancement based on bi-histogram equalization with a clipping limit". Computers & Electrical Engineering, 40(8), 86-103.

[34] Lai, Y. R., Chung, K. L., Chen, C. H., Lin, G. Y., & Wang, C. H. (2012). "Novel mean-shift based histogram equalization using textured regions". Expert Systems with Applications, 39(3), 2750-2758.

[35] Khan, M. A., Khan, T. M., Bailey, D. G., & Kong, Y. (2016). "A spatial domain scar removal strategy for fingerprint image enhancement." Pattern Recognition, 60, 258-274.

[36] Gupta, P., & Gupta, P. (2015, January). "Slap fingerprint segmentation using symmetric filters based quality." In Advances in Pattern Recognition (ICAPR), 2015 Eighth International Conference on (pp. 1-6). IEEE.

[37] Bian, W., Ding, S., & Xue, Y. (2017). "An improved fingerprint orientation field extraction method based on quality grading scheme." International Journal of Machine Learning and Cybernetics,pp 1-12.

[38] Ji, Luping, and Zhang Yi. "Fingerprint orientation field estimation using ridge projection." Pattern Recognition 41.5 (2008): 1491-1503.

[39] Malalur, S. S., Manry, M. T., & Narasimha, P. L. (2004, November). "A pseudospectral fusion approach to fingerprint matching." In Signals, Systems and Computers, Conference Record of the Thirty-Eighth Asilomar Conference (Vol. 1, pp. 572-576). IEEE.

[40] Yuanyuan, Z. (2012, September). "Fingerprint image enhancement based on elliptical shape Gabor filter." In Intelligent Systems (IS), 2012 6th IEEE International Conference (pp. 344-348). IEEE.

[41] Ahmed, M., & Ward, R. (2002)." A rotation invariant rule-based thinning algorithm for character recognition. "IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(12), 1672-1678

[42] Guo, Z., & Hall, R. W. (1989). "Parallel thinning with two-sub iteration algorithms." Communications of the ACM, 32(3), 359-373.

[43] Chen, W., Sui, L., Xu, Z., & Lang, Y. (2012, May)." Improved Zhang-Suen thinning algorithm in binary line drawing applications". In Systems and Informatics (ICSAI), 2012 International Conference on (pp. 1947-1950). IEEE.

[44] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

The Analysis of the Concepts of Informatics, Cyber Crimes and Computer Forensics

Prof. Dr. Asaf VAROL
Fırat University, Technology Faculty
Software Engineering Department
Elazığ, Türkiye
varol.asaf@gmail.com

Yeşim ÜLGEN SÖNMEZ
Fırat University, Technology Faculty
Software Engineering Department
Elazığ, Türkiye
yesimulgen123@gmail.com

Abstract

Informatics is a discipline that involves the whole process of storing, processing, rearranging, copying and transferring all types of data obtained from the processing of information numerically and electronically. The various devices that perform these processes are called the information system. Cybercrime is a top definition that includes the concepts of "digital crime", "electronic crime", "cybercrime", "internet crime", "hi tech crime", "computer crime" etc. Every illegal and unauthorized behavior showed by people while they are using the information systems is considered as cybercrime

Computer forensics is the whole of evidence investigation process that applies scientific technical procedures on a classical crime or a cybercrime. The possible electronic evidences are obtained on the media and then these evidences are transformed to legal electronic evidences by applying computer forensics methods. Finally, they are submitted to the judicial authorities in an understandable manner.

Index Terms

Informatics, information systems, cybercrimes, computer forensics

I. INTRODUCTION

A. Information Society

Considering human history, it is seen that there are three important and fundamental changes [1]. These are respectively; the agrarian revolution, the industrial revolution and the information revolution [1]. Human communities engaged in hunting and gathering live as nomads, living with the agrarian revolution once they start farming. [2]. The period up to the 1600s was agricultural society [3]. In Europe, the production of goods and services began with the contribution of the new inventions. The industrial revolution began in 18th and 19th centuries [4]. The period between the 1600s and the early 1900s was the industrial society period [3].

Information society has formed with information revolution. The information society use information technologies in every part of life and have easy access to information [5]. The concept of the information comes from the Latin root of "informato" and it is used to mean "formation", "formalization" and "communication" [6].

In the information societies, information is a major factor of competition and the societies that aim to become information society place greater importance on science and technology in order to maintain their stability. Transformation to information society; Not only in one department, but also in all social and institutional areas in every part of the society.

B. The Concept of Informatics and Information Systems

The word "Informatics" [7], is an academic and professional discipline that involves the whole process of storing, automatically processing, rearranging, copying and transferring all types of data that is obtained from the processing of information numerically and electronically [8, 9].

In the last century, the concept of informatics is used to mean storing, processing, organizing, assessing and transferring data that people have in many fields like technical, economic, social, cultural, legal or social life [10].

C. Computer

The definition of the computer becomes important due to the increase in cybercrimes [1]. According to a definition, the computer is an electromagnetic, optical and mechanical device that stores and processes data obtained via electromagnetic optical methods, mathematical principles and programs [11].

The computer can also be called "computer [12]", "electronic brain", "automatically processing system" [13], "regulator", "electronic machine" [10]. The common name is "systems that automatically process data in the framework of programs prepared with mathematical and logical action sequences" [14].

D. Information System

The term "system" should be understood not only in the computer but also in the various devices that enable the storage, processing, use and transmission of shelves and data [12, 15].

Although informatics and computer are sometimes used with the same meaning in teaching and practice, they do not have the same meaning. Informatics is more extensive

and includes computer [12]. Information systems involve all technologies including communications and computers that are used to collect, process, store, transmit information from one place to another via networks [16].

In the Turkish Criminal Code numbered 5237, "The information system referred, is the magnetic systems which enable the automatic process after collecting and placing data" [17]. The characteristics of information systems can be expressed as follows [16];

It is formed by the combination of many structures. One of these structures is the computer.

- Informatics has an interdisciplinary structure. It contains multiple sciences such as Mathematics, Statistics, Computer-based systems, Electronics.
- Information systems focus on solving problem. They ensure the development of practical thinking and quick decision-making.
- It prioritizes not only the improvement of a program but also its design and it forms the system.
- It is not just application-based, but it contains theory and it also allows them to be carried out in harmony.

Information systems are considered as three classes [18]. These are as below;

The first of these is open computer systems and they are desktop, portable computers and small servers used in everyday life.

The second group of information systems are communication systems. Communication systems provide more and more data transfer, while they store huge amount of data regarding the communication that can be an electronic evidence source.

Embedded information systems are the integrated systems that are formed by electronic hardware and software. The biggest difference of these systems is to perform a single task and indirectly interact with the user. Personal computers, printers, scanners, calculators, mobile phones, televisions, cameras, dishwashers, washing machines and electronic toys have these systems [19].

E.. Information Technologies

Information technology is a concept used for all information services that can be connected with communication and computer systems [19]. Therefore, this concept should not be limited to only computer hardware and software. Within the context of information technology, four main categories such as software, services, hardware and equipment can be mentioned [19].

We can classify the history of information technologies in four main periods [3, 20]. These are;

- Pre-Mechanical Age (3000 B.C. - 1450 A.D.),
- Mechanical Age (1450-1840),
- Electro Mechanical Age (1840-1940),
- Electronic Age (1940 - ….).

In the first age, human beings found the writing and created alphabets, realized new counting systems and ensured the collection of information with the books they wrote and the libraries they created [3, 20].

The Mechanical Age developed through the activation of positive sciences starting with the Renaissance period on the world stage. The distribution of information increased with the invention of the printing press. Tools that were invented by especially Blaise Pascal (1623-1662) and Gottfried Wilhelm von Leibniz (1646-1716) and then mathematical calculations were developed [20].

In the Electromechanical Age, the discovery of electricity, the Volt's battery and telegraph are major developments. Telegraph can be regarded as the historical milestone of telecommunication in today's sense. The balance between electronics and mechanics in inventions began to shift gradually towards electronics with Graham Bell's phone. Sending the sound away in 1876 with the phone followed, spreading electronic waves away with Marconi's radio invention in 1894 [20].

The period from the beginning of the 1940s up to today is the Electronic Period. The discovery of vacuum tubes and the invention of the first computer ENIAC (Electronic Numeral Integrator and Computer) in 1946, became a sign of removing from mechanics. "The computer composes the core of the modern information technology" [20].

F. Cyber Space

The cyber that is the basic word of the information age. It is the abbreviated form of the cybernetic word. The cyberspace word is derived from the word kübernetes in Greek, which means "pilot who manages the ship" or "helmsman" [21]. Cyber space covers all mechanisms within information and communication systems [3].

Cyberspace is a "globally interconnected, computer-aided, computer-accessible or computer-based, diverse, artificial or "virtual" reality [22]. The physical components of cyber space are; computers, electronic devices and the tools that provide access to the Internet. The virtual environments of cyber space are computer networks, network systems and the Internet [23].

II. THE SEPARATION OF CYBER CRIMES AND COMPUTER FORENSICS

A.. Cyber Crimes and Information Law

The word "crime" means "the unlawful act that is defined by the state in laws" [24]. Within the legal system, crimes are divided into two as crimes with legal sanctions and offences with administrative sanctions [3]. Since cybercrimes are a special type of crime separated from classical crimes in many ways, A new discipline, "information law" has emerged. This discipline will meet the new requirements.

Although cybercrime is referred to as "digital crime", "electronic crime", "cybercrime", "internet crime", "high technology crimes", "computer crime", the concept of cybercrime is a top definition covering all. Although there is not a common

definition of cybercrime, the most widely accepted definition in the international arena is the definition made by The Commission of European Economic Community (EEC) at Paris meeting in May 1983.

According to this definition, cybercrimes are illegal, unethical or an unauthorized actions in a system that processes information automatically or provides data transfer [3, 25]"

A large part of crimes in our national legal system was regulated in the Turkish Criminal Code numbered 5237 [26]. Cybercrimes were regulated in according to international law in Articles 243, 244, 245 and 246 of the Turkish Criminal Code [27, 28]. Cybercrimes are divided into two parts. One of them is "true cybercrimes" and other one is "crimes committed through information" [26].

İf the information technologies are the aim of the crime, it is "cybercrimes". If Information technology is a tool in classical crimes, it is the "the crimes committed through information" [26].

B. The Separation of Cybercrimes and Computer Forensics

Computer forensic is the resolution method of cybercrimes and it is a process that should definitely be applied in these criminal crimes [26].

Computer forensics is the whole of evidence investigation process that applies scientific technical procedures. The electronic evidences related to the crime on the media are submitted to the judicial authorities without destroying, damaging and in an understandable manner by using scientific and technology-assisted methods [26, 29]. At the end of the investigation of information devices, the identification of whether the suspect is guilty is called computer forensics [30].

With the use of information technologies in the world of crime, "information-related crimes" have emerged [31]. Figure 1 shows the separation of information-related crimes and computer forensics. Figure 2 shows the information-related crimes and legal regulation of computer forensics process. The computer forensics process was regulated under the heading "search, copy and seizure of computers, computer programs and records in Article 134 of the Code of Criminal Procedure numbered 5237 [26].

In the international area, the most comprehensive regulation on cybercrimes is the "European Cybercrime Convention" [1]. This Convention was adopted by the Committee of Ministers of the European Council on 8 November 2001 and was presented for signature at the International Conference on Cybercrimes held in Budapest on 23 November 2001 [32]. The Crime Convention that consists of four parts and forty-eight articles was signed by the European Council that has 26 member States, the United States, Japan, Canada and South Africa [32]. The Convention signed by Turkey in Strasbourg on 10 November 2010 started to be implemented, after Law No. 6533 (on the Approval of the Turkish Grand National Assembly for the Convention on Crimes committed in the Virtual Environment) was published in the 2014 official newspaper [1].

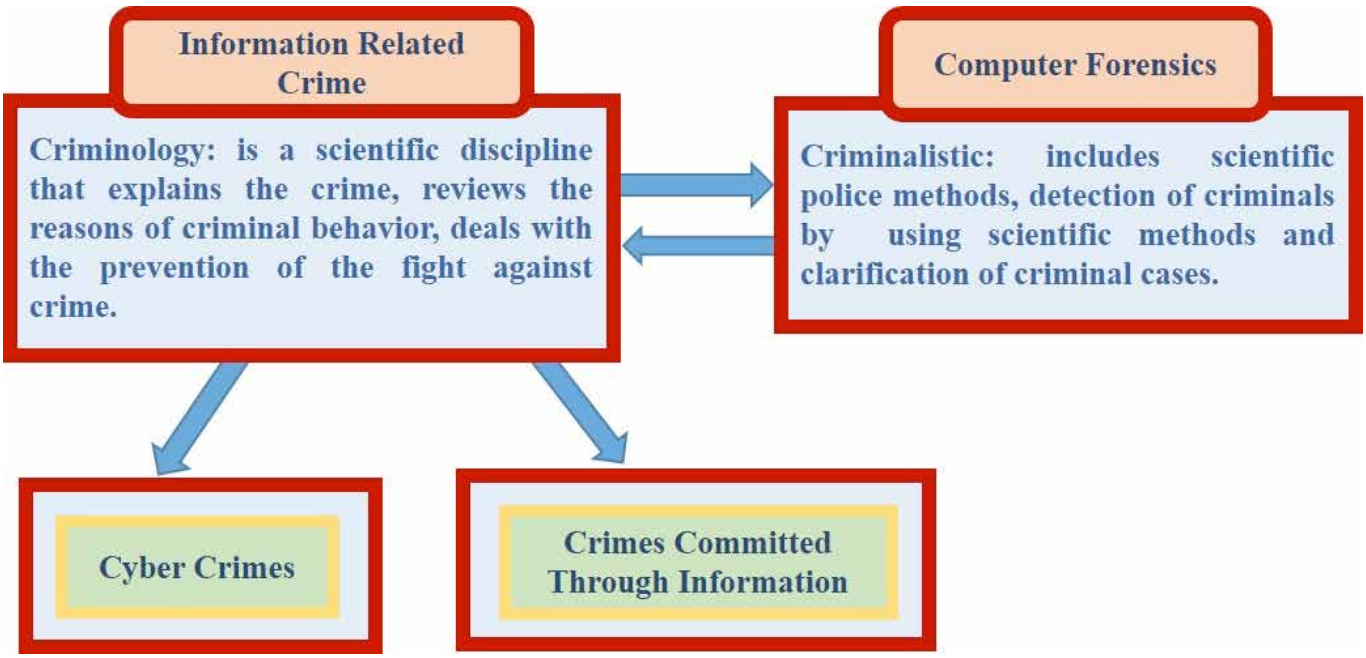


Figure. 1. The separatıon of Information-Related Crimes and Computer Forensics [26].

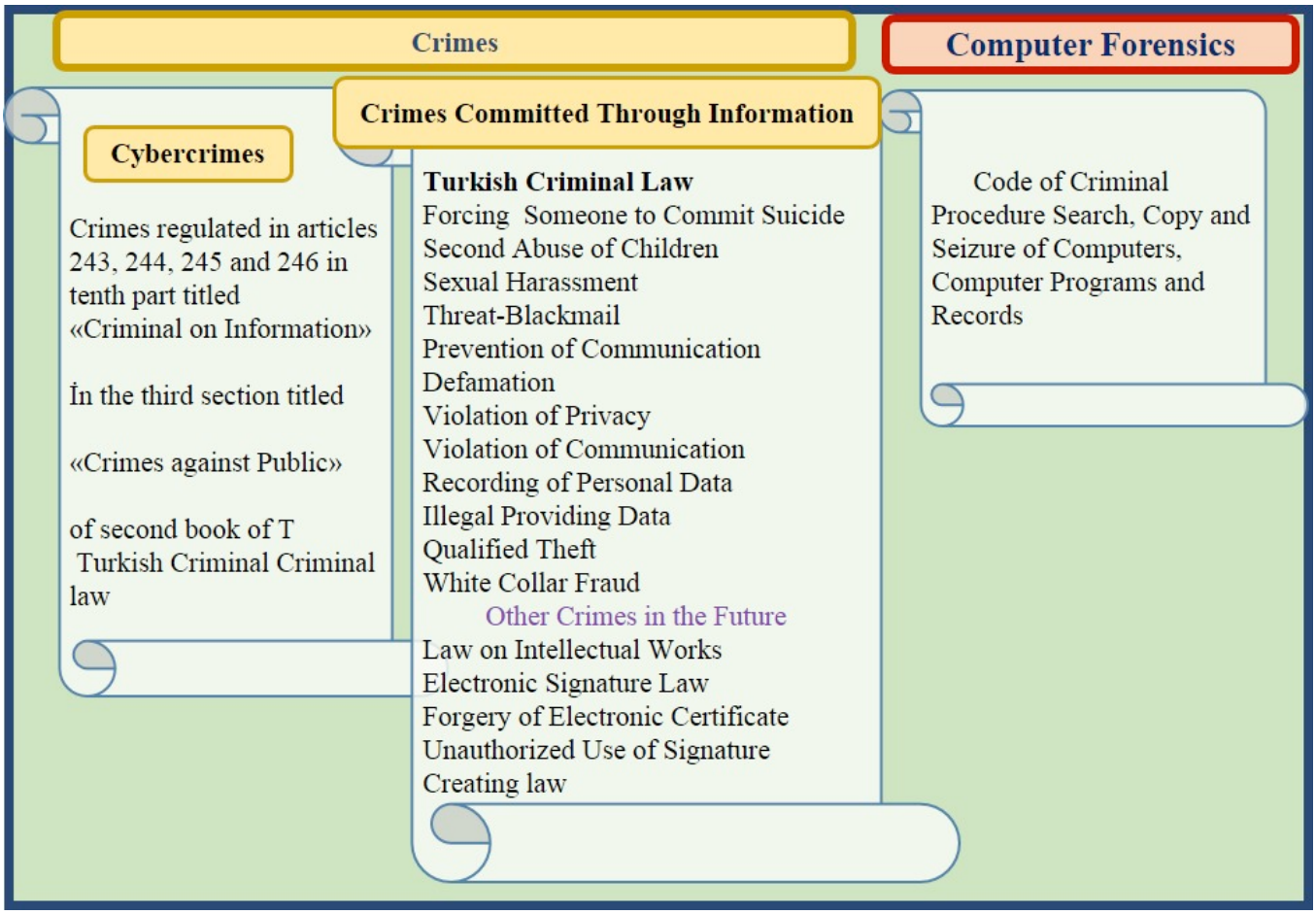


Figure 2. Legal Framework for the separatıon of Information-Related Crimes and Forensic Informatics [26].

III. COMPUTER FORENSICS SCIENCE

A. The Formation of Computer Forensics Discipline

Finding true evidences in the right ways, analyzing, reviewing and submitting them to the judicial authorities in criminal cases led to the creation various sub-sciences in the main heading of the criminal procedure law. Disciplines such as computer forensics, forensic medicine and forensic psychology can be shown as example of these sciences [33].

The original name is "Computer Forensics". This concept consists of the words "computer" and "forensics" it can be called "computer criminalistics" or "computer forensics science" [1]; but in the doctrine, the term "Computer Forensics" is predominantly preferred [30]. Therefore, computer forensics was emerged as one of the most common methods of finding evidence on computers and other electronic devices [33].

B. Computer Forensics and Information Security

Computer forensics is also considered as a subdiscipline of law and computer security under the main heading of "Information Security". This discipline can also be regarded as an approach involving forensic analysis and studies against cybercrimes, information security vulnerabilities, national security measures and computer abuses [34].

The items of information security are "privacy", "integrity", "accessibility" and "recoverability". The integrity of the information is that the information is not damaged. Accessibility is the ability to access information when requested. Recoverability is to take precautions to replicate information when it is lost. [26, 35].

The reflection of information security in the world is "information security". Information security is based on security, privacy, reliability and availability. Safety and usability are inversely proportional [36].

C. Purpose of Computer Forensics

The main purpose of computer forensics is collection, analysis and submission of legal electronic evidences [34, 37]. The purpose of computer forensics is not to show any person guilty or innocent, but to submit numerical evidences in full and impartial manner to forensic units. From this point of view, computer forensics is a completely technical review method, although it does not involve a commentary activity [34]. The interpretation of the evidences and the determination of whether a person is guilty or not is obtained after computer forensics processes [33].

D. Computer Forensics Process

The processes that should be followed, finding electronic evidence in order to obtain a legal evidence in computer forensics is called "the phases of computer forensics". Without following these phases, electronic evidence is not used to solve the concrete case and to clarify the material facts before the judicial authorities [1].

The phases of computer forensics shown in Figure 3 are as follows [30, 33]. It starts with Identification of the evidence in the crime scene investigation,

- Collection of evidence
- Protection of evidence
- Analysis of evidence
- Reporting and submission of the evidences.

Figure. 3. Computer forensics loop model [1].

IV. CONCLUSION

The computer, information, cybercrime and computer forensics have different contents. The rapid development of information systems, including computers, revealed the concepts of cybercrime and information law. These terms are new. Their content is constantly changing and improving. This study can be helpful for researchers that work in fields like information law, law enforcement agencies, computer forensics and academy.

This paper will be useful to reveal the separation of these concepts, scientifically and can increase the speed of scientific studies and give ideas who will work in these fields.

A statistical research can be done to detect how many people know the differences of informatics, cybercrime and computer forensics terms.

REFERENCES

[1] M. Orta, Bilişim Suçlarında Adli Analiz, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, 2015.

[2] İ. Ortaş, "Bilgi Toplumuna Geçiş ve Sorunları," [Online]. Available: Çukurova Üniversitesi, http://turkoloji.cu.edu.tr/GENEL/ibrahim_ortas_bilgi_toplumuna_gecis _ve_sorunlar.pdf. [Access: 20. 10. 2016].

[3] M. Gözüşirin, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Ankara: Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2011.

[4] Ü. Acar and Ö. URHAL, Devlet Güvenliği İstihbarat ve Terörizm, Adalet Yayınevi Hukuk Yayınları Dizisi:205, Birinci Baskı, 2008, pp.96.

[5] O. Değirmenci, Bilişim Suçları, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2002, pp. 24.

[6] R. Balay, "Küreselleşme, Bilgi Toplumu ve Eğitim," Ankara Üniversitesi Eğitim Fakültesi Dergisi, cilt 37, no. 2, pp. 66, 2004.

[7] V. Ö. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu," DEÜHFD, cilt 9, no. Özel Sayı, pp. 1023, 2007.

[8] C. Yenidünya and O. Değirmneci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul: Legal Yayıncılık, 2003, pp. 27.

[9] A. İ. Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)," GÜHFD, cilt XIV, no. 2, pp. 277, 2010.

[10] B. Akbulut, "Bilişim Suçları," SÜHFD, Milenyum Armağanı, cilt 8, no. 1-2, pp. 545, 2000.

[11] A. Koltuksuz, "Adli Bilişimde Olay Yeri İnceleme Esasları," Bilişim Hukuku Konferansı, Ankara, 09-10 Ekim 2008.

[12] E. Artuk, A. Gökçen and C. Yenidünya, Ceza Hukuku Yeni Hükümler, Adalet Yayınları, 2015, pp. 826.

[13] Ö. Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul: Filiz Kitabevi, 1994, pp. 504.

[14] D. Soyaslan, Ceza Hukuku Özel Hükümler, Ankara: Yetkin Yayınları, 2014, pp. 607.

[15] Y. Yazıcıoğlu, Bilgisayar Suçları 97, Alfa Yayınları, 2014, p. 224.

[16] "Bilişim Enstitüsü Bilişim Sistemleri," [Online]. Available: http://be.gazi.edu.tr/posts/view/title/bilisim-sistemleri-98744. [Access: 25 10 2016].

[17] İ. Özgenç, Türk Ceza Kanunu Gazi Şerhi, Genel Hükümler, Ankara: Seçkin Yayınları, 2006, pp. 987.

[18] Y. Uzunay, "Dijital Delil Araştırma Süreci," http://slideplayer.biz.tr/slide/1918963/, Ankara, 2005.

[19] "Elektrik Port," [Online] Available: http://www.elektrikport.com/teknik-kutuphane/gomulu-sistem-nedir/. [Access: 10 10 2016].

[20] M. Mahoney, "The History Of Computing In The History Of Technology," [Online] Available: http://www.princeton.edu/~hos/mike/articles/hcht.pdf.. [Access: 23 09 2009].

[21] T. Akman, Sibernetik Dünü, Bugünü, Yarını, İstanbul: Kaknüs Yayınları, 2003.

[22] L.-E. Janlert, "The Idea Of Syberspace19.8.2009.," [Online]. Available: http//www8.cs.umu.se-/kurser/TDBD07/.../The%20idea%20of%20cyberspace.pdf. [Access: 19 08 2009].

[23] H. Çakmak and T. Altunok, "Suç, Terör ve Savaş Üçgeninde Siber Dünya," Ankara, Barış Platin Kitabevi, 2009, pp. 23-55.

[24] Büyük Türkçe Sözlük, "Suç", Türk Dil Kurumu.

[25] L. Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması, Ankara: Seçkin Yayınları, 2005.

[26] H. Akarslan, Bilişim Suçları Bilişim Yoluyla İşlenen Suçlar Ve Adli Bilişim Ayrımı, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2011.

[27] F. Nacar, Avrupa Birliği Ülkeleri Ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları, Ankara: Atılım Üniversitesi Sosyal Bilimler Enstitüsü, 2010.

[28] M. Ketizmen, Türk Ceza Hukuku'nda Bilişim Suçları, Cybercrimes in Turkish Criminal Law, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

[29] A. H. Ekizer, "Adli Bilişim (Computer Forensics)," [Online]. Available: http://www.ekizer.net/content/view/16/1/. [Access: 14.10.2016]

[30] L. Keser Berber, Adli Bilişim, Ankara: Yetkin Yayınlar, 2004.

[31] "UNODC – United Nations Office on Drugs and Crime," Computer Related Crime 2005. Available: http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf. [Access: 06 10 2016].

[32] M. Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği," MHFD, cilt 19, no. 2, pp. 1229–1269, 2013.

[33] M. Özen and G. Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)," Ankara Barosu Dergisi, 2015.

[34] Ş. Sağıroğlu and M. Karaman, "Adli Bilişimi," Telepati Dergisi, no. 203, pp. 62, 2012.

[35] B. Güngören, "Bilgi Güvenliği Nedir?," 2008. [Online]. Available: http://www.emo.org.tr/ekler/1440ca9ca2c5e0b_ek.pdf?dergi=2. [Access: 03 10 2016].

[36] K. Burlu, Bilişimin Karanlık Yüzü, Ankara: Nirvana Yayınları, 2010.

[37] Y. Kim and K. J. Kim, "A Forensic Model on Deleted-File Verification for Securing Digital Evidence," 978—1-4244-5493-8710 IEEE, 2010.

Siber Savunma Tatbikatları: Planlama, Uygulama, Değerlendirme

Cyber Defense Drills : Planning, Implementation and Evaluations

Ensar Şeker
NATO CCD COE
ensar.seker@ccdcoe.org

Özet

Siber savunma tatbikatları, siber güvenlik bilinirliliğini arttırmak, siber alanda meydana gelebilecek olası farklı senaryolarda nasıl hareket edilmesi gerektiği konusunda gerekli ortamın oluşturulması, ve konuyla ilgili uzmanların uygulamalı olarak eğitimleri açısından bakıldığında çok önemli bir araçtır. Söz konusu tatbikatlar siber alanda alınabilecek önlemler konusunda karar vericilere ve bu alan için geliştirilebilecek araçlar, teknikler ve prosedürler konusunda siber savunma ile görevli veya ilgili kurum, kuruluş, ve personele de fikirler verebilmektedir. Siber savunma tatbikatlarında gerçeğe en yakın şekilde oluşturulan senaryolarla özellikle siber saldırılar ile karşı karşıya iken özellikle stress altında en iyi kararları verebilme ve takım olarak koordineli hareket edebilmenin zorunluluğunu beraberinde getirerek çok önemli katkılar sağlamaktadır. Bu makalenin amacı uluslararası siber savunma tatbikatları göz önünde bulundurularak ve karşılaştırılarak bu tatbikatların planlama, uygulama ve değerlendirme aşamalarını ortaya koyarak konuyu bilimsel açıdan ele almaktır. Çalışmanın bir diğer amacı ise söz konusu süreçler her ne kadar yapılması planlanan tatbikatın hedef kitlesine göre farklılıklar arz etse de, türüne bakılmaksızın genel bir siber savunma tatbikatında olması gerekli süreçleri de ortaya koyabilmektir.

Anahtar Kelimeler

Siber savunma, siber tatbikat, siber tehdit, siber güvenlik.

I. GİRİŞ

Siber alan kara, deniz, hava ve uzaydan sonra beşinci savaş alanı olarak kabul edildiğinden beri özellikle ulusal güvenlik açısından kritik derecede önem arz etmeye başlamıştır. Siber saldırıların anonim olarak gerçekleştirilebilmesi, reddedilebilirliliği ve diğer alanlara nispeten gerçekleştirilen faaliyetlerin daha düşük maaliyetlerde olması, bu saldırıları son zamanlarda daha popüler hale getirmiştir. Öyleki ülkeler, basit seviyede gerçekleştirilen siber saldırılar bir kenara, çok ileri seviyede teknoloji ve sofistike düzeyde siber silahlar geliştirmeye ve kullanmaya başlamışlardır.

Ulusal güvenliğin ayrılmaz bir parçası haline gelen siber saldırılara karşı ülkeler, kritik alt yapılarla, kamunun ve toplumun dijital güvenliğini koruma altına alabilmek adına, siber savunma komutanlıkları, ulusal siber olaylara müdahale ekipleri ve diğer bilgi güvenliği merkezleri gibi otoriteleri kurmaya ve yaygınlaştırmaya, yine bu sebeple ulusal siber güvenlik stratejileri geliştirmeye ve uygulamaya koymaya başlamışlardır.

Siber savunma konusunda kurum, kuruluş yada ülkelerin teknik kapasitelerini test etme, gerekli bilinçlendirmeyi ve eğitimleri sağlaması açısından siber savunma tatbikatları çok önemli rol oynamaya ve tüm dünya genelinde yaygınlık kazanmaya başlamıştır. Siber savunma tatbikatlarının başlıca amaçları arasında [1, 2, 3, 4];

- Ulusal bazda meydana gelebilecek siber saldırılara karşı ortak ve koordineli, teknik ve stratejik hareket kabiliyetini test etme ve geliştirebilme,
- Uluslararası bazda meydana gelebilecek siber saldırılara karşı ortak ve koordineli, teknik ve stratejik hareket kabiliyetini test etme ve geliştirebilme,
- Siber güvenlik yetenekleri ile devamlılık ve süreklilik süreçlerini test etme ve geliştirebilme,
- Siber savunma alanında kamu ve özel sektör arasında işbirliği ve koordinasyonu güçlendirme,

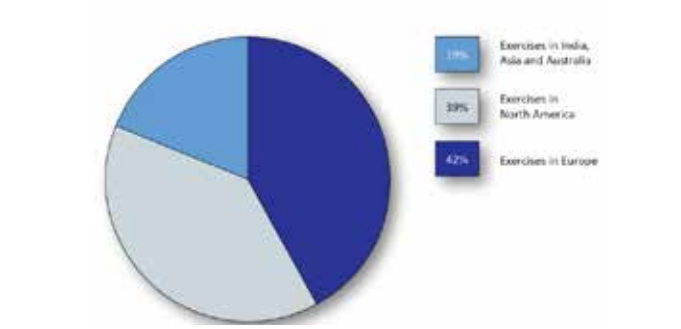
sayılabilir.

İlerleyen bölümlerde dünya genelinde siber savunma tatbikatları, bu tatbikatlarin süreçleri, türleri ve katkıları güncel senaryo ve örneklerle incelenmiştir.

Söz konusu tatbikatlar planlama aşamasından uygulama ve nihai olarak değerlendirme aşamasına kadar hem tatbikat planlayıcılarına hem de katılımcılarına konuyla ilgili önemli katkılar sağlamaktadır. Tatbikat ile ilgili bu süreçlerin incelenmesi gerçekte planlamak istenen siber savunma mekanizmaları için de fikir verebilmektedir.

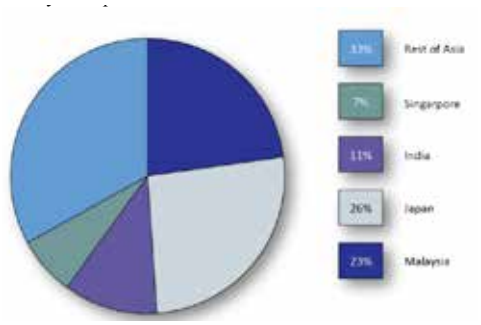
II. DÜNYA'DA SİBER SAVUNMA TATBİKATLARI

Siber savunma tatbikatları alanında en büyük oyuncuların başında Avrupa gelmektedir. Geçtiğimiz senelerde dünya genelinde gerçekleştirilen siber savunma tatbikatlarının yüzde 42'si şekil 1'de de görülebileceği üzere Avrupa kıtasında gerçekleştirilmiştir.



Şekil 1 – Siber Savunma Tatbikatlarının Dünya Genelinde Dağılımı [5]

Siber Savunma Tatbikatları alanında en az Avrupa kadar önemli bir diğer aktör özellikle ABD'nin başını çektiği Kuzey Amerika kıtasıdır. Bunların içinde Japonya, Malezya, Hindistan, ve Singapur'un başı çektiği Asya ve sonra Avusturalya takip etmektedir.



Şekil 2 - Siber Savunma Tatbikatlarının Asya Genelinde Dağılımı [5]

Şekil 2'de Asya kıtasında gerçekleştirilen siber savunma tatbikatlarının güncel dağılımı şekil 2'deki gibidir. Asya kıtasında Japonya'dan sonra özellikle Malezya'nın son yıllarda bu alana yapmış olduğu yatırımlarla ikinci sıraya yükselmesi dikkat çekicidir. Japonya ve Malezya'nın oranları her ne kadar birbirine yakın olsada Japonya'nın Malezya'dan çok daha uzun süredir siber savunma tatbikatlarına ağırlık verdiği ve dolayısı ile Malezya'dansa bu alanda çok daha fazla tecrübeye sahip olduğu muhakkaktır [5].

Uluslararası boyutta gerçekleştirilen birkaç siber savunma tatbikatına örnek olarak Locked Shields, Cyber Coalition, Cyber Europe u verebiliriz.

• Locked Shields: Locked Shields (Kilitli Kalkan) siber savunma tatbikatı, merkezi Talin, Estonya'da bulunan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (NATO CCD COE) tarafından yıllık organize edilmekte ve dünyanın en geniş katılımlı ve birçok otoriteye göre en karmaşık ve ileri teknolojilerine sahip siber savunma tatbikatı olarak kabul edilmektedir. 2017 Locked Shields tatbikatına, tüm dünya genelinden 900'den fazla siber güvenlik uzmanı dahil olmuş olup, 20 ülkenin ulusal takımı katılım sağlamıştır. 3000'den fazla sanal sistemin yer aldığı tatbikatta ulusal takımlara (mavi takımlara) kırmızı takım tarafından 2500'den fazla saldırı gerçekleştirilmiştir. Yeni gelişen bilişim teknolojilerini adapte etme konusuda başarlı bir rota izleyen Locked Shields siber savunma tatbikatları, 2017 yılında diğer yıllardaki tatbikatlardan farklı olarak akıllı şebeke sistemleri, hava üssü yakıt tesis sistemleri, drone kontrol sistemlerini de senaryolara dahil etmiş ve mavi takımların sorumlulukları arasına diğer sistemlerin yanında bu özel sistemlere eklenmiştir [6].

• Cyber Coalition: Cyber Coalition (Siber Koalisyon) siber savunma tatbikatı, NATO tarafından yıllık olarak organize edilmektedir. Üç günlük süren etkinliğe, NATO üyesi ve ittifak ülkelerden katılım gerçekleşmektedir. 2016 yılı Aralık ayında gerçekleşen tatbikata 700'den fazla siber savunma ve hukuk uzmanı, hükümet yetkilileri, subay, akademisyen ve endüstri temsilcileri katılım göstermiştir. Tatbikatta, Cezayir, Avusturya, Finlandiya, İrlanda, Japonya ve İsveç gibi NATO üyesi olmayan ülkelerin temsilcileri gibi Avrupa Birliği'nden siber savunma personeli de yer almıştır [7].

• Cyber Europe: Cyber Europe (Siber Avrupa) bir Avrupa Birliği kurumu olan ENISA (European Union Agency for Network and Information Security) tarafından 2 yılda bir Avrupa Birliği üyesi ülkeler için düzenlenmektedir. Locked Shields ve Cyber Coalition gibi askeri temelli tatbikatlardan farklı olarak sivil bir otorite tarafından organize edilmektedir. 2016 yılında gerçekleştirilen tatbikata 28 Avrupa Birliği üye ülkesi ve Avrupa Birliği üyesi olmamasına rağmen 2 EFTA (the European Free Trade Association) üyesi ülke dahil olmuştur [8].

III. SİBER SAVUNMA TATBİKATLARI TAKSONOMİSİ

Siber savunma tatbikatları çeşitli formlarda gerçekleştirilebilmektedir. Elde edilmek istenen veri setine göre, bu tatbikat türleri farklılık göstermektedir. Bununla birlikte söz konusu farklılıklar uluslararası bir standart olan ISO 22398'den gelen parametrelere dayanmaktadır. Siber savunma tatbikatlarını amaçları doğrultusunda karakterize ederken, aşağıdaki dört kategoriyi takip etmek mümkündür [9].

1.Siber yeteneklerin geliştirilmesi.

2.Bireylerin, organizasyonların ve sistemlerin siber yeteneklerinin değerlendirilmesi.

3.Bilgi, yetenek, dayanıklılık ve/veya teknik kapasitenin ölçülmesi.

4.Katılımcıları eğitilmesi ve bilgi, anlama ve beceri kazanma fırsatının sağlanması.

Şekil 3 – Türlerine göre Siber Savunma Tatbikatları [10]

Oluşturulabilecek tüm farklı tatbikat türlerine (capture the flag, discussion based game, simulation, workshop, drills, seminar gibi) karşın, siber savunma tatbikatları temelde 3 kategoriye ayrılabilir [11].

• Masa Üstü (Table Top) Tatbikatlar: Tüm senaryo/alt senaryolar, enjeksiyonlar ile kırmızı takım saldırıları tatbikat öncesinde yazılmıştır ve hazırdır. Çoğu durumda tatbikat planlayıcıları ve oyuncuları bir masaya oturup tatbikatı uyguladığından bu tür tatbikatlar masa üstü tatbikatları adını almıştır. Masa üstü tatbikatları oldukça sınırlı sayıda bir eğitim kitlesine ve çok iyi tanımlanmış amaçlara sahip olmalıdır [12]. Diğer tatbikat türlerine göre daha hızlı ve kısa sürede planlanabildiği gibi uygulama süreci de nispeten daha kolaydır.

• Karma (Hybrid) Tatbikatlar: Tatbikat senaryo/altsenaryolar ve enjeksiyonlar önceden yazılmış fakat kırmızı takım saldırılarını tatbikat sırasında canlı olarak ifa etmektedir. Tatbikat planlayıcıları, gerçek olayları önceden belirlenmiş hedeflere göre uygulayan bir kırmızı takım ile birlikte tatbikatı gerçekleştirirler [13].

• Tam Canlı (Full Live) Tatbikatlar: Bu tür tatbikatlarda her ne kadar ana senaryo ve bazı alt senaryolar önceden hazırlanmış olsada takımların gidişatı ve startejilerine göre ilgili takımlarca (genellikle beyaz takım) anlık senaryolar ve enjeksiyonlar geliştirilmekte, kırmızı takım ise mavi takımın savunma kapasitesi ve durumuna göre yeni saldırı stratejileri üretmektedir. Diğer siber savunma tatbikatlarına göre planlama süreci çok daha uzun bununla birlikte gerçek hayatta meydana gelebilcek senaryolara göre daha gerçekçidir [14].

IV. SİBER SAVUNMA TATBİKATLARI YAŞAM DÖNGÜSÜ

Bir siber savunma tatbikatı için genel olarak yaşam döngüsü şu dört aşamadan oluşmaktadır [15];

1. Tanımlama: Katılımcı profilini tanıma ve oluşturma, tatbikat türü ve büyüklüğünü belirleme, mevcut senaryo opsiyonlarını değerlendirme gibi konuları içerir.

2. Planlama: Finansal kaynakların temin edilmesi, tatbikat takvim ve yerinin ayarlanması, rollerin dağıtılması ve gerçekçi bir senaryonun oluşturulması, tatbikat materyallerinin hazırlanması, tatbikatta görev alacak kişilerin ve takımların görevleri ile ilgili bilgilendirilmesi ve eğitilmesi, medya politikasının belirlenmesi, gözlemci ve medya mensuplarının davet edilmesi konularını içerir.

3. Uygulama: Tatbikatın belirlenen çerçeve ve kurallar içinde en düzgün şekilde tatbik edilmesi, senaryo ve enjeksiyonların belirlenen sıraya göre uygulanması, meydana gelebilecek aksaklık ve sorunların en kısa ve hızlı bir biçimde çözüme kavuşturulması, katılımcıların gözlemlenmesi ve katılımcıların karar ve aktivitelerinin not alınması, değerlendirme aşamasını desteklemek amacıyla anket ve soruların katılımcılara yönetilmesi gibi konuları içerir.

4. Değerlendirme: Değerlendirmeyi yapacak bir grubun oluşturulmasını, katılımcılar tarafından cevaplanan anket ve soruların toplanıp, değerlendirilmesini, tatbikatta görev alanlardan gerekli bilgilerin toplanmasını, medya ve umuma sunulacak dökümanların hazırlanmasını, değerlendirmeler sonucu katılımcılarla paylaşılacak raporların hazırlanması konularını içerir.

Şekil 4 – Siber Savunma Tatbikatı Yaşam Döngüsü [13]

V. PLANLAMA

Tatbikat planlama süreci, katılımcılar, tatbikat senaryosu/alt senaryoları, enjeksiyonları, tatbikat ortamının hazırlanması ile birlikte, tatbikatın olağan seyrinde yürütme düzenini belirler. Tatbikat uygulaması ve senaryolar, katılımcı gruba ve spesifik olarak gerçekleştirilmesi istenilen hedeflere göre çeşitlilik göstermektedir. Farklı tatbikat türlerini ve herbirinin yerine getirdiği hedefleri anlamak, tatbikatın gerçekçiliğini ve etkinliğini artıracaktır.

A.Amaçların Belirlenmesi

Bir siber tatbikat, izole edilmiş bir ağ üzerinde tek başına bir etkinlik olarak ya da operasyonel bir ağ üzerinde daha geniş bir eğitim tatbikatı olarak düzenlenebilir. Planlama süreçleri benzerdir. Tatbikat planlama süreci, tatbikatın amaç ve arzulanan sonuçlarının tanımlanmasıyla başlar. Açık hedefler olmadan, planlayıcılar anlamlı bir tatbikat tasarlayamazlar. Belirlenecek bu amaçlar planlayıcıların; katılımcıların, savaş ortamı

olarak düzenlenen bir siber ortamında başarıyla çalışması ve siber tehditlere karşı savunma için gerekli yeteneklere sahip olup olmadığını belirlemek için tatbikat içindeki senaryoları açıkça yapılandırmalarını sağlar. Farklı organizasyonların, her tatbikat için bir başlangıç noktası oluşturmayı önemli hale getiren farklı rehber ilkeleri, araçları, taktikleri ve prosedürleri vardır.

•Tatbikat başlamadan önce katılımcılara sağlanan siber eğitimin etkililiğinin belirlenmesi,

•Tatbikat olay raporlarının etkinliğinin değerlendirilmesi ve tatbikat vasıtasıyla ortaya çıkarılan eksiklikleri gidermek için analiz kılavuzlarının hazırlanması,

•Tatbikat sırasında, katılımcıların zararlı faaliyetleri algılayıp gerekli karşılığı verebilme yeteneğinin değerlendirilmesi,

•Siber saldırıların operasyonel etkilerini belirleme ve bu saldırılar için gerekli kurtarma ve iyileştirme prosedürlerinin uygulama yeteneğinin değerlendirilmesi,

•Senaryo planlamasının ve uygulanmasının başarısının belirlenmesi,

•Siber güvenlik sistemlerindeki zayıflıkların açığa çıkarılması ve düzeltilmesi,

•Siber alanla ilgili politika ve prosedürlerdeki zayıflıkların açığa çıkarılması ve düzeltilmesi,

•Bir bilgi sistemini korumak ve zararlı saldırıların gerçekleştirildiği bir siber ortamda gerekli aktivitilerin gerçekleştirmesi için hangi donanımların veya yeteneklerin gerekli olduğunun belirlenmesi,

•Enjeksiyonların tatbikatın amaçlarını karşılayıp karşılamadığının belirlenmesi,

•Siber farkındalık, siber saldırılar karşısında hazır olma durumu ve koordinasyonun artırılması,

•Bilişim sistemlerinin siber saldırılar karşısında korunabilmesi ve gerekli önlemlerin alınarak en az zararla müdafaasına yönelik önceden hazırlanacak acil durum planlarının geliştirilmesi,

gibi maddeler genel olarak tüm siber savunma tatbikatları icin belirlenen ortak hedeflerdir.

B.Planlama Süreci

Şekil 5 – Planlama Süreci [10]

1)Ön Planlama Toplantısı (Initial Planning Meeting/Conference);

• Gereksinim ve koşulların belirlenmesi,

• Senaryo değişkenlerinin ve taslak senaryo tekliflerinin belirlenmesi,

• Gerekli bilgilerin toplanması ve tatbikat planlayıcıları arasında görev dağılımlarının yapılması,

konularını kapsamaktadır. Tatbikattan yaklaşık 6, 7 ay önce gerçekleşmektedir.

2)Ana Planlama Toplantısı (Main Planning Meeting/Conference);

• Personel, senaryo ve zaman çizelgesi geliştirme ve idari gereklilikler gibi lojistik ve örgütsel sorunları çözüme kavuşturulması,

• Tatbikatta kullanılacak tüm taslak belgelerin incelenip, değerlendirilmesi ve nihayete erdirilmesi,

• Nihai planlama aşamasının öncesinde injeklerin incelenmesi ve geliştirmesi,

• Tatbikatın amacına göre belirlenen görev, koşul ve standartların gözden geçirilmesi,

konularını kapsamaktadır. Tatbikattan yaklaşık 3, 4 ay önce gerçekleşmektedir.

3)Nihai Planlama Toplantısı (Final Planning Meeting/Conference);

Nihai plan toplantısı, tatbikat süreçlerini ve prosedürlerini gözden geçirmek için yapılan son toplantıdır. Bu toplantıdan sonra, tatbikatın tasarımı veya kapsamı veya destekleyici dokümantasyonu üzerinde önemli bir değişiklik yapılmamalıdır. Tatbikattan 3, 4 hafta önce gerçekleşmektedir.

4)Test Uygulaması (Test Run)

Test uygulaması, siber savunma tatbikatlarının teknik alt yapısını ve organizasyonla ilgili çıkması muhtemel sorunların tatbikat öncesinde test edilip değerlendirilmesine yönelik son hazırlık aşamasıdır. Test uygulamasında tatbikat için seçilen yerde tatbikat için kullanılacak tüm bilişim alt yapıları kurularak bu alt yapılar, tatbikat süreci sanki normal sürecinde işliyormuş gibi test edilip gözlemlenerek, tatbikat önceside olası muhtemel aksaklıkların önüne geçilmesi amaçlanmaktadır. Test uygulamasına mavi takımlar dışındaki tüm takımlardan katılım gerçekleşmektedir. Böylelikle tüm takımlar tatbikat öncesinde son durumlarını ve tatbikat işleyiş süreçlerini son kez gözden geirme şansını elde etmiş olurlar. Test uygulaması tatbikattan bir hafta önce gerçekleşmektedir.

VI. UYGULAMA

A.Takımlar

1) Mavi Takım

Bir kuruluşun bilgi sistemlerini yada tatbikat kapsamında oluşturulan sanal ortamları temsili hackerlara (kırmızı takım) karşı güvenliğini sağlamakla ve savunmakla sorumlu grup yada takımdır. Uluslararası siber savunma tatbikatlarında, mavi takımlar her bir katılımcı ülkenin kendi ülkesini temsilen oluşturduğu ulusal takımları ifade etmektedir. Mavi takım, simüle edilen saldırılara karşı;

1-verilen belli bir süre boyunca,

2-temsili savunma temelli ve operasyonel bağlamda,

3-nötr bir grup (genellikle beyaz takım) yardımıyla kurulan ve izlenen kurallara,

göre sorumlu olunan sisteme dayalı herhangi bir veri sızıntısını tanımlama ve bunları engelleme ile gizliliğin, bütünlüğün ve kullanılabilirliliğin korunması üzerine dayalı savunma yapmalıdır.

Son zamanlarda siber savunmanın ulusal ve uluslararası hukuk ve politikalar, medya, ulusal güvenlik stratejilerinin de bir parçası olması nedeniyle siber savunma tatbikatları da bu bağlamda dizayn edilmeye başlanmış ve mavi takım tarafından sadece teknik savunma yapılması siber savunma kapsamında yeterli görülmemeye başlanmıştır. Bu nedenle özellikle uluslararası siber savunma tatbikatlarına teknik senaryolara ek olarak hukuk, politika, strateji ve medya senaryoları da dahil edilmeye başlanmış, dolayısı ile mavi takımın bu konulardaki sorumlulukları da artırılmıştır.

Mavi takımın sorumlulukları arasında angajman kuralları çerçevesinde [1, 2, 3, 4], yürürlükteki kanunlara ve yönetmeliklere her zaman uyulması zorunluluk arz etmekte ve takım üyeleri tarafından alınan yada gerçekleştirilen herhangi bir yasadışı işlem kabul edilemez olarak görülmektedir. Dolayısı ile simülasyon ortamında dahi olsa mavi takım tarafından gerçekleştilen tüm eylem ve kararların mevcut kanun ve yönetmelikler göz ardı edilmeden gerçekleştirilmesi oldukça önemlidir.

Angajman kuralları içerisindeki bir diğer net kural, mavi takım tarafından kırmızı takıma, diğer mavi takımlara yada tatbikat sanal sistemlerinin alt yapılarına hiçbir şekilde saldırı yapılamamasıdır.

Mavi takım üyeleri, istenildiğinde kendi operasyonel güvenliklerine zarar vermeyecek doğru bilgileri vermelidir.

Mavi takım, tatbikat ortamı ile ilgili meydana gelen teknik sorunlarla alakalı bildirim ve taleplerini kendileri için tasarlanan web sayfası üzerinden bu konu ile sorumlu bulunan yeşil takıma iletilebilmelidir. Yeşil takım kendisine iletilen bu teknik sorunları makul olan en kısa sürede çözüme kavuşturmakla mesuldür.

Takım tarafından yapılacak tüm raporlamaların takım içindeki komuta zinciri üzerinden yapılması önemlidir.

Mavi takıma kendi araçlarını ve yazılım ürünlerini kullanma izni verilmektedir, ancak bu ürünlerin lisanslı yasal kopyalarının olması konusunda tüm sorumluluk bu takıma aittir.

'Blonde user' olarak adlandırılan ve bilinçsiz kullanıcıları temsil eden ve mavi takımların sistemlerini kullanıp, gönderilen zararlı eposta ve dosyaları açıp, zararlı linkleri bilinçsizce tıklayan bu kullanıcıların yada bu kullanıcıların kullandığı hizmet ve sistemlerin mavi takımlar tarafından engellenmesi angajman kurallarına aykırıdır. Ayrıca bu kullanıcılar tarafından mavi takıma gönderilen, kullandıkları sistemlerle alakalı teknik sorunlarla ilgili gönderdikleri taleplerin mavi takım tarafından en kısa süre içerisinde çözüme kavuşturulması beklenmektedir.

Mavi takımlara tatbikat öncesinde, tatbikat ortamı ile kullanacakları sistemlere yönelik ön bilgi aktarabilmek amacıyla internet üzerinden yapılan seminerlerle bilgi aktarımı yapılmaktadır.

2)Kırmızı Takım

Kırmızı takımın amacı, tatbikata katılan tüm mavi takımlara eşit derecede dengeli siber saldırılar gerçekleştirmektir. Bunun için kırmızı takım önceden tanımlanmış bir senaryoyu izlemekle birlikte, mavi takımın sistemlerinde daha önceden oluşturulan güvenlik açıklarını kullanma iznine sahiptir. Kırmızı takım tarafından gerçekleştirilen başarılı saldırılar, saldırının başarıyla yapıldığı mavi takımın eksi puan almasına yol açar. Kırmızı takım ve beyaz takım yakın işbirliği içirisinde çalışmak durumundadır. Kırmızı takım, tatbikat planına göre hareket ederken, her zaman beyaz takım tarafından verilen talimatlara da uymak zorundadır. Kırmızı takımın tatbikat alt yapı sistemlerine yada yeşil takım tarafından kullanılan servislere saldırması kesinlikle yasaktır. Kırmızı Takım tarafından gerçekleştirilecek tüm saldırıların tatbikat ortamının içinde kalması zorunludur. Buna sosyal mühendislik saldırıları da dahildir.

3)Yeşil Takım

Yeşil takım tatbikat altyapısını hazırlamak ve tatbikat boyunca işlevlilirliğini korumakla sorumlu olan takımdır. Bu altyapılar yönetimsel bilgisayar nodlarını tasarlama, kurma ve yönetme, sanallaştırma platformu, depolama, çekirdek ağ oluşturma gibi sistemlerle birlikte mavi takımların tatbikat sırasında savunmak zorunda oldukları sistemleri de kapsamaktadır. Söz konusu sistemlerin fonksiyonlarının tatbikat süresince sağlıklı bir şekilde çalışırlılığını sağlayabilmek adına mavi takımlar tarafından teknik sorunların çözümüne yönelik gönderilen taleplerin makul bir süre içerisinde yeşil takım tarafından çözüme kavuşturulması beklenmektedir.

4)Sarı Takım

Sarı takımın rolü, tatbikat sırasında tatbikatla ilgili başta beyaz takıma ve sonra tüm katılımcılara durumsal farkındalık sağlamaktır. Sarı takım için ana bilgi kaynakları, mavi takımlar tarafından sağlanan ara raporlar, kırmızı takım üyelerinden gelen saldırı kampanyalarının durumu ilgili raporlar ve sistem tarafından sağlanan raporlardır. Beyaz takım liderilerine ve mavi takımlara düzenli olarak öne çıkan güncellemeler sarı takım tarafından sağlanmaktadır.

5)Beyaz Takım

Beyaz takım, tatbikat hazırlama ve yürütme sırasında kontrol etme sorumluluğuna sahiptir. Beyaz takım, talim hedefleri, senaryo, kırmızı takım için üst seviye hedefleri, yasal enjeksiyonları, kuralları, medya hazırlıklarını ve iletişim planlarını belirler. Yürütme sırasında beyaz takım, farklı aşamaların ne zaman başlayacaklarını, kırmızı takımın kampanyasının yürütülmesinin denetlenmesi ve puanlama ile ilgili konularda karar vererek tatbikatın kontrolünü sağlar. Yönetim, blonde kullanıcılar, enjeksiyonlar, puanlama ve medya simülasyonu da beyaz takımın sorumlulukları arasındadır.

B.Senaryo

Tatbikat sonrası arzulanan sonuçlar yada çıktılar herbir tatbikat için farklılık gösterir, ancak bu çıktılar her zaman katı-

lımcılara siber tehdit yöntemlerini göstermek ve tatbikat hedeflerini karşılamak için kullanılan talim programlarının ve araçlarının başarısını değerlendirmek için gerçekçi bir senaryo sunmak etrafında döner. Tatbikat çıktıları, farkındalık yaratmayı ve çeşitli siber tehditlere karşı aktiviteleri planlamasını ve değerlendirilmesini amaçlamalıdır ve bu senaryolar tatbikatın ana hedefleri çevresinde dönmelidir.

Geçmiş senelerde gerçekleştirilen bir uluslararası siber savunma tatbikatının örnek sanaryosu şöyledir; X ülkesi, Afrika'nın batı yakasında bulunan bir ada cumhuriyeti olup ülkede, üyesi olduğu uluslararası bir organizasyonun koalisyon gücü bulunmaktadır. Adanın büyüklüğü İrlanda ile karşılaştırılabilir iken, iklim ve manzara Fas'a daha yakındır. Yoksul bir ülke olan X Cumhuriyeti'nin yerel altyapısı, ve özellikle sanitasyon, iletişim, tıbbi hizmetler ve eğitim oldukça yetersiz ve kötü bir durumdadır. Örneğin, ülke, dünyanın geri kalanıyla güvensiz bir internet bağlantısına sahipken ve bağlantının bant genişliği ise düşüktür. Ülke içinde bağlantı, çok sayıda ücretsiz (ve anonim) kablosuz ağlardan yararlanan şehir merkezleriyle sınırlıdır. Ülkenin, USOM (Ulusal Siber Olaylara Müdahale) ekibi ya da bilişim sistemlerini korumaya yönelik kolluk kuvvetleri bulunmamaktadır. Bu, çoğu uluslararası aktörü pahalı uydu bağlantısına veya yerel olarak çalıştırılan sistemleri kurmaya ve kullanmaya zorlamaktadır.

X Cumhuriyeti, yıllardır komşusu olan ve uluslararası toplum tarafından anti demokratik uygulamaları hayata geçiren bir yönetime sahip olduğu eleştirilerine muhattap olan Y ülkesi ile diplomatik çatışma içerisinde bulunmaktadır. Uzun zamandır X Cumhuriyeti, Y ülkesi kaynaklı olduğu tahmin siber saldırılara maruz kalmaktadır. X Cumhuriyeti ve Y ülkesi arasında en son yaşanan diplomatik krizin hemen akabinde, X Cumhuriyeti'nin Hava Kuvvetleri üssüne siber saldırılar gerçekleştilmeye başlanmış ve bir takım gizlilik dereceli bilgi ve belgeler çalınmıştır. Mavi takımın görevi uluslararası koalisyonun bir parçası olarak, X Cumhuriyeti'nin Hava Kuvvetleri üssünde bulunan bilgi işlem cihazları üzerinde gerekli analizleri yaparak raporlamak ve mevcut devam eden saldırılar yada muhtemel yapılması planlanan başka siber saldırıları önlemek adına gerekli tedbirleri almaktır.

Mavi takım, tatbikat boyunca sonradan dahil olacak hukuk, medya, ve starteji tabanlı alt senaryolar ve enjeksiyonları da dikkate alarak daha önce hiç tanıdık olmadığı bir bilişim sistemde kendisine verilen görevleri, belirlenen kuralların dışına çıkmadan yerine getirmeye çalışmalıdır.

C.Puanlama

Puanlama, siber savunma tatbikatları için en sıkıntılı konulardan birtanesidir. Yapılan puanlama sistemleri her ne kadar standartlaştırılmaya çalışılırsa çalışılsın, genelde beyaz takımın kararları doğrultusunda, zaman zaman yine insiyatiflere dayanarak puanlamalar yapıldığından mavi takımlardan her zaman itirazlar gelme ihtimali oldukça yükseltir. Bu nedenle özellikle uluslararası boyutta düzenlenen birçok siber savunma tatbikatı yarışma ortamı yaratarak değil, mevcut tatbikat sonuçlarına göre dersler çıkarılıp, bu konuyla ilgili gerekli tedbirlerin alınmasının asıl amaç olduğunu ileri sürerek puanlama sistemine karşı çıkmıştır. Avrupa Birliği tarafından düzenlenen Cyber Europe puanlama sistemini kullanmayan tatbikatlara örnek gösterilebilir. Bununla birlikte, puanlama sisteminin bu tür tatbikatlarda kullanılmasının katılımcılar için birer motivasyon aracı olarak görüldüğü ve katılımcılar arası oluşan pozitif rekabetin daha başarılı sonuçlara ulaşma konusunda daha büyük bir itici güç olduğu NATO CCD COE tarafından organize edilen Locked Shields siber savunma tatbikatlarında gözlemlenmiştir.

D.Medya Aktivite Simülatörü

Medya simülatörü, tatbikat oyuncularının gerçek hayatta olduğu gibi medya ve sosyal medyayı görüntülemesine ve bunlarla etkileşime geçmesine izin verir. Tüm oyuncuların sosyal medya kullanımları için kendilerine mahsus şifreleri bulunmaktadır. Twitter, Facebook, TV, radyo, çevrimiçi haberler ve gazeteler gibi yayın organları olarak kullanılan tüm medya ve sosyal platformlardan canlı yayın imkanı simülator yardımıyla sağlanabilmektedir. Bu simülasyon ile senaryo gereği oluşturulan temsili ülkenin ve bu ülkede senaryoda yer alan kurum ve organizayonlara ait web sayfalarına da yer verilmektedir. Mavi takımlar, kırmızı takımlardan gelen saldırılara karşı gerekli tedbirleri almakla meşgullerken tıpkı gerçek yaşamda olduğu gibi işin medya boyutu ile ilgili de gereken adımları atmak durumundadırlar.

E.Enjeksiyonlar

Enjeksiyonlar; senaryo enjeksiyonları, medya oyunu, yasal oyun ve adli bilişim olmak üzere 4'e ayrılmaktadır.

1)Senaryo enjeksiyonları; Haberlerin takip edilmesi, istihbaratların değerlendirilmesi, siber saldırıları gerçekleşirenlerle ve bu saldırılarla ilgili malumatların toplanıp ve raporların hazırlanması, suistimal bildirimi ve mavi takım sistemlerini kullanan sıradan kullanıcıların (blonde users) meydana getirdiği yada getirebileceği zayıflıklara karşı gerekli önlemleri almak ve bu kullanıcılardan gelen sorunların en kısa sürede çözümlerini sağlamak konularını içeren ve beyaz takım tarafından hazırlanan enjeksiyonları.

2)Medya oyunu; Daha önce de bahsedildiği üzere medya simülasyonunun amacı, gerçek dünyadan haberler ile tatbikatı medya ortamına taşımak ve kırmızı takımın faaliyetleri dışında geliştirilen enjeksiyonlarla mavi takımlara baskı yapmaktır. Haberlerde yer alan hikayelerde senaryo gereği oluşturulan ülke ile ilgili arka planda cereyan eden olaylarla hakkında bilgiler, devam eden siber olaylar hakkında raporlar, siber saldırılardan etkilenelerden gelen yorumların yanı sıra yalan, değiştirilmiş, ve doğrulanmamış haberler de yer almaktadır.

3)Hukuk Enjeksiyonları: Mavi takımın senaryo gereği emir-komuta zincirinden gelen soruları cevaplayabilmesi derin yasal bilgilere sahip olmasına bağlıdır. Karışık hukuki meseleleri ele

almak, yanlış ifadeleri ve yorumları çürütmek ve aynı zamanda meydana gelen siber saldırılarla alakalı açıklamaları konunun uzmanı olmayan kişilere anlaşılabilir kılmak amacıyla medya ile iletişim kurmak ve medyanın yayınladığı, yalan ve gerçeği yansıtmayan yada gerçeği çarpıtan haber ve analizlere hukuki bağlamda karşılık vermek yasal oyunun gereklilikleri arasındadır.

4)Adli Bilişim: Adli bilişim oyunu, meydana gelen siber saldırılarla alakalı adli bilişim raporu hazırlamaya ve yine bu saldırılarla alakalı kim, ne, ne zaman, nasıl ve neden sorularına cevap aramaya yöneliktir.

VII. DEĞERLENDİRME

Siber savunma tatbikatlarının en önemli çıktılarından birisi Faaliyet Sonu Raporudur. Bu raporda, tatbikat sonrasında her bir mavi takım ile ayrı ayrı detaylı ve özel olarak sadece o takıma mahsus tatbikat performasının paylaşıldığı rapordan farklı olarak, tatbikatta yer alan senaryo ve alt senaryolar, enjeksiyonlar, tatbikat amaçları, katılımcılar, puanlama, teknik alt yapı, kırmızı takım tarafından gerçekleştirilen saldırılar (client-side, web, network), genel manada mavi takım tarafından yapılan savunmalar, bu savunmalardaki zayıflıklar, yapılan genel hatalar, tüm takım ve alt takımlardan gelen gözlem, tavsiye ve değerlendirmeleri içermektedir.

Ayrıca herbir mavi takım ile o takıma özel yapılan analizler, değerlendirmeler, tatbikat boyunca gösterdikleri zafiyet ve zayıf oldukları noktalar, tavsiye ve önerileri içeren ayrı bir rapor da paylaşılmaktadır.

VIII. SONUÇ VE GELECEK ÇALIŞMALAR

Siber savunma tatbikatlarına verilen önem her geçen gün artmaktadır. Ülkelerin gerek ulusal bazda kendi siber savunma tatbikat platformlarını geliştirme ve uygulamasını yaygınlaştırma gerekse uluslararası arenada organize edilen siber savunma tatbikatlarına dahil olmaları ve bu tatbikatların planlama ve gelişimlerine daha yüksek bütçeli rakamlar ayırmaları ileride daha güçlü siber savunma sistemleri oluşturabilmeleri adına faydalı sonuçlar elde etmelerine katkılar sağlayabilecektir. Ulusal ve uluslararası alanda bu tatbikatlara ağırlık verilmesi bir yandan siber alandaki zayıf noktaların ortaya çıkarılması ve siber savunma bilincinin canlandırılmasına bir yandanda siber savunma ile ilgili konularda geliştiren tatbikatlara da entegre edilen teknolojilerin de takip edilebilmesi açısından yararlar sağlayacaktır.

Gelecek çalışmalar için daha önce de bahsedildiği gibi siber savunma tatbikatları için sorunlu bir konu olan puanlama sistemi ve bu sistemin standartlaştırılması ve daha adil paunlama sistemi geliştirilmesi üzerine teknik bir araç geliştirilecektir. Yine bahsedildiği gibi elektrik şebeke sistemleri ve drone kontrol sistemleri gibi yeni teknolojilerin siber savunma tatbikatlarına entegrasyonu oldukça kritik bir konudur. Bu özel sistemlerin tatbikatlara entegre edilmesinde mevcut sorunlar ve izlenmesi gerek metodlar gelecekte yapılacak bir başka çalışma konusudur.

Bu özel sistemlerin tatbikatlara entegre edilmesinde mevcut sorunlar ve izlenmesi gereken metodlar gelecekte yapılacak bir başka çalışma konusudur.

TERMİNOLOJİ

Faaliyet Sonu İncelemesi (After Action Review – AAR) [16]: Proje yada faaliyetten sorumlu kişiler ve katılımcılar tarafından gerçekleştirilen faaliyet ile ilgili, ne olduğu, neden olduğu ve daha iyi nasıl yapılabileceği sorularına cevap olabilecek nitelikte, analiz amaçlı hazırlanan analitik gözden geçirmedir.

Faaliyet Sonu Raporu (After Action Report – AAR) [16]: Gerçekleştirilen faaliyet ile ilgili, faaliyeti gerçekleştirenler tarafından üstlenilen belirli bir hedef odaklı eylem dizisi üzerine geriye dönük analiz için hazırlanan rapordur.

Siber Güvenlik [17]: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder.

Ana Senaryo Etkinlik Listesi (Master Scenario Event List – MSEL) [16]: Belli çıktıları elde etmek amacıyla önceden yazılmış senaryolar bütünüdür.

Enjeksiyon [16]: Ana senaryo etkinlik listesinin bir parçası olarak yürütülen belirli bir etkinliği ifade eder.

Tatbikat [16]: Talim ve durum değerlendirme amaçlarıyla yürütülen, planlama, hazırlık ve uygulama aşamalarını içeren simüle edilmiş savaş anı ortamıdır.

Tatbikat Senaryosu [16]: Tatbikat ve talim hedeflerini başarmak için yeterli kapsam ve ayrıntıda olan stratejik ve operasyonel ortamı tanımlar.

Hotwash [18]: Tatbikatın hemen sonrasında görevli personel ve katıımcılarla yapılan bilgilendirme ve değerlendirmelerdir.

Angajman Kuralları (Rules of Engagement) [18]: Bilgi güvenliği testinin yürütülmesine ilişkin detaylı yönergeler ve kısıtlamaları ifade etmektedir. Angajman kuralları bir güvenlik testinin başlamasından önce oluşturulur ve test ekibine ek izinlere gerek kalmaksızın tanımlanmış faaliyetleri yürütme yetkisi verir.

Tehdit [17]: Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedenini ifade eder.

KAYNAKÇA

[1] Cyber Defence Exercise Locked Shields 2013 – After Action Report, NATO CCD COE, Tallinn, 2013.

[2] Cyber Defence Exercise Locked Shields 2014 – After Action Report, NATO CCD COE, Tallinn, 2014.

[3] Cyber Defence Exercise Locked Shields 2015 – After Action Report, NATO CCD COE, Tallinn, 2015.

[4] Cyber Defence Exercise Locked Shields 2016 – After Action Report, NATO CCD COE, Tallinn, 2016.

[5] The 2015 Report on National and International Cyber Security Exercises, ENISA, 2015.

[6] Locked Shields 2017, NATO CCD COE, Retrieved from: https://ccdcoe.org/locked-shields-2017.html, 2017.

[7] Cyber Coalition 16: NATOs Largest Cyber Defence Exercise, NATO SHAPE, Retrieved from: https://www.shape.nato.int/2016/cyber-coalition-16-ends-natos-largest-cyber-defence-exercise, 2017.

[8] Cyber Europe 2016, Retreived from: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016, 2017.

[9] Cyber Defense Exercises – Participant Information Package, ENISA, 2013.

[10] Introduction to Cyber Exercises, National Cyber Security, Division Cyber Exercise Program, DHS, 2003.

[11] N. Wilhelmson, T. Svensson, "Handbook for Planning, Running, and Evaluating Information Technology and Cyber Security Exercises", CATS, 2013.

[12] C. A. M. Forero, Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development, Master's Thesis, 2016.

[13] J. Kick, "Cyber Exercise Playbook", The MITRE Corp., 2014.

[14] Cyber-Exercises Analysis Report, ENISA. 2016.

[15] Good Practice Guide on National Exercises, ENISA, 2009.

[16] Joint Training Manual for the Armed Forces of the United States, Chairman of the Joint Chiefs of Staff Manual, 2012.

[17] 2016 - 2019 Ulusal Siber Guvenlik Stratejisi, T.C. UDHB, 2016.

[18] R. Kissel (Ed.), "Glossary of Key Information Security Terms", NIST, 2013.

Saldırı Tespit Sistemlerinde Ajan Sistemlerin Kullanımı

Using Agent System In Intrusion Detection System

Esra SÖĞÜT
Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
esrasogut@gazi.edu.tr

O. Ayhan ERDEM
Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
ayerdem@gazi.edu.tr

Aydın ÇETİN
Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
acetin@gazi.edu.tr

Özet

Saldırı tespit sistemlerinde, ana sistemin yanı sıra ağın ve ağ bileşenlerinin performansları üzerinde daha iyi bir gelişme sağlanması amaçlanmaktadır. Saldırıların veya tehditlerin sistem içerisinde yayılmadan önce giriş noktalarında engellenmesi ve durdurulması gerekmektedir. Mobil ajan teknolojisi bu amaçları gerçekleştirmek için kullanılmaktadır. Bir sistemden diğerine bağımsız şekilde hareket edebilen ve hedef sistem üzerinde işlevini sürdüren yazılım veya cihazlar mobil ajanlar olarak adlandırılmaktadır. Merkezi olmayan dağıtık ortamdaki saldırıların tespiti için geliştirilmiştir. Bu çalışmada, mobil ajan temelli saldırı tespit sistemleri incelenmektedir. Saldırı tespit sistemlerinde mobil ajanlar vasıtasıyla gerçekleşen performans değişiklikleri ve geliştirilen teknikler örnek uygulamalara yer verilerek gösterilmektedir.

Anahtar Kelimeler

Mobil Ajanlar, Saldırı Tespit Sistemleri, AAFID, IDA

I. GİRİŞ

Saldırı tespit sistemleri (STS), ağ kaynaklarının ya da bilgisayar sistemlerinin hedef alındığı saldırılar ile ilgilenmektedir. Bilgisayar sistemlerine yapılan saldırıların tespit edilmesi ve saldırılara ait özelliklerin belirlenmesi STS çalışma alanlarıdır. Saldırı kaynağının belirlenmesi ve daha önce tanımlanan çerçeveye sahip olan saldırıların fark edilip tekrar uygulanması durumunda tespit edilmesi STS'ler için önemli konulardır [1].

Saldırı tespiti için farklı alanlarda yapılan çalışmalardan biri de dağıtık mimari yapısıdır. Dağıtık mimarinin dağıtık saldırıların daha hassas tespit edilmesinde kullanılması için çalışmalar yapılmaktadır. İstemci-sunucu ve merkezi yaklaşımların sınırlamalarını aşmak için dağıtık mimari ile mobil ajan sistemleri kullanılmaktadır. Ajan tabanlı sistemlerde merkezi bir istasyon bulunmadığı için merkezi bir başarısızlık noktası da bulunmamaktadır. Ayrıca ajanlar otonom hareket edebildiği için aralarında hiyerarşik bir dizilim de yoktur. Ajanlar diğer ajanlardan bağımsız olarak hareket edebilir ve farklı görevleri yerine getirebilirler.

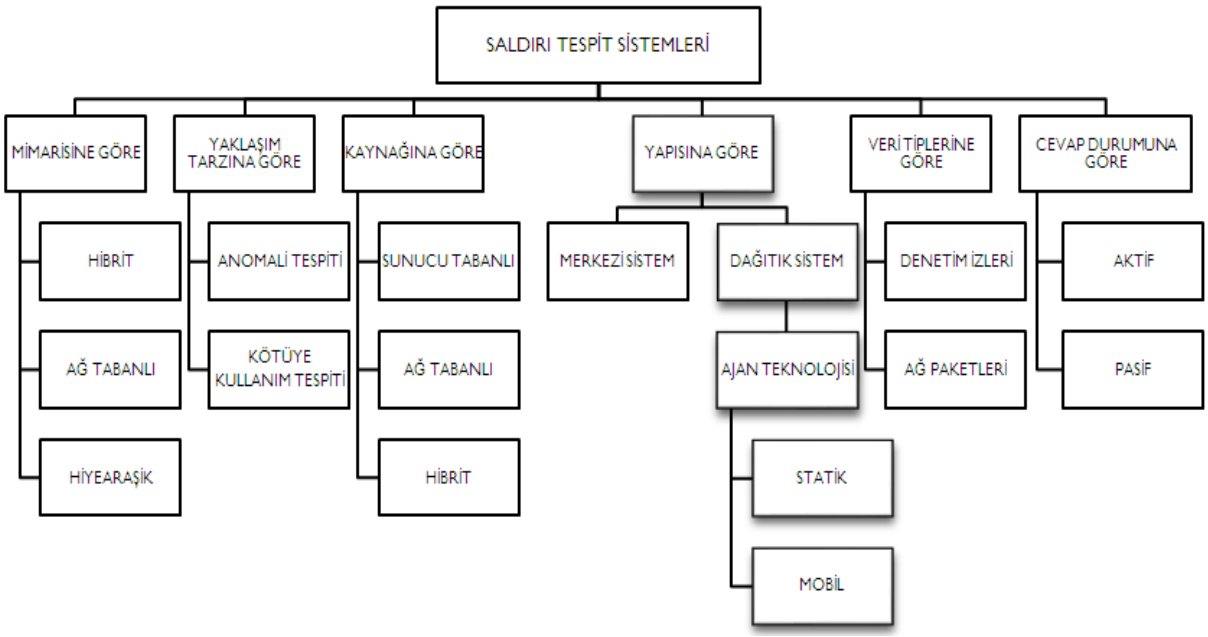
STS'lerde mobil ajan kullanımıyla ilgili yapılmış birçok çalışma vardır. Barrus ve arkd. 1998 yılında yaptıkları çalışmada saldırıları durdurmak için işlemlerin otomatik olarak yapılması gerektiğini belirtmişlerdir. Bunu sağlamak için heterojen bir ağda gerçek zamanlı algılama yapan ve yanıt veren otonom ajanların kullanılmasını önermişlerdir [2]. Jai Sundar ve ark. 1998'de dağıtık mimari kullanarak Autonomous Agent For Intrusion Detection sistemini geliştirmiştir [3]. Zhang ve ark. 2000'de ve Thomas Toth ve ark. 2002'de dağıtık mimari kullanarak mobil ajan teknolojisi çalışmalarını sürdürmüştür [4,5]. 2015'de Al-Yaseen ve ark. yaptıkları çalışmada çoklu ajan ortamlarında STS için makine öğrenmesi yöntemlerini kullanmışlardır. Yaptıkları çalışmada C4.5 ile K-Means algoritmalarını kullanarak ajan sistemler için melez bir uygulama önermişlerdir [6].

Bu çalışmada, Mobil Ajan Teknolojisi incelenerek, bu teknolojinin saldırı tespit sistemlerinde kullanılabilirliği hakkında bilgi verilmiştir. Mobil ajanların sahip olduğu olumlu ve olumsuz davranışlar hakkında değerlendirme yapılmıştır. Ayrıca, saldırı tespit sistemlerinde kullanılan farklı mobil ajan uygulamaları birlikte ele alınarak kıyaslamaları yapılmış ve sonuçları tablo halinde sunulmuştur.

II. SALDIRI TESPİT SİSTEMLERİ

Saldırı varlığını tespit etmek için antivirüs, güvenlik duvarı ve STS gibi çeşitli araçlar/yazılımlar araştırma kuruluşlarında olduğu kadar günlük hayatta da kullanılmaktadır. Bu araçlar/yazılımlar algılama yetenekleri bakımından incelendiğinde STS'nin diğerlerine göre daha güçlü olduğu görülmektedir [7]. STS'ler, ağ veya sistem üzerindeki kötü niyetli faaliyetleri veya kural ihlallerini izleyen cihaz veya yazılım uygulamalarıdır. STS'ler ile elde edilen sonuçlar sistem veya ağ yöneticisine rapor edilir ve gerekli işlemlerin yapılması için uyarılarda bulunulur [8].

STS'leri sınıflandırmak için çeşitli yaklaşımlar bulunmaktadır. Bu yaklaşımlar Şekil 1.'de gösterilmektedir.



Şekil. 1 STS sınıflandırılması [9]

Şekil 1.'de görüldüğü üzere STS sınıflandırması 6 farklı yaklaşıma göre yapılmış ve Ajan Teknolojisinin kullanıldığı yaklaşım belirtilmiştir. Buna göre STS, yapısına göre incelendiğinde dağıtık sistemler Ajan Teknolojisini içermektedir. Ajan Teknolojisi de statik ve mobil olmak üzere iki bölüme ayrılmaktadır. Bu çalışmada, sabit bir sistem üzerinde işlevlerini sürdürmesinden dolayı statik ajan teknolojisi kapsam dışı tutulmuştur.

III. MOBİL AJAN SİSTEMLERİ

Dağıtık sistemlerin geliştirilmesi ile saldırı tespiti yapmak için yazılım ajanları kullanılmaya başlanmıştır. Bunun sonucunda mobil ajan teknolojisi bu alanda kendini göstermeye başlamıştır. Mobil ajanlar, kendi kendine yeten ve tanımlanabilir otonom bilgisayar programlarıdır. Bunlar sahip oldukları kodları, verileri ve çalışma durumları ile birlikte heterojen ağ yapılarına sahip bilgisayar sistemlerinde hareket edebilmektedir [10]. Bu tür ajanlar, saldırı tespit sistemleri dışında uzay aracının otomasyonu, oyun oynama, direksiyon kullanımı, tıbbi teşhis, robotik, dilin anlaşılması ve problem çözümü gibi çeşitli endüstriyel uygulamalarda da kullanılmaktadır [11].

Mobil ajanların kullanımı ile dağıtık yapıda veri toplama ve veri işlemenin birden fazla düğümde yapılması sağlanmaktadır. Düğüm sayısının fazla olmasına rağmen, yapılan incelemelere göre işlem yanıt süresinde ve ajan boyutunda iyileşme yapılabileceği tespit edilmiştir [7].

Mobil ajanlar, program kodlarının farklı ortamlarda çalıştırılması özelliğinden faydalanmaktadır. Ajanlar, bir makinedeki çalışmasına ara vererek veya çalışmasını sonlandırarak başka bir makineye geçebilir ve çalışmalarına kesintisiz devam edebilirler.

STS'lerde Mobil ajanların kullanımı birçok avantaj sağlamaktadır. Bunun yanısıra Mobil ajan kullanımının dezavantajları da bulunmaktadır.

A. Avantajlar

Mobil ajanların kullanılabilmesi için ağdaki her makinenin ajan platformuna sahip olması gerekmektedir. STS'lerde statik bileşenler kullanmak yerine mobil ajan tabanlı sistemlerin kullanılması birçok avantaj sunmaktadır. STS'lerde mobil ajan kullanımının avantajları aşağıda belirtilmektedir [12,13].

- Ağ yükünü azaltma: Büyük miktarda veriyi veri işleme birimine göndermek yerine, işleme algoritmasını (ajanı) verilere taşımak daha basit olabilir.
- Ağ gecikmesini azaltma: Mobil ajanlar, çevredeki değişikliklere gerçek zamanlı olarak yanıt verdikleri için ağın başka bir yerinde olan merkezi koordinatörle iletişim kurmaya gerek kalmadan hızlı yanıt verebilir.
- Ölçeklenebilirlik: Ağdaki işlem öğelerinin sayısı arttıkça, ajanlar çoğalabilir ve ağdaki yeni makinelere gönderilebilir.
- Hata toleransını arttırma: Mobil ajanlar çevrelerindeki değişikliklere dinamik ve otonom olarak tepki verdikleri için hataya karşı dayanıklı ve sağlam yapılı hale gelirler.
- Eş zamanız ve otonom yürütme: Mobil ajanlar, ana makine müdahalesi olmadan otonom ve eş zamansız olarak çalışabilir. Ana makineye tekrar bağlanabilir.
- Platform bağımsızlığı: Ajanlar, ana makine platformundan bağımsız olarak çalışabilir.
- Dinamik ve statik uyarlama: Ajanların dinamik davranışı nedeniyle sistem çalışma zamanı yeniden yapılandırılabilir. Statik uyarlama özelliği ile tüm sistem yeniden başlatılmaksızın ajanların algoritmaları güncellenebilir.

B. Dezavantajlar

Ajan tabanlı STS'lerin sahip olduğu avantajların yanı sıra, güvenlik, kod boyutu ve performans gibi konularda bazı problemleri bulunmaktadır [12,14].

• Güvenlik: Kötü amaçlı bir mobil ajan, ana makineye veya başka bir mobil ajana zarar verebilir, işleyişe engel olabilir ve sistemi aksatabilir.

• Kod boyutu: Ajanın gerekli kodu ağ üzerinden aktarması zaman kaybına sebep olabilir fakat her bir ana makine ajanının bu kodu yerel olarak bir kez depolaması yeterlidir.

• Performans: Ajanlar genellikle farklı platformlar arasında kolaylıkla taşınabilmek için komut dosyası veya yorumlanmış dillerde yazılmıştır. Bu durum ajanların hareketini yavaşlatmaktadır.

• Öncelikli bilgi eksikliği: Bir sistemin nasıl yapılandırıldığı, verilerin nasıl düzenlendiği ve sistem yükünün nasıl ayarlandığı konularında mobil ajanların önceden bilgi sahibi olması önemlidir.

IV. ÖRNEK AJAN TABANLI STS UYGULAMALARI

Bilgisayar ağlarında mobil ajanların kullanımı ile saldırı tespit sistemlerine yeni bakış açışı kazandırılmıştır. Literatürde çok sayıda mobil ajan tabanlı STS bulunmaktadır. Bu örnek uygulamalara karşılaştırmalı olarak Tablo 1.'de yer verilmektedir.

Tablo 1. Örnek Ajan tabanlı STS uygulamalarının karşılaştırılması

Model	Yaklaşım	Avantajlar	Dezavantajlar	Kaynak No
Autonomous Agents For Intrusion Detection (AAFID)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Ölçeklenebilir sistem yapısı Toplanmış ve önişleme tabi tutulmuş bilgi kullanımı	Ajanlar ve monitör arasındaki katmanın saldırı tespitinde gecikmeye sebep olması Monitörlerin tek başarısızlık noktası olması	3
Intrusion Detection Agent System (IDA)	Mobil ajan yaklaşımı	Saldırgana ait izlerin takibi Basit sistem yapısı	Sınırlı derecede ölçeklenebilirlik. Merkezi veri toplama	15
Intelligent Mobile Agents for Intrusion Detection System (IMA-IDS)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Toplayıcı ajanların sonuçları yöneticiye bildirmesi Anormallik tespitinde alarm üretilmesi	Merkezi veri toplama	15
Micael	Mobil ajan yaklaşımı	Ajanların bilgi toplama dışında da kullanılması Ajanların olaylara tepki vermesi Taşınabilir sistem yapısı	Yalnızca JAVA'yı destekleyen platformlarda çalışması	15
Intelligent Agents for Distributed Intrusion Detection System (IA-DIDS)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Ağdaki ana makineler üzerinde otonom çalışma	-	15
Preemptive DIDS	Ağ tabanlı mobil ajan yaklaşımı	Saldırı tespit edildiğinde, saldırının engellenmesi için şüpheli paketlerin işleme alınmadan sistem dışına atılması	-	15
Distributed Soft Computing for Intrusion Detection System (DSCIDS)	Hibrit yaklaşım	Hiyerarşik sistem yapısı Katmanlar arasında rahat iletişim Farklı hesaplama algoritmaları	Ajanların dağılımının yeterli ve düzenli olmaması Hesaplama algoritmalarının tespit konusunda çalışmasının tartışmaya açık olması	16
Multi-Level and Secured Agent-based Intrusion Detection System (MSAIDS)	Kötüye kullanım tespiti	Mobil ajanların güvenliğine ek olarak kaydedilmiş durum mekanizmasının kullanımı Ajanların iyi organize edilmesi	Her seviyede saldırı tespiti için aynı algoritma kullanılması ile raporlamada gecikme yaşanması Değişik saldırı davranışlarına göre yeterli tedbirler bulunmaması	17
Mobile Agent for Network Intrusion Resistance	Hibrit yaklaşım	Geleneksel dağıtık tespit sistemlerinin hiyerarşik yapısından farklı olması	Saldırı tespitinin önemli bölümünün yapıldığı yerde tek bir kontrol merkezi olması Bu merkezin ele geçirilmesi ile sisteme ciddi zararların verilebilmesi	18

Örnek ajan tabanlı STS uygulamaları yaklaşım biçimi, sahip olunan avantaj ve dezavantaj kriterlerine göre değerlendirilmektedir. Yaklaşım biçimi olarak ana bilgisayar tabanlı mobil ajan dışında hibrit ve kötüye kullanım tespiti yaklaşımları da kullanılmaktadır. Her örnek uygulamanın kendine özel avantajları ve dezavantajları bulunmaktadır. Ölçeklenebilir, basit, taşınabilir veya hiyerarşik sistem yapılarına sahip olunması avantajlar arasında yer almaktadır. Merkezi şekilde veri toplama gerçekleştirilmesi, tek bir kontrol merkezinin bulunması veya gecikmelerin yaşanması dezavantajlar arasında kendini göstermektedir.

V. SONUÇ

Bu çalışmada, ajan tabanlı sistemlerin STS'lerde kullanımı incelenmiştir. Ajan tabanlı STS örnek uygulamaları değerlendirilmiş ve karşılaştırmaları yapılmıştır.

Saldırı tespit sistemlerinde ajan tabanlı sistemlerin kullanımı ile ilgili birçok çalışma bulunmaktadır. Farklı yapılarda ve özelliklerde olan çalışmalar ile elde edilen sonuçlar incelenmiştir. Buna göre bir takım çıkarımlar yapılmıştır. Bunlar:

- STS'nin tamamında ajanların kullanılması tam anlamıyla işlevsellik sağlamayabilir.
- Bazı bileşenlerin statik olması sistem çalışması için verimli olabilir.
- Sistemlerin tümünde mobil anlayışın yer alması sisteme fazladan yük gelmesine sebep olabilir.
- Taşınabilirlik sistemde gerekli görülen bölümlerde ve zamanda yapılmalıdır.
- Ajanların kötü amaçlı kullanılabilmesi sistem güvenliğini tehlikeye atabilir. Yeni güvenlik çözümlerinin geliştirilmesi gerekmektedir.
- Yapılarından ve kullanım şekillerinden dolayı farklı boyutlarda olan kodların ajan tarafından aktarılması gecikmeli olabilir. Bunun önüne geçilebilmesi için farklı sistem şekilleri veya yöntemleri kullanılabilir.
- Sistem yapılandırılması ve işleyişi konularında ajanların bilgi sahibi olması gereklidir. Bunu sağlamak için ajan eğitimi, ajan keşfi ve ajan kullanımı konularında yeni çözümlerin geliştirilmesi gerekmektedir.
- Yakın gelecekte çok daha fazla bilgi toplayıcı ajanın kullanılacağı ve toplanan bilgilerin analiz edilmesi için daha fazla ajana ihtiyaç olacağı öngörülmektedir.
- Gelecekte özelleşmiş ajanların kullanılması ile analiz ajanlarının birden fazla tip saldırıyı tespit edebilecek duruma geleceği öngörülmektedir.
- Her sistemde birden fazla ajanın birlikte çalışabileceği öngörülmektedir.

Farklı sistemlere farklı ajan tabanlı öneriler sunulabilmektedir. Gelecekte yapılacak çalışmalar için daha gelişmiş, dezavantajları azaltılmış ve performans düzeyi iyileştirilmiş ajan sistemlerinin kullanılacağı öngörülmektedir.

KAYNAKLAR

[1] Söğüt, E. Gelişmiş Israrci Tehdit Tespit Yöntemleri Ve Bir Uygulamasi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2016.

[2] Barrus, J. (1998). A Distributed Autonomous-Agent Network-Intrusion Detection and Response System. Procedings of the 1998 Command and Control Research and Technology Symposium. June-July. Monterey, CA.

[3] Balasubramaniyan, J.S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., Zamboni, D., An Infrastructure for Intrusion Detection using Autonomous Agents, COAST Technical Report 98/05, June 11, 1998.

[4] Spafford, E. H., Intrusion Detection Using Autonomous Agent, Computer Networks, 2000, 3(4): 547-570.

[5] Krügel, Christopher, Thomas Toth. Flexible, mobile agent based intrusion detection for dynamic networks, European Wireless. 2002.

[6] Al-Yaseen, W. L., Othman, Z. A., Nazri, M. Z., Hybrid Modified k-Means with C4.5 for Intrusion Detection Systems in Multiagent Systems, The Scientific World Journal, Volume 2015, Article ID 294761, 14.

[7] Shah, B., Trivedi, B., Improving Performance of Mobile Agent Based Intrusion Detection System, IEEE International Conference on Advanced Computing & Communication Technologies-2015.

[8] İnternet: http://suricata-ids.org/ [Son erişim tarihi: 05.05.2017].

[9] Onashoga, S.A., Adebayo D. Akinde A., Strategic Review of Existing Mobile Agent- Based Intrusion Detection Systems, Issues in Informing Science and Information Technology Volume 6, 2009.

[10] Christopher, K., Thomas, T., Applying Mobile Agent Technology to Intrusion Detection, In ICSE Workshop on Software Engineering and Mobility, 2001.

[11] Trivedi, B. H., Mobile Intelligent Agents in Intrusion Detection, proceeding of NCC-06 National Conference on Computing and Communication, Hyderabad, 13th-15th July- 2006.

[12] Jain P., Raghuwanshi, S., Pateria, R., New Mobile Agent-Based Intrusion Detection Systems for Distributed Networks, International Journal of Wireless Communication Volume 1, Issue 1, 2011, pp-01-04.

[13] Albag, Hakan. Network & Agent Based Intrusion Detection Systems, TU Munich Dep. of Computer Science, Istanbul Technical University, 2001.

[14] Srivastava, S., Gupta N., Saugata, G., Chaturvedi, S., A Survey on Mobile Agent based Intrusion Detection System, International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011.

[15] Khobragade, S., Padiya, P., Distributed Intrusion Detection System Using Mobile Agent, International Journal of Engineering and Innovative Technology (IJEIT), Volume 5, Issue 4, October 2015.

[16] Abraham, A., Jain, R., Thomas, J., Han, S. Y., D-SCIDS: Distributed soft computing intrusion detection system. Journal of Network and Computer Application, 30, 81-98, 2007.

[17] Sodiya, A. S., Multi-level and secured agent-based intrusion detection system. Journal of Computing and Information Technology, 14(3), 217-223, 2006.

[18] Wang, H. Q., Wang, Z. Q., Zhao Q., Wang G. F., Zheng R. J., & Liu, D. X., Mobile agents for network intrusion resistance. APWeb Workshops 2006, LNCS 3842, pp 967-970, 2006.

Siber Güvenlikte Kamu ve Özel Sektör İşbirliği

Public and Private Sector Cooperation for Cyber Security

Gülcihan Aydaner
Uluslararası Ticaret ve İşletmecilik Bölümü
Bandırma Onyedi Eylül Üniversitesi
Bandırma, Türkiye
gulcihan.aydaner@gmail.com

Yrd.Doç.Dr. Ufuk Çelik
Bilgi Teknolojileri Bölümü
Bandırma Onyedi Eylül Üniversitesi
Bandırma, Türkiye
ucelik@bandırma.edu.tr

Yrd.Doç.Dr. Senem Nart
Uluslararası Ticaret ve İşletmecilik Bölümü
Bandırma Onyedi Eylül Üniversitesi
Bandırma, Türkiye
zudesenem@hotmail.com

Abstract

Nowadays, the rapid pace of committing crimes of information has become one of the most difficult crimes, low cost of attack, high social and commercial costs. Even those who are innately talented in the Internet and in computer science are experts in their fields, updating the techniques of attack without any training. Hackers are improving their attack potentials and strengths day by day. The cyber security gap between the public and the private sector raises the appetite of hackers fed with cyber attacks. In this study, which was made to contribute to our knowledge accumulation, the quantitative, theoretical and theoretical framework for cooperation between the public and the private sector was studied together and the communication, control and information flow mechanism existing between the public and private sectors was evaluated.

Index Terms

Cyber security, national cyber strategy, cyber attacks, industry 4.0, public and private sector cooperation

Özetçe

Günümüzde bilişim suçları hızla artan durdurulması zor, işlenmesi kolay, saldırı maliyeti düşük, toplumsal ve ticari maliyeti yüksek suçlar arasına girmiştir. İnternet ve bilişim konusunda doğuştan yetenekli olan kişiler, herhangi bir eğitim almadan saldırı tekniklerini güncelleyerek ve alanlarında uzmanlaşarak siber saldırılarla ulusları tehdit eder hale gelmişlerdir. Bununla birlikte siber saldırıların faili olan hackerler, saldırı potansiyellerini ve yöntemlerini her geçen gün geliştirirerek sosyal ve ekonomik anlamda uluslara zarar vermektedirler. Bu doğrultuda; Kamu ve özel sektör arasında var olan siber güvenlik açığı siber saldırılarla beslenen hackerlerin iştahını kabartmaktadır. Bilgi birikimimize katkıda bulunmak amacıyla yapılmış olan bu çalışmada siber güvenlikte kamu ve özel sektör arasında ki işbirliğine yönelik nicel, kuramsal ve teorik çerçeve birlikte çalışılmış, siber güvenlikte kamu ve özel sektör arasında var olan iletişim, kontrol ve bilgi akışı mekanizması değerlendirmeye alınmıştır.

Anahtar Kelimeler

Siber güvenlik, ulusal siber strateji, siber saldırılar, endüstri 4.0, kamu ve özel sektör işbirliği

I. GİRİŞ

İçinde bulunduğumuz yüzyılda, internetin gelişmesiyle uluslararası platformlarda ülkelerin savaş saldırı ve savunma yöntemleri de zamana uygun olarak değişmiştir. İnternetin tarihsel gelişimi askeri, kamusal, ticari ve son olarak kişisel alanlarda ilerlemiştir. İnternetin hayatımıza girmesiyle birlikte, dünyanın her yerinden mağazalara gitmeden EFT, havale gibi işlemlerle para dolaşımına gerek kalmadan bankacılık işlemleriyle alım satım yapılabilmekte ve birçok bilgiye internet üzerinden ulaşılabilmektedir [1]. Böylelikle kamu kurum ve kuruluşları, ticari işletmeler ve bireyler tüm işlemlerini internet üzerinden yaparak daha hızlı ve rahat mal ve hizmet sunup satın alma imkanına sahip olmaktadırlar. Bununla birlikte dünya bugün endüstri 4.0 deyimiyle tanımlanan yeni bir sanayi devrimine uyum sağlamaya çalışmaktadır. Hannover, 2011 Fuarında Almanların ortaya attığı Endüstri 4.0 deyimiyle tanımlanan yeni bir sanayi devrimininin üzerinde durulmaktadır [2]. Neredeyse sanayi sektörünün tamamının teknolojik yatırımlara öncelik verdiği bu devrimde, yapay zeka üzerinde gerçekleştirilen çalışmalar ise ivme kazanmıştır. Tüm bu gelişmeler doğrultusunda bilgi ve iletişim teknolojilerinin gelişimini sağlayan ve sınırlamaları ortadan kaldıran siber fiziksel sistemler kullanılmaya başlanmıştır. Endüstri 4.0 ile yakın zamanda akıllı fabrikalar insansız üretime geçerek sağlık, finans, eğitim ve savunma gibi bir çok sektörün, kısa sürede endüstri 4.0 ile bütünleşmiş olacağı öngörülmektedir. Tüm sektörlerin dijital ortama kaydığı bu sistemde ise, tüm kamu kurumları, kamu kuruluşları ve ticari işletmeler siber güvenliğe yönelik risk yönetimine ve siber güvenlik stratejisine ihtiyaç duymaktadır. 2020 yılında yaklaşık 50 milyar cihazın birbiriyle iletişim halinde olacağı tahmin edilmektedir [3]. Akıllı üretim sistemlerinin, akıllı şehir, ev, lojistik, şebeke, cihaz unsurlarının, sosyal ağlar ve e-ticaret ağlarıyla birleşmesi sonucu veriler, hizmetler, nesneler ve bireylerin internet ortamını kullanarak kuracağı ekosistemdeki ağın önümüzde ki

çeyrek asırda küresel ticaret hacminin yaklaşık 46'sını etkileyeceği öngörülmektedir [3]. Devamlı gelişen ve değişen dünyamızda en önemli servetimiz bilgiyi iyi korumak ve muhafaza edebilmektir. Kurumlarımızın ve şirketlerimizin bilgi

güvenliğini korumak ve bu durumu sürdürülebilir hale getirmek ayrı bir uzmanlık ve iletişim bilgeliği gerektirmektedir. Elektronik alanlarda var olan sistemsel açıklardan faydalanan hackerler, bu alanlarda kendilerine maddi çıkar sağlayacak hırsızlıklara yönelerek haksız kazanç sağlamayı en zahmetsiz, rahat ve kolay para kazanılır bir yol olarak tercih etmektedirler [4]. Ayrıca teknik ve teorik anlamda var olan güvenlik açıklarımız nedeniyle bu durumu kontrol edebilmek günden güne zorlaşmaktadır [5]. Gizli tutulan devlet bilgilerinden gizli tutulan şirket bilgilerine kadar her bilgi ulusların geleceklerinin teminatı olmuştur. Bu bilgilerin etkin bir şekilde korunması ve saklanması ülkelerin milli güvenliği ve ticari ilişkileri açısından büyük öneme sahiptir. Aktarılan tüm bu bilgiler ışığında bu çalışmada, kamu ve özel sektör arasında var olan siber güvenlik ve işbirliğinin kuramsal, teorik ve nicel çerçevesi açıklanmaya çalışılmıştır.

II. SİBER SALDIRILAR

Siber Saldırı: Bilgisayar ve internet alanında uzmanlaşmış hacker olarak tabir edilen hack veya hacker gruplarının banka, polis, jandarma, devlet, şahıs, firma vb. sitelere veya bilgisayarlara zarar vermek amacı ile yaptıkları saldırıya, Siber Saldırı denir [21].

Siber Suç: Herhangi bir bilişim sisteminin güvenliğini tehlikeye düşürecek faaliyetlerde bulunmak ve kişi veya kişilerin haklarına karşı bilişim sistemlerinin kullanılarak gerçekleştirildiği suçların tümüdür. Yasalar ile cezası sabit olan siber suçların, normal bir suçtan hiçbir farkı bulunmamakla birlikte, birçoğu para veya hapis cezası olarak infaz edilebilmektedir [22].

Türkiye, en çok siber saldırıya uğrayan ülkeler arasında son yıllarda ilk beş arasında yer almaktadır. Ancak genel olarak Türkiye'de bankalar dünya ortalamasının üstünde bir seviyede güvenli diyebiliriz [22]. Türkiye'de bankacılık sektörünün en fazla maruz kaldığı başlıca siber saldırı çeşitleri ise; DDoS Saldırıları, Fidye Yazılımları, Atm Zararlı Yazılımları ve Mobil Tehditlerdir [22].

TABLO I. SIBER SALDıRı TÜRLERI

1.Kötücül Yazılım (Malware): Bilgisayar sistemlerini kötü amaçlı kullanmak için tasarlanmışlardır.Sızdıkları bilgisayarlarda yazılan yazılım türüne göre çeşitli hasarlar verebilir, kişisel verilere ulaşabilme ve bunları değiştirme gibi izinlere sahip olabilirler.
2.Virüsler: Sistemdeki dosyalar ile kendilerini değiştiriler ve değiştirdikleri sistem dosyasının kimliğine gizlenerek çeşitli bilgisayar işlemine olanak sunarlar.
3.Solucanlar: Virüslerin yazılımına benzerler. Bir bilgisayardan başka bir bilgisayara kopyalanmak için tasarlanırlar.
4.Truva Atı: Genellikle bilgisayar kullanıcılarının içeriği hakkında derinlemesine bilgisi olmayan programlara yerleştirilir.Adından da anlaşıldığı gibi Truva atları (trojen) sisteme kendini gizleyerek yerleşir.Örneğin bir kullanıcının Adobe Flash Player'i 'Adobe' kaynaklı indirdiğini sanarken farklı bir kaynaktan indirmesi verilebilir.
5.RootKit: Bilgisayarda çalışan sistemler arasında kendini gizleyen oldukça kötü niyetli bir yazılım türüdür.Çalışma mantığı virüsler gibidir ancak virüsler gibi yayılmak ve sisteminizi aksatmaktan çok,bilgisayarınızı uzaktan kontrol etmeye odaklıdır.
6.Yemleme (Pishing): Yasa dışı yollarla kullanıcıların kullanıcı adı, şifre kimlik bilgisi gibi önemli bilgileri ele geçirme yöntemidir. Örneğin, kurumsal bankaların mail adreslerini taklit ederek kullanıcılardan kart bilgisi, şifre gibi bilgiler verilmesi istenerek yemleme yöntemi uygulanılmaktadır.

Kaynak: Dönence Bilişim Siber Saldırı Türleri [23]

TÜRKİYE'NİN SİBER SALDıRı İSTATİSTİKLERİ

A. Kötücül Yazılım Bulaşma Oranı

2016 yılına ait güvenlik ve araştırma şirketleri tarafından yayımlanan çeşitli güvenlik raporlarında, Türkiye açısından oldukça dikkat çekici sonuçlar göze çarpmaktadır. Tablo II'de gösterilen çizelgede, Türkiye'nin kötücül yazılım bulaşma oranının en yüksek olduğu 10 ülke arasında Çin'den sonra %48'lik bir oran ile 2. sırada olduğu gözükmektedir [9].

TABLO II. KÖTÜCÜL YAZıLıM BULAŞMA ORANı

SIRA	ÜLKE	BULAŞMA ORANI (%)
1.	ÇİN	52
2.	TÜRKİYE	48
3.	TAYVAN	42
4.	EKVATOR	39
5.	GUATEMALA	38
6.	RUSYA	38
7.	MEKSİKA	36
8.	PERU	36
.	POLONYA	35
10.	BREZİLYA	33

Kaynak: Havelsan Siber Güvenlik Bülteni, Sayı 8, Mart 2017 [9]

B. Her DD0S Saldırısından Biri Türkiye Kaynaklı

Tablo III'de ise Türkiye Dağıtık Hizmet Aksattırması (DDoS) saldırılarının en çok kaynaklandığı 10 ülke sıralanmaktadır. Burada da Türkiye, Çin ve ABD'den sonra saldırıların çıktığı 3. ülke olarak gözükmektedir. [9] Daha açık bir ifade ile her 10 DDoS saldırısından biri Türkiye kaynaklıdır [9].

TABLO III. DDoS SALDIRILARININ KAYNAKLANDIĞI ÜLKELER (2016 İLK ÇEYREK)

SIRA	ÜLKE	BULAŞMA ORANI %
1.	ÇİN	27.24
2.	ABD	17.12
3.	TÜRKİYE	10.24
4.	BREZİLYA	8.60
5.	GÜNEY KORE	7.47
6.	HİNDİSTAN	6.67
7.	İSPANYA	6.32
8.	TAYLAND	5.65
9.	JAPONYA	5.55
10.	RUSYA	5.14

Kaynak: Havelsan Siber Güvenlik Bülteni, Sayı 8, Mart 2017 [9]

Tablo III'de yer alan rapora göre, Avrupa siber suçlar çerçevesinde Türkiye'de artan kimlik sahteciliğine dikkat çekilmiştir. İngiltere ile aynı oranda mobil ticari işlemin gerçekleştiği ve kendi ifadeleri ile "sayısal olarak ileri bir ülke" olma yolundaki Türkiye'de en yaygın saldırı sektörünün Avrupa'daki diğer tüm ülkelerden de yüksek seviyede kimlik sahteciliği (spooing) olduğu ifade edilmektedir [9].

C. 2016 Yılına Ait Genel Türkiye Siber Güvenlik İstatistikleri

Tablo IV ile gösterilen siber güvenlik istatistiklerine göre Türkiye siber saldırıların büyük çoğunluğunda ilk beşte yer almaktadır [9]. Bununla birlikte dünya çapında, haftada ortalama yüz binin üzerinde siber saldırı gerçekleştirilmektedir. Saldırıların sayısı kadar neden olduğu hasarın parasal boyutları incelendiğinde, yıllık 400 milyar dolar kayıptan bahsedilmekle birlikte 2019'da bu rakamın 2,1 trilyon doları bulacağı öngörülmektedir. Siber suçların her ülkenin gayrisafi yurt içi hasılasının ülkelere göre maliyeti hesaplandığında Türkiye'ye maliyetinin %7 olduğu bilinmektedir [10].

TABLO IV. 2016 YILI TÜRKIYE SIBER GÜVENLIK İSTATISTIKLERI

KONU	SIRA	YÜZDE
Kötücül Yazılım Bulaşma Oranı	2.	%18
DDoS Saldırıları Yapan Ülkeler	3.	%10.24
Sazan Avlama Tabanlı Kötücül Barındırma Oranı	10.	%1
Banka Truva Atı Kurbanları	4.	%2.77
Fidye Yazılım Ülke Dağılımı	4.	%6
'Humming Bad' Mobil Kötücül Yazılım Hedefleri	5.	%6

Kaynak: Havelsan Siber Güvenlik Bülteni, Sayı 8, Mart 2017 [9]

D. 2017 'nin En Önemli 5 Siber Güvenlik Gerçeği ve İstatistikleri

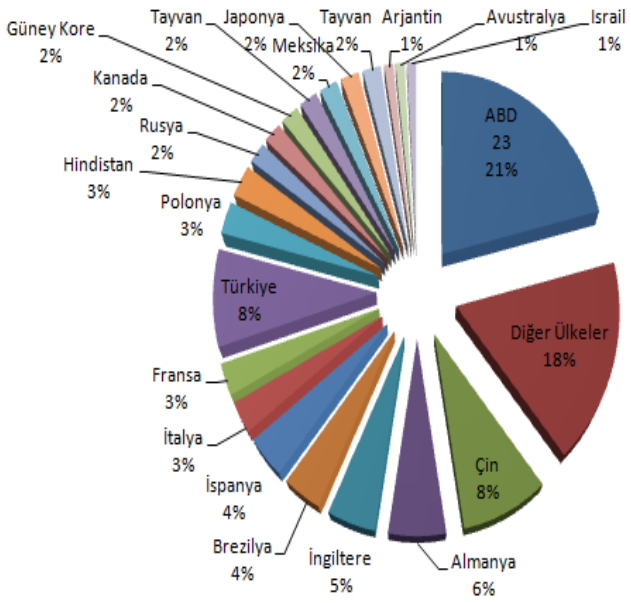
2017'nin en önemli 5 siber güvenlik istatistik sonuçları;

1. Siber suçlar 2021'e kadar 6 trilyon dolarlık bir zarara yol açacaktır.
2. Siber güvenlik harcamaları önümüzdeki 5 sene içinde 1 trilyon dolar sınırını geçecektir.
3. 2019 yılına kadar siber güvenlik alanında 1,5 milyon işgücü gerekecektir.
4. Saldırı hedefindeki insan sayısı 4 milyara ulaşacaktır.
5. 200 milyar IoT cihazı 2020 yılına kadar güvenlik altına alınmak zorundadır [11].

E. Siber Suçların Küresel Dağılımı

Şekil 1'de siber suçların küresel dağılımında Türkiye'nin sıralamasını görmekteyiz. Türkiye %8'lik dilime sahiptir.

Dünya genelinde Türkiye 9. sırada yer almaktadır. Yapılan araştırmalara göre siber saldırılar sebebiyle her 100 şirketten 44'ü arıza sorunu ile karşılaşmaktadır. Yine 100 şirketten 41'i fikri mülkiyette çalıntı sorunuyla karşılaşırken, şirketlerin %44'ü web sitesinin risk taşıdığını ifade etmektedir. 31'i ise bu süreçten direkt olarak maddi zarar gördüğünü ifade etmektedir [13].



Şekil 1. Siber Suçların Küresel Dağılımında Türkiye Sıralaması

Kaynak: NETAŞ Siber Güvenlik Sunumu - C. Müjdat Altay – 15 Haziran 2015 [12]

F. Emniyet Genel Müdürlüğü Siber Güvenlik İstatistikleri Faaliyet Raporları

Tablo-V ile T.C. İçişleri Bakanlığı Emniyet Genel Müdürlüğü'nün son üç yılına ait olan (2014, 2015, 2016), faaliyet raporları incelenmiştir.

TABLO V. 2014-2015-2015 YILLARı EGM FAALIYET RAPORLARı

Yıl	Adli Mercilere Sevk Edilen Şüpheli Sayısı
2014	2.788
2015	3.581
2016	6.648

Kaynak: T.C. İçişleri Bakanlığı Emniyet Genel Müdürlüğü 2014, 2015, 2016 Yılları Faaliyet Raporları [14, 15, 16]

Tablo V, son üç yılda, Türkiye'de siber suçlarda yaşanan artış oranını göstermektedir. 2014 yılında EGM tarafından adli mercilere sevk edilen şüpheli sayısı 2.788 iken, 2016 yılına gelindiğinde bu sayının 6.648'e ulaşmış olduğunu görmekteyiz. Faaliyet raporunda 2014'den 2016 yılına kadar geçen 2 yıllık sürede siber suçlarda neredeyse 2,5 kat artış olduğu görülmektedir.

G. 2015- 2016 Siber Güvenlik İstatistiklerine Genel Bakış

Tablo- VI'da son iki yıla ait kayıt altına alınmış siber güvenlik istatistikleri yer almaktadır.

Tablo VI. 2015- 2016 Siber Güvenlik İstatistikleri

Siber Güvenlik Ekonomisi:
1.Siber saldırıların tahmini global maliyeti yıllık 400 milyar dolar. (17.01.2016)
2.2019 yılında siber saldırıların tahmini küresel maliyeti yıllık 2,1 trilyon dolar olacak. (17.01.2016)
3.Veri ihlalinin küresel toplam maliyeti yıllık 3,8 milyar dolar. (04.02.2016)
4.Veri ihlalinin maliyeti 2013-2015 yılları arasında %23 arttı. (27.05.2015)
5.Veri ihlalinde her çalınan kayıt için oluşan ortalama tahmini maliyet 154 dolar. (27.05.2015)
6.Ekim 2013- Şubat 2016 tarihleri arasında işletmelerin e-posta sahtekârlığından dolayı yaşadığı kayıp 2,3 milyar dolar.
7.2016 yılında büyük sağlık kuruluşlarının %63'ü siber güvenlik için 1 milyon dolardan fazla harcama yapmayı planlıyor.
8.Siber sigorta pazar büyüklüğü: 2,5 milyar dolar. (16.10.2015)
9.Siber güvenlik farkındalık eğitimleri için yıllık 1 milyar dolar harcanıyor.
10.2020 yılında siber güvenlik pazarının global maliyeti yıllık 170 milyar dolar olacak.
11.2015 yılında siber güvenlikle ilgili startup'lara 3,8 milyar dolar yatırım yapıldı.
Siber Saldırıların Kişi Ve Kurumlara Yönelik Etkileri:
1. 2015 yılında rapor edilen veri ihlali sayısı: 781
2. Yıllık ortalama 80-90 milyon siber güvenlik olayı yaşanıyor.
3. Siber güvenlik olayları 2014-2015 yılları arasında %38 arttı.
4. 2015 yılında en fazla olan siber saldırılar; Kimlik avı ve kötü amaçlı yazılım.
5. 2015 yılında alıcıların %30'u kimlik avı ile ilgili mesajları açtı
6. 2015 yılında kimlik avı ile ilgili mesajları açan insanların %12'si kötü amaçlı dosyalara veya linklere de tıkladı.
7. Küçük ve orta ölçekli firmaların %20'si siber suç hedefinde bulunuyor. (2016)
8. Kötü amaçlı yazılımların %90'ı insan etkileşimi olmadan bulaşmıyor. (2016)
9. 2015 yılındaki web saldırılarının %95'i finansal kazanç için yapıldı. (2016)
10. Microsoft'un dijital altyapısında her gün gördüğü siber saldırı sayısı 10 milyonun üzerinde. (06.05.2016)
11. Tüketicilerin %40'ından fazlası kredi kartı veya bankamatik kartı dolandırıcılığı yaşıyor. (03.03.2016)
12. Çalışanların %85'i kişisel bilgileri şirketleri tarafından ihlal edildiğinde, negatif bir reaksiyon gösteriyor. (20.03.2016)
13. Çalışanların %33'ü şifrelerini iş arkadaşları ile paylaşıyor. (20.03.2016)
14. Çalışanların %20'si şifrelerini 3. şahıslara satıyor. (20.03.2016)
15. Saptanamayan siber atakların oranı: %70. (09.09.2015)
16. İşletmelerdeki karar mercilerinin %65'i gelecekte veri ihlaline uğrayacaklarını düşünüyor. (10.02.2016)
17. Şirketlerin %22'si verilerinin tamamıyla güvende olduğuna inanıyor. (2016)
18. 2016'da siber güvenlik ile ilgili 1 milyon iş açığı olacak. (12.02.2016)
19. 2015'in en kötü şifresi: 12345
En Çok Etkilenen Sektörler
1. 2015 yılında en çok saldırıya uğrayan sektör: Sağlık sektörü.
2. 2015 yılında en çok saldırıya uğrayan 2. sektör: İmalat sektörü.
3. 2015 yılında sağlık sektöründe rapor edilen veri ihlali sayısı: 277

Kaynak: Sibel Hoş Dijital Pazarlama ve İnfografik [17]

H. Türkiye İstatistik Kurumu Hanehalkı Bilişim Teknolojileri Araştırma Raporu 2016

Tablo VII Hanehalklarının internet kullanım oranlarını raporlamıştır.

Tablo VII. Hanehalkı Bilişim Teknolojileri İstatistikleri

Hanehalkları Bilişim Teknolojileri Kullanım Araştırması (2016)
1. İnternet kullanan bireylerin oranı %61,2 oldu
2. 10 hanenin 8'i internet erişim imkanına sahip
3. Hanelerin %96,9 'unda cep telefonu var
4. İnternet kullanım amaçları arasında sosyal medya ilk sırada
5. İnternet kullanan bireylerin %61,8 i e-devlet hizmetlerini kullandı
6. Bireylerin internet üzerinden mal ve hizmet siparişi %34,1 oldu
7. Düzenli internet kullanıcı sayısı 2016 Yılının İlk 3 ayında %94,9

Kaynak: Türkiye İstatistik Kurumu Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2016 [18]

Tablo VII'ye göre Hanehalklarının internet kullanım oranında ki yüksek artış dikkat çekici düzeydedir.

III. SİBER GÜVENLİKTE KAMU VE ÖZEL SEKTÖR İŞBİRLİĞİ

A.Türkiye'nin Siber Güvenlik Kurulu ve Ulusal Siber Güvenlik Stratejisi

Ulusal siber güvenliğimizin sağlanmasına ilişkin politika, strateji ve eylem planlanlarını hazırlamak ve koordinasyonunu sağlamak görevi T.C. Ulaştıma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir [6].

İlk olarak 20 Ekim 2012 tarihinde 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin karar Bakanlar Kurulu Kararı ile atılmıştır. Bu karar "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak, bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Siber Güvenlik Kurulu kurulmuştur [6]. Ulaştırma, Denizcilik ve Haberleşme (UDH) Bakanı'nın başkanlığını yaptığı kurul, Dışişleri, İçişleri, Milli Savunma, UDH Bakanlıkları müsteşarlarının yanı sıra, Kamu Düzeni ve Güvenliği Müsteşarı, MİT Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, BTK Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve UDH tarafından belirlenen bakanlık ve kamu kurumu üst düzey yöneticilerinden oluşmaktadır [19].

2012/3842 sayılı karar kapsamında UDH Bakanlığı'nn görevleri şunlardır [6].

- Ulusal Siber Güvenliğin sağlanması için politika strateji ve eylem planlarını hazırlamak,
- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usül ve esasları hazırlamak,
- Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,
- Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya bu sistemlerin denetimi işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak,
- Ulusal siber güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretimini teşvik etmek, kullanımını sağlamak,
- Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,
- Bu karar çerçevesinde diğer ülkeler ve uluslar arası kuruluşlarla işbirliği yapmak,

• Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı arttırma çalışmaları yürütmek,

• Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esasları belirleyerek güvenlik belgesi vermek,

• Siber Güvenlik Kurulunun sekreterya hizmetlerini yürütmek,

Bu karardan bir sene sonra; ülkemizde ilk ulusal siber güvenlik stratejisi, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından 2013-2014 eylem planı stratejisiyle oluşturulmuştur [20]. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem planının getirisi tehditlerin fark edilmesi ve uyarıların geliştirilip paylaştırılması amacıyla kurulan bir Siber Olaylara Müdahale Merkezi kurulması olmuştur. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve USOM koordinasyonunda çalışacak sektörel, Siber Olaylara Müdahale Ekiplerinin (SOME) kurulması çağrısını yapmıştır. USOM ayrıca kritik altyapı sektörleri ve kamu kurumları için sektörel SOME'ler kurmakla birlikte, eğitim ve koordinasyonun sağlanmasıylada görevlidir. Ocak 2015 itibariyle 720 personelle işletilen 245 kurumsal SOME kurulmuştur. Kurumsal SOME'lerin kurulmasını koordine etme görevi UDH'ye verilmiştir (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı). Siber Güvenlik Kurumu tarafından belirlenecek kritik sektörlerin sektörel SOME'leri olması mecbur kılınmıştır. Düzenleyici ve denetleyici kurumların sektörel SOME'leri BTK tarafından koordine edilmektedir [19]. Şu anda uygulamada olan strateji ise T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığının, 2016-2019 Ulusal Siber Güvenlik Stratejisidir [25].

B. Siber Güvenlik Riskleri

Siber güvenlik kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi için siber güvenlik riskleri gerçekçi bir biçimde değerlendirilmiş ve belirlenen başlıca riskler aşağıda sıralanmıştır [25].

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma vb. kritik hizmetlerin kesintiye uğraması.

2. Kamu ve kritik altyapıların kullandığı bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda; Vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

3. Araştırma, geliştirme ve üretim yapan kurum ve kuruluşların (özel firmalar, araştırma kurumları ve savunma sanayi) ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

4. Propaganda amaçlı bilgisayar korsanlığı (hacktivizm) saldırıları sonucu çeşitli kurum ve kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa olması, değiştirilmesi veya yok edilmesi.

5. E-ticaret yapan kuruluşların, E-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların hizmet dışı bırakma ve benzeri saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin saldırganlar tarafından ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda çevrimiçi işlemlere yönelik güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.

7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

8. Toplumun internete ve sosyal ağlara olan bağımlılığı, siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.

9. Her türlü kurum ve kuruluşta yığın posta, kötücül yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla karşı karşıya kalınması.

10. Her türlü kurum ve kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması.

C. Ortak Akıl Platformu

Siber Güvenlik Stratejisi ve Eylem Planı T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı nezdinde hazırlanırken; kamu kurumları, kritik alt yapı işletmeleri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzman katılımıyla (Ortak Akıl Platformu) gerçekleştirilmiştir [7]. Bu platformun hedefleri [8];

• Kurumsal Siber Olaylara Müdahale Ekibi (SOME) kurulması gereken kamu kurumlarında siber güvenlik bütçesinin oluşturulması.

• SOME'lerde çalışan siber güvenlik personelinin iş tanımlarının belirlenmesi.

• Kurumlarda sızma testlerinin zorunlu hale getirilmesi.

• Kamu ve kritik altyapı sistem odalarının sahip olması gereken asgari kriterler.

• Siber suçlar ile ilgili ceza ve muhakeme mevzuatının düzenlenmesi.

• Güvenli IPv6 kullanımının yaygınlaştırılması.

• Milli adli analiz kapasitesinin geliştirilmesi.

• Adli analiz uzman havuzu oluşturulması ve kriterlerinin belirlenmesi.

• Siber suçları tespit için büyük veri analizi altyapısının

kurulması.

- Siber güvenlik terimleri sözlüğünün oluşturulması.
- İlk, orta, lise ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması.
- Siber güvenlik yaz kampları, yarışmaları ve tatbikatlarının düzenlenmesi.
- Bilişim hukukcusu yetiştirilmesi.
- Siber güvenlik farkındalığı kamu spotlarının oluşturulması.
- Yüksek lisans ve doktora düzeyinde siber güvenlik ders içeriklerinin oluşturulması.
- Siber güvenlik ekosistemi ulusal iş modelinin oluşturulması.
- Siber güvenlik teknoloji yol haritasının ve araştırma gruplarının oluşturulması.
- Siber güvenlikle ilgili yerli teknoloji ve ürünlerin desteklenmesi.
- "Güvenli yazılım geliştirme ve güvenli yazılım kullanımı" kültürünün yaygınlaştırılması.
- Pardus'un yaygınlaştırılması.
- Labaratuar/test yatağı alt yapısının kurulması ve kritik siber güvenlik teknolojilerinin kazanımı.
- Kritik ürünleri denetleyecek ve sertifikalandıracak mekanizmaların çalıştırılması.
- Ulusal Siber Güvenlik Portalı'nın oluşturulması.

D. Bilgi Güvenliği Farkındalık Anketleri Sonuçları

Gerek yazılı basında gerek görsel basında siber güvenliğe ilişkin kamu ve özel sektör işbirliğinin gerekliliği sürekli vurgulanmaktadır [24]. Bununla birlikte araştırma şirketlerince kamuoyu araştırmalarına yönelik bir çok anket çalışması yapılmıştır. [26,27]. Kritik altyapı şirketlerinde çalışan bilgi teknolojileri (BT) yöneticilerinden ankete katılan katılımcıların %86'sı siber güvenlik tehditlerine karşı tedbir alınması gerektiğini düşünmektedir [24]. Katılımcıların %76'sı ulusal sınırlar içerisinde kritik bir altyapı şirketi, siber tehdit altında zarar gördüğünde, ulusal savunma gücünün müdahale etmesi gerektiğini düşünmektedir. Ankete katılan şirketlerin %70'i saldırıların giderek arttığını düşünmektedir. Ankete yanıt verenlerin %48'i önümüzdeki 3 yıl içerisinde kritik altyapılara, yüksek ihtimalle siber saldırı gerçekleştirileceğini ve bu saldırıların büyük ihtimalle insan hayatına mal olacağını düşünmektedir. Ankete yanıt verenlerin %89'u son 3 yıl içerisinde güvenli olduğunu düşündükleri şirketlerinde en az bir saldırı yaşadıklarını söylemektedir. Yılda ortalama 20 saldırı yaşanmakta ve bu saldırıların sonucunda %41 fiziksel hasar yaşandığı belirtilmektedir. Konu hakkında her ülke farklı bakış açısına sahiptir. ABD kaynaklarının %18'i önümüzdeki 3 yıl içerisinde bu senaryoların gerçekleşme ihtimalini doğrulamaktadır.Diğer taraftan Almanyada ki katılımcıların %2 'si ile Birleşik Krallıktaki katılımcıların sadece %3 'ü bu ihtimalin çok yüksek olduğunu dile getirmektedirler [24].

Bir başka bilgi güvenliği farkındalık anketi sonuçlarına gore; "Kurumunuzda düzenli işleyen bir siber güvenlik farkındalık programı var mı?" sorusuna katılımcıların %65'i hayır, %35'i evet yanıtını vermiştir. "Bir bilgi güvenliği ihlali olduğunda bunu kime bildirirsiniz?" sorusuna katılımcıların % 28'i kendim çözmeye çalışırım şeklinde yanıtlamıştır. % 59 'u çalıştığım firmanın güvenlik birimine iletirim demiş, % 10'u devletin kolluk makamlarına bildiririm şeklinde ifade etmiştir. "Kurumunuz kullanıcıların şirket dışında olduğu durumlarda, güvenli internet erişimi için size erişim seçeneği sunuyor mu?" sorusuna %57'si SSL–VP cevabını verilmiştir. Bir çok kurumun bu konuda bilinçli davrandığı ifade edilmektedir. Ancak kurumların %36'sı hayır sunmuyor cevabını vererek, bazı kurumların siber saldırılara karşı, doğru savunma gerçekleştirmediklerini yada kullanıcıların bundan haberdar olmadıklarını ifade etmişlerdir. "Siber güvenlik farkındalığı programınız, eğitimin yanısıra davranış değişikliği yaratacak materyaller sunuyor mu?" sorusuna %59'u Hayır cevabını vermiştir. Soruda %32 oranında oltalama kampanyaları cevabı 2. sırada gelmekte birlikte, kullanıcılara dikkat ve beceri kazandırıracak çalışmaların yapıldığına dikkat çekilmektedir. Anketin son sorusunda, "Oltalama saldırılarına karşı e-posta servisinizi ne sıklıkla kullanıyorsunuz?" sorusuna katılımcıların %47'si test ettirmiyoruz cevabını vermiştir. %33'ü sızma testlerine baktırıyoruz cevabını verirken %20'si yeni tehditler çıktıkça test ettiriyoruz cevabını vermiştir [26].

E. Milli İşletim Sistemimiz Pardus

Pardus 2003 yılında temelleri atılan milli işletim sistemi olan, Türkiye'de TÜBİK–UEKAE tarafından geliştirilen, özgür, hızlı kurulabilen, kolay kullanılır, çok dil içeren, bilgisayar kullanıcılarının temel masa üstü ihtiyaçlarını gidermek üzere hali hazırdaki linux dağıtımlarının üstün taraflarını kullanan, kurulum, yapılandırma ve kullanım kolaylığı sağlayan açık kaynak kodlu bir işletim sistemidir. Pardus'un bugüne kadar yayınlanmış 5 ana sürümü ve 9 ara sürümü mevcuttur. Bu bilgilere ek olarak 2 kurumsal sürümü vardır. Pardus'un adı Anadolu Parsı'nın bilimsel adı olan Panthere Pardus Tulliana'dan gelmektedir.

Pardus'un Özellikleri:

- Açık kaynaklıdır.
- GPL lisanslıdır.
- Özgürdür.
- Adını Anadolu panterinin isminden alır.
- TÜBİTAK–UEKAE tarafından gerçekleştirilen bir işle tim sistemidir.
- Ücretsiz olarak sürünümler sayfasından edinilebilir [29].

Mevcut ve yeni geliştirilen ürünlerin milli işletim sistemi PARDUS'a uyumlu hale getirilmesi için çalışmalara başlanılmalıdır. PARDUS'un herbir parçasının ve yazılımının yerli üretim olması, kullanımının yaygınlaştırılmasında büyük öneme sahiptir [27]. Kamu ve özel sektör PARDUS işletim sistemine birlikte entegre edilmelidir [28].

F. Endüsti 4.0 ve Siber Güvenlik Üzerindeki Etkileri

Endüstri 4.0 Nedir? Endüstri 4.0; 4. Sanayi Devrimi ya da 4. Endüstri Devrimi olarak da adlandırılır. Dünyada ilk kez 2011'de Almanya Hannover Fuarı'nda kullanılan bu terim, 2012 sonlarında Alman Federal Hükümeti'ne "4. Sanayi Devrimi öneri dosyası" olarak sunulmuştur, 2013 yılında da Endüstri 4.0 raporu halini almıştır. 4. Endüstri Devrimi, üretim sektöründe artan rekabet sonucu Almanya tarafından geliştirilen bir strateji olarakda nitelendirilebilir [31].

Endüstri 4.0, genel olarak 3 yapıdan oluşmaktadır.

- Nesnelerin interneti
- Hizmetlerin interneti
- Siber-Fiziksel sistemler

Endüstri 4.0 ile modüler yapılı akıllı fabrikalar kapsamında fiziksel işlemleri siber fiziksel sistemlerle izlemek, fiziksel dünyanın sanal bir kopyasını oluşturmak ve merkezi olmayan kararların verilmesi hedeflenmektedir. Nesnelerin interneti ile siber fiziksel sistemler birbirleriyle ve insanlarla gerçek zamanlı olarak iletişime geçip işbirliği içinde çalışabilecektir [32].

Endüstri 4.0 ile oluşacak yeni iş kollarının tamamı yönetim ve bilişim sistemlerine dolayısıyla siber ortam ve siber uzaya entegre olacaktır. Tüm sistemlerin dijitalleştiği, Endüstri 4.0 ile aktif hale gelecek 7 yeni iş kolu bulunmakla birlikte, her sektörde ve branşta yeni iş kolları sayılarının artması beklenmektedir. Endüstri 4.0 ile yeni iş kolları aşağıdaki gibi sıralanmıştır.

- Endüstriyel yazılım programcıları
- Bilişim sistemleri ve nesnelerin interneti çözüm üreticisi
- Endüstriyel veri analiz uzmanı
- Robot koordinatörü, programcısı, tamircisi
- Üretim teknoloji uzmanı
- Akıllı şehirler planlayıcılar
- Ürün tasarımcı ve üreticiler

Yeni meslek dallarının tamamı programlama, yazılım, tasarım ve donanım ağırlıklı olmaktadır. [33]. Tüm sektörel faaliyetlerin dijital ortama kaydığı endüstri 4.0 ile ulusların siber güvenlik politikaları iyileştirilmeli ve geliştirilmelidir.

Siber fiziksel sistemlerin üretim, lojistlik ve hizmetlerle entegrasyonu sonucunda bugünün fabrikalarının kayda değer ekonomik potansiyele sahip Sanayi 4.0 fabrikalarına dönüşmesi mümkün olacaktır [34]. Alman ulusal bilim ve mühendislik akademisi (acatech) 2013 yılında sanayi 4.0'ın temel düşüncesini 'manifesto' olarak yayımlamasıyla konu kuramsal çerçeveye oturtulmuştur. Acatech'in Sanayi 4.0 forumunun final raporunda (acatech 2013) bu yeni dönemin getirmekte olduğu ayırt edici yenilikleri şöyle sıralamaktadır;

- Depolama sistemleri ve kaynakları ile makinaların global etkileşimi,
- Konum bilgisine sahip benzersiz akıllı ürünlerin gelişimi,
- Ürün özelliklerine adapte olan, kaynak optimizasyonunu sağlayan akıllı fabrikaların hayata geçmesi,
- Yeni iş modelleri ve hizmetlerinin gerçekleşmesi,
- Çalışanlar için işyerlerinde yeni sosyal altyapı, bireysel farklılıklara duyarlı iş yapısı,
- Daha iyi iş ve yaşam dengesi,
- Bireysel tüketici isteklerine yanıt verme,
- Anında mühendislik ve problemlere anlık cevap için geliştirilmiş akıllı yazılımlar [35].

Bilgi ve veri güvenliği, endüstri içinde kritik bir öneme sahiptir. Üretimdeki her noktanın birbiriyle güvenli şekilde iletişim kurabilmesi, farklı tesislerin etkileşime girebilmesi, üretimde optimizasyonun temel anahtarlarından birini oluşturmaktadır. Tüm dünyada gerçekleşen bu süreçlerin temeli, bilgi ve veri aktarımına dayanmaktadır. Günümüzde rekabetin böylesine yoğun olduğu bir ortamda aktarılan verilerin güvenliğinin sağlanması büyük öneme sahiptir. Özetle Endüstri 4.0 hem siber güvenlik ortamlarını sağlamada hemde Siber Güvenlik'ten yararlanmada çok önemli bir noktada bulunmaktadır [36].

IV. TİCARİ İŞLETMELERİN SİBER GÜVENLİK FARKıNDALıĞı ÜZERİNE YAPıLAN BİR ANKET ÇALIŞMASı VE ELDE EDİLEN BULGULAR

Balıkesir ilinin Bandırma ilçesinde, sağlık, eğitim, sanayi, finans, toptan-perakende ve muhasebe sektörlerinde faaliyette bulunan 30 adet ticari işletmenin çalışanları üzerinde, siber güvenlik farkındalığı anket çalışması yapılmıştır. Ankette siber güvenlikte kamu ve özel sektör işbirliğine ticari işletmelerin bakış açıları sorgulanmıştır. Katılımcılara toplamda 7 adet soru yöneltilerek alınan yanıtların frekans dağılımları ve histogramı incelenmiştir. Ticari işletmelerin sektörlere göre dağılımı tablo VIII ile gösterilmiştir. Tablo VIII 30 Adet ticari işletme üzerinde yapılan araştırmada kayıp veri olmadığını ve ankete katılan tüm ticari işletmelerin soruları eksiksiz olarak yanıtladığını göstermektedir. Anket çalışmasının soruları, bilgisayar mühendisliği anabilim dalında bir doktora tezi olan; Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü başlıklı tez çalışmasından esinlenerek oluşturulmuştur [30].

Tablo VIII. Sektörlere Göre Frekans Dağılımları

	Freguency	Percent	Valid Percent	Cumulative Percent
Valid Finans	2	6,7	6,7	6,7
Sağlık	4	13,3	13,3	20,0
Eğitim	7	23,3	23,3	43,3
Sanayi	6	20,0	20,0	63,3
Toptan - Perakende	8	26,7	26,7	90,0
Muhasebe	3	10,0	10,0	100,0
Total	30	100,0	100,0	

A. Kuramsal Çerçeve

Genel olarak gerek yazılı gerek görsel basında, siber güvenlikte kamu ve özel sektör işbirliğinden bahsedilmektedir. Özellikle son yıllarda artış gösteren siber saldırılar, ülkelerin gündemini daha fazla meşgul eder olmuştur. Bu noktada uluslar var olan siber güvenlik politikalarını sorgulamaya başlamakla birlikte siber güvenlik politikalarınıda güncellemeye başlamışlardır. Ülkemizde ulusal siber güvenlik politikaları ve siber güvenlik tedbirleri kamu sektöründe ve özel sektörde farklılık göstermektedir. Siber güvenlikte kamu kurum ve kuruluşları daha profesyonel ve nitelikli korunurken özel sektör kendi olanakları ve bilgi birikimleri dahilinde korunmaktadır. İki sektör arasında var olan farklı siber güvenlik uygulamaları ve politikaları, bilgiyi korumayı güçleştirmektedir. Günümüz dünyasında ulusların serveti bilgi güvenliğidir. Bir örnekle açıklamak gerekirse; Su bilinmeyen bir yerlerden sızıyorsa fatura mutlaka yüksek gelecektir. Bu doğrultuda siber güvenlikte kamu ve özel sektör işbirliğinin hayata geçirilmesi büyük öneme sahiptir.

B. Araştırma Yöntemi

Araştırma saha araştırması şeklinde nicel araştırma deseni çerçevesinde gerçekleştirilmiştir.

C.Evren ve Örneklem

Araştırmanın evreni küçük, büyük ve orta ölçekli ticari işletmelerdir.30 Adet küçük, orta ve büyük ölçekli işletme üzerinde çalışılmıştır.

D. Veri Toplama Aracı

Araştırmada veri toplama aracı olarak literatür taraması yapılmış araştırmacıların meta analizlerinden yararlanılarak anket tekniği kullanılmıştır. İşletmelere 7 adet soru yöneltilmiştir. Soruların frekans istatistik dağılımı ve histogramı üzerinden değerlendirmede bulunulmuştur.

E. Siber Güvenlikte Kamu Ve Özel Sektörişbirliği Farkındalık Anketi Soruları ve Sonuçlar

1.Soru: Kurumunuza yapılan bir siber saldırı kurum imajını ve kurum maliyetlerini etkiler mi? Sorusunun frekans dağılımlarının istatistiği IX. Tablo ile gösterilmektedir. Merkezi eğilim ölçülerinin ortalaması alındığında %100 Evet sonucuna ulaşılmıştır. Ankete katılan şirketlerin tamamı siber saldırıların kurum imajını ve kurum maliyetlerini etkilediğini düşünmektedir.

Tablo IX. Frekans İstatistik Dağılımı

	Freguency	Percent	Valid Percent	Cumulative Percent
Valid Evet	30	100,0	100,0	100,0

2. Soru: Katılımcılara " Olası bir siber saldırı durumunda kamu sektöründe var olan kurum ve kuruluşlardan nasıl yardım alabileceğimi biliyorum" Likert ölçekli değerlendirme sorusuna, katılımcıların yalnızca %33,3'ü Katılıyorum ve Kesinlikle Katılıyorum yanıtını verirken kalan %66,6'sı konu hakkında bilgi sahibi olmamakla birlikte olası bir siber saldırı durumunda ne yapacaklarını bilememektedirler. Detaylar X. Frekans İstatistik Dağılımı Tablosu ile gösterilmektedir.

Tablo X. Frekans istatistik Dağılımı

	Freguency	Percent	Valid Percent	Cumulative Percent
Kesinlikle Katılmıyorum	4	13,3	13,3	13,3
Katılmıyorum	6	20,0	20,0	33,3
Kararsızım	10	33,3	33,3	66,7
Katılıyorum	7	23,3	23,3	90,0
Kesinlikle Katılıyorum	3	10,0	10,0	100,0
Total	30	100,0	100,0	

3.Soru: Katılımcılara yöneltilen 'Olası bir siber saldırı durumunda kamu kurum ve kuruluşlarından alacağımız yardım kurumumu güvende hissettirir' Likert ölçekli değerlendirme sorusuna katılımcıların %86,7'si Kesinlikle Katılıyorum ve Katılıyorum yanıtını vererek siber güvenlikte kamu sektöründen yardım almak istediklerini beyan etmişlerdir. Detaylar XI. Frekans İstatistik Dağılımı Tablosu ile gösterilmektedir.

Tablo XI. Frekans İstatistik Dağılımı

	Freguency	Percent	Valid Percent	Cumulative Percent
Katılmıyorum	2	6,7	6,7	6,7
Kararsızım	2	6,7	6,7	13,3
Katılıyorum	11	36,7	36,7	50,0
Kesinlikle Katılıyorum	15	50,0	50,0	100,0
Total	30	100,0	100,0	

4. Soru: Katılımcılara yöneltilen" Siber güvenlikte uzman kamu kurum ve kuruluşların kurumumuza verdiği eğitimler kurumumuzu siber tehditlere karşı güçlendirir" Likert ölçekli değerlendirme sorusuna katılımcıların %90'ı Katılıyorum ve Kesinlikle katılıyorum yanıtını vererek bu tür eğitimlere ihtiyaç duyduklarını beyan etmişlerdir. Detaylar XII. Frekans İstatistik Dağılımı Tablosu ile gösterilmektedir.

Tablo XII. Frekans İstatislik Dağılımı

	Freguency	Percent	Valid Percent	Cumulative Percent
Kararsızım	3	10,0	10,0	10,0
Katılıyorum	10	33,3	33,3	43,3
Kesinlikle Katılıyorum	17	56,7	56,7	100,0
Total	30	100,0	100,0	

5. Soru: Katılımcılara yöneltilen 'Kurumumuzda siber tehditlere karşı oluşturulan bir siber güvenlik eylem planı var' Likert ölçekli değerlendirme sorusuna katılımcıların %73,3'ü katılmamakta ve kararsız kalmaktadırlar. Bu sonuç şirketlerin büyük çoğunluğunun, siber saldırılara karşı savunmasız olduklarını göstermektedir. Detaylar XIII. Frekans İstatistik Tablosu ile gösterilmektedir.

Tablo XIII. Frekans İstatistik Dağılımı

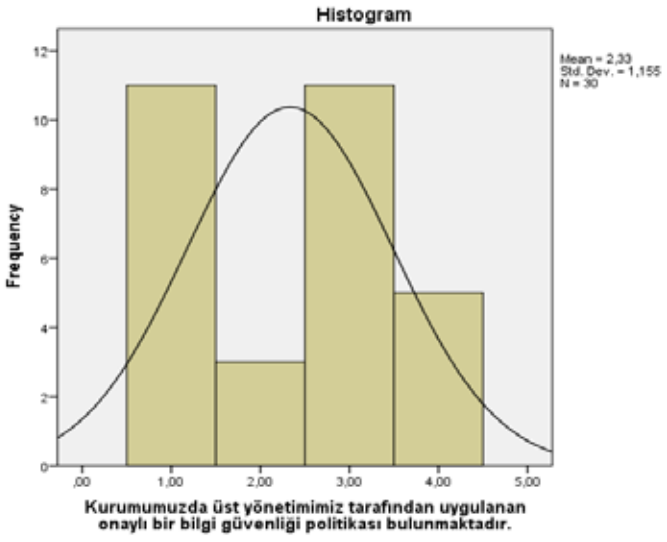
	Freguency	Percent	Valid Percent	Cumulative Percent
Kesinlikle Katılmıyorum	9	30,0	30,0	30,0
Katılmıyorum	3	10,0	10,0	40,0
Kararsızım	10	33,3	33,3	73,3
Katılıyorum	3	10,0	10,0	83,3
Kesinlikle Katılıyorum	5	16,7	16,7	100,0
Total	30	100,0	100,0	

6. Soru: Katılımcılara yöneltilen 'Kurumumuzda siber tehditlere karşı eğitim veriliyor' Likert ölçekli değerlendirme sorusuna katılımcıların %80,1'i katılmamakla birlikte kararsız kalmaktadırlar. Bu sonuç şirketlerin büyük çoğunluğunun siber saldırılara karşı savunmasız olduklarını yinelemektedir. Detaylar XIV. Frekans İstatistik Tablosu ile gösterilmektedir.

Tablo XIV. Frekans İstatistik Dağılımı

	Freguency	Percent	Valid Percent	Cumulative Percent
Kesinlikle Katılmıyorum	17	56,7	56,7	56,7
Katılmıyorum	5	16,7	16,7	73,3
Kararsızım	2	6,7	6,7	80,0
Katılıyorum	5	16,7	16,7	96,7
Kesinlikle Katılıyorum	1	3,3	3,3	100,0
Total	30	100,0	100,0	

7. Soru: Katılımcılara yöneltilen 'Kurumumuzda üst yönetimimiz tarafından uygulanan onaylı bir bilgi güvenliği politikası bulunmaktadır'Likert ölçekli değerlendirme sorusunda, ankete katılan şirket çalışanlarının bilgi güvenliği politikası değişkenin histogramı incelenmiştir. Şekil 2'de ankete katılan şirket çalışanlarının, şirket bilgi güvenliği politikalarının varlığı sorgulandığında büyük çoğunluk şirketlerinin bilgi yönetimi politikalarının olmadığını ifade etmiştir. Şekil 2'nin yatay ekseninde gösterilen 1. Bölgede katılımcılar, işletmelerinin onaylı bir bilgi güvenliği polikalarının olduğuna kesinlikle katılmamaktadırlar. 2. Bölgede onaylı bir bilgi güvenliği politikaları olduğuna katılmadıklarını ifade etmektedir. 3. Bölge ise kararsız kaldıklarını göstermektedir. Şirketlerin onaylı bir bilgi güvenliği politikalarının olduğu kabul edilen, 'Kesinlikle katılıyorum' 5.Bölge ile gösterilmiş ve katılımcılar tarafından tamamen reddedilmiştir. Detaylar Şekil 2 ile gösterilmektedir.



Şekil 2. Bilgi Güvenliği Politikası Değişkeni Histogramı

F. Anket Çalışmasının Güvenilirlik Analizi Sonuçları

Tablo XV. İle anket çalışmasının güvenilirlik analizi sonucu gösterilmiştir. Cronbach's Alpa sorular arası korelasyona bağlı uyum değeridir. Cronbach's Alpa değeri, 0,70 ve üzeri olduğunda ölçeğin güvenilir olduğu kabul edilir. XV. Tabloda görüldüğü gibi soruların tamamı birlikte kullanıldığında Cronbach's Alpa değeri 0,897 bulunmuştur. Bu değer ölçeğin güvenilir olduğunu göstermektedir. Sorular anlamlı şekilde bir araya gelmiştir.

Tablo XV. Güvenilirlik Analizi Alpa Değeri

Cronbach's Alpha	N of Items
,897	28

V. SONUÇLAR

Paylaşılan tüm bilgiler ışığında; Siber güvenlikte kamu ve özel sektör arasındaki işbirliği her ne kadar sıklıkla dile getiriliyor olsada, aralarında olması gereken iletişim ve bilgi akışı mekanızmasının eksik çalıştığı, uygulamada var olan bir sistem olsa bile bu sistemin doğru çalışmadığı tespit edilmiştir. Ticari işletmelerin büyük çoğunluğu siber tehditler altında yalnız olmakla birlikte siber tehditlere karşı kamu kurum ve kuruluşlarından yardım talep etmekte ve siber tehditlere karşı kamu kurum ve kuruluşlarından eğitim almaya ihtiyaç duymaktadırlar. Ayrıca ticari işletmelerin siber güvenlik konusunda bilinçli olmadıkları tespit edilmiştir. Bir diğer ilgi çekici nokta; İşletmeler siber saldırıların kurum imajını ve kurum malliyetlerini etkilediğine katılmakla birlikte stratejik olarak tepkisiz kalmaktadırlar. Bu doğrultuda; Var olan tüm kurum ve kuruluşlarımızın siber güvenlik konusunda ki çalışmaları ayrı ayrı değerlendirmeye alınmalı, faaliyet ve hizmet alanları genişletilmelidir. Siber güvenlik açığının oluşmaması için yeterli düzeyde siber güvenlik uzmanı yetiştirilmelidir. Teknolojik gelişim ve yenilenmeyle birlikte siber güvenlik uzmanlarına olan ihtiyaç gün geçtikçe artmaktadır. Gelecekte oluşması muhtemel siber tehditlere yönelik bilişim hukukunda ihtisaslaşmış uzman yetiştirilmeside son derece önemlidir. Üniversitelerin hukuk fakülteleri bilişim hukukunda ulusal ve uluslararası düzeyde araştırma ve geliştirme faaliyetleri düzenlemeli, hukuk fakültesi öğrencileri bilişim hukukuna yönlendirilmelidir. Yeterli düzeyde bilişim hukukcusu yetiştirilmediği takdirde tüm siber güvenlik çalışmaları sonuçsuz kalacaktır. Bir diğer önemli nokta, İktisadi ve İdari Bilimler Fakülteleri ile Sosyal Bilimler Enstitülerinde teknoloji yönetimleri üzerine ders programlarının açılıp derslerin verilmesidir. Üniversite yıllarında oluşturulan siber güvenlik eğitimleri, ülkelerin siber güvenlik maliyetlerini yüksek oranda azaltarak bu alana ayrılan fonların, farklı alanlarda kullanılmasına katkı sağlayacaktır. Ayrıca üniversitelerde siber güvenlik enstitülerinin kurulması ve yaygınlaştırılması desteklenmelidir. Siber güvenlik enstitüleri ticari işletmelerede hizmet verecek şekilde yapılanmalıdır. Siber saldırılar her ne kadar teknik bir sorun olarak gözükmekte olsada bu saldırıların ekonomik ve sosyal maliyetleride bulunmaktadır. Açılmış yada açılacak olan tüm siber güvenlik enstitülerinde fen bilimciler ve sosyal bilimciler birbirlerine entegre olacak şekilde çalışmalar yapmalıdır. Fen bilimciler teknik sorunlarla ilgilenirken, sosyal bilimciler saldırıların sosyal ve ekonomik boyutuyla ilgilenerek tüm ticari işletmelere enstitülerde danışmanlık hizmeti vermelidirler. Bu ortak çalışmayla bir bakıma ABD'de hayata geçirilen silikon vadisi, ülkemizde de hayata geçirilmiş olacaktır. Silikon vadisi şeklinde yapılanmalara zaman kaybedilmeden başlanılmalıdır. Özellikle sanayi, lojistik ve dış ticaretin yoğunlaştığı bölgelerde siber güvenlik enstitülerinin kurulması büyük önem arz etmektedir. Daha net bir ifadeyle, siber güvenlikte kamu ve özel sektör işbirliği çalışmalarında üniversiteler bir araç olarak kullanılmalı ve değerlendirilmelidir. Bilgi Teknolojileri ve İletişim Kurumunun bölge müdürlük sayılarının çoğaltılması düşünülmesi gereken bir diğer önemli noktadır. Teknolojik hizmet sunan yerli ve yabancı, bilgisayar ve internet güvenliği şirketleriyle siber güvenlik hizmeti sunan bilgisayar yazılım ve danışmanlık şirketlerinin yıllık faaliyet raporları her yıl siber güvenlik stratejisinden sorumlu olan T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığına gönderilmeli ve ilgili bakanlık müfettişlerince denetlenmelidir. Milli işletim sistemimiz olan PARDUS'un geliştirilmesi ve yaygınlaştırılması için TÜBİTAK ve ULAKBİM desteklenmeli, yeterli düzeyde AR-GE yatırımı yapılmalıdır. Devlet tarafından üniversitelere ve danışmanlık şirketlerine AR-GE desteği sağlanmalıdır. Endüsrtri 4.0 ile birlikte tüm siber güvenlik sistemlerimizde değişmeli ve geliştirilmelidir. Daha etkin bir siber güvenlik politikası için daha fazla kaynak ayrılmalıdır. Türk mühendis odaları birliğinin etkinliği ve faaliyet alanları genişletilmelidir. Bu odalar tarafından tüm ticari işletmelerin bilgi işlem servisleri denetlenmeli ve işletmelerin siber güvenlik eğitimleri desteklenmelidir. Tüm illerdeki halk eğitim merkezleri vatandaşlara siber güvenlik eğitimi verecek şekilde yapılanmalıdır. Böylelikle toplumsal siber farkındalık oluşturulmuş olacaktır. Siber Güvenlikte özellikle uluslararası platformlarda ortaklıklar kurulmalı, üniversitelerle ortak çalışılmalıdır. Siber güvenlik pazarının ulusallaşması bir diğer önemli noktadır. Siber güvenlik pazarına yatırım yapılmalı ve ürün gelişimi desteklenmelidir. Aksi takdirde sürekli gelişen ve değişen bu pazarda dışarıya yüksek miktarda kaynak aktarmak kaçınılmaz olacaktır. Bu sorun ilerde dış ticaret açığı ,cari açık ve nihayetinde milli gelirimize olumsuz yönde etki ederek ülke ekonomisini geriye taşıyacaktır. Özellikle finans sektöründe hizmet veren finansal kuruluşların ve bankaların, müşterilerine ulusal siber güvenlik politikalarımızda etkili olacak bilgilendirici sms'ler göndermesi, yazılı ve görsel yayında kullanılacak kamu spotları, siber güvenlikte farkındalık yaratacak bir başka yol olacaktır. Finansal kuruluşların ve bankaların ulusal siber güvenlik politikalarımıza katkıları Bankacılık Düzenleme ve Denetleme Kurumu ile Sermaye Piyasaları Kurulu tarafından ayrıca takip edilmelidir. Danışmanlık şirketileri ve üniversiteler aracılığıyla her ilde düzenli aralıklarla siber güvenlik akademileri kurulmalı ve yaygınlaştırılmalıdır.

KAYNAKLAR

[1] http://openaccess.bilgi.edu.tr:8080/xmlui/bitstream/handle/11411/60/G%C3%B6k_5651%20Say%C4%B1l%C4%B1%20Kanun_2013.pdf?sequence=1&isAllowed=y Erişim Tarihi;07.07.2017

[2] http://www.mahfiğilmez.com/2017/05/endustri-40.html. Erişim Tarihi; 08.07.2017.

[3] (http://www.fortuneturkey.com/akilli-uretim-cagi-endustri-40-42841 Erişim Tarihi; 08.07.2017.

[4] www.digisophia.com/Article/Details/34. Erişim; 08.07.2017

[5] www.havelsan.com.tr/TR/Main/haber/3406/akademisyenler-"siber-güvenlik"-için-bir-arada Erişim Tarihi; 08.07.2017

[6] www.resmigazete.gov.treskiler/2012/10/20121020-18.htm/ Erişim Tarihi; 08.07.2017

[7] www.haber51com/siber-güvenlikte-yeni-dönem_d90.html Erişim Tarihi; 08.07.2017

[8] http://webrazzi.com/2016/09/09/bugun-aciklanan-ulusal-e-devlet-ve-siber-guvenlik-strateji-ve-eylem-planlarinda-hangi-hedefler-var/ Erişim Tarihi; 08.07.2017

[9] www.havelsan.com.tr/files/files/HSB%208_sayı.pdf

Erişim Tarihi; 08.07.2017

[10] www.cybermagonline.com/siber-güvenlik-pazari-bas-donduruyor ErişimTarihi; 09.07.2017

[11] https://siberest.com.tr/2017nin-en-onemli-5-siber-guvenlik-gercegi-ve-istatistikleri Erişim Tarihi; 09.07.2017

[12] https://www.slideshare.net/melihbayramdede/neta-siber-gvenlik-sunumu-15-haziran-2015 ,Erişim Tarihi; 29.06.2017

[13] https://www.haberler.com/siber-saldiriya-ugrayan-100-sirketten-31-i-kar-8181968-haberi/ Erişim Tarihi; 10.07.2017

[14] http://www.sp.gov.tr/upload/xSPRapor/files/jW60O+EGM_2014_yili_idare_faaliyet_raporu.pdf Erişim Tarihi; 10.07.2017

[15] https://www.egm.gov.tr/SiteAssets/Sayfalar/StratejiGelistirmeFaaliyetleri/EGM%20FAALIYET%20RAPORU%202015.pdf Erişim Tarihi; 10.07.2017

[16] https://www.egm.gov.tr/Documents/EGM2016FaaliyetRaporu.pdf Erişim Tarihi; 10.07.2017

[17] http://www.sibelhos.com/siber-guvenlikle-ilgili-en-ilginc-35-istatistik ,Erişim Tarihi;28.06.2017.

[18] http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779 Erişim Tarihi ; 10.07.2017

[19] http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf Erişim Tarihi; 10.07.2017

[20] http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf Erişim Tarihi; 10.07.2017

[21] http://www.milliyet.com.tr/sibel-saldiri-nedir--teknoloji-haber-1991343/ Erişim Tarihi; 10.07.2017

[22] https://www.fraudandchargeback.com/tr/siber-saldirilara-karsi-bankalarimiz-ne-kadar-guvenli Erişim Tarihi; 10.07.2017

[23] http://donencebilisim.com/siber-saldiri-turleri-nelerdir.html Erşim Tarihi; 10.07.2017

[24] https://www.haberler.com/siber-guvenlik-konusunda-kamu-ozel-sektor-7532272-haberi/ Erişim Tarihi; 11.07.2017

[25] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf Erişim Tarihi; 11.07.2017

[26] https://www.bgasecurity.com/2017/03/bilgi-guvenligi-farkindalik-anketi-sonuclari/ Erişim Tarihi; 11.07.2017

[27] http://www.gunes.com/gundem/bakan-siktan-pardus-cagrisi-760624 Erişim Tarihi; 11.07.2017

[28] http://www.bthaber.com/kamu/acik-kaynak-uretkenligi-artirmak-icin-buyuk-firsat/1/19256 Erişim Tarihi; 11.07.2017

[29] http://www.iha.com.tr/haber-pardus-nedir-nasil-edinebilirim-pardus-adi-nereden-gelmektedir-pardusun-ozellikleri-nelerdir-622748/ Erişim Tarihi; 11.07.2017

[30] Şahinaslan, Ö. (2013). Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma.

[31] http://www.tuyad.org/upload/data/ckfinder/files/GOKHAN%20SERT.pdf Erişim Tarihi 23.08.2017

[32] Dali, E. A. B., & Sistemleri, Y. B. Endüstri 4.0.

[33] Sener, S., & Elevli, B. (2017). Endüstri 4.0'da Yeni İş Kolları Ve Yüksek Öğrenim.

[34] Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.

[35] Alçin, S. Üretim İçin Yeni Bir İzlek: Sanayi 4.0.

[36] http://siemens.edergi.com/pubs/Endustri40/Endustri40/assets/common/downloads/page0015.pdf Erişim Tarihi 23.08.2017

Türkiye'de Siber Saldırılara Karşı Caydırıcılık
Deterrence Against Cyber Attacks in Turkey

Mustafa Şenol
İstanbul Teknik Üniversitesi, Bilişim Enstitüsü Bilgi Güvenliği Mühendisliği ve Kriptografi Bölümü (Dr.), İstanbul, Türkiye
senolm15@itu.edu.tr

Özet

Bu çalışmada, siber güvenliğin önemi, siber güç, siber saldırı, siber savaş ve siber caydırıcılık kavramlarıyla ilgili bilgiler verilmiş, siber saldırılara karşı caydırıcılık sağlayarak da karşı konulabileceği vurgulanmış, Türkiye'de bu güne kadar siber güvenlik strateji ve politikaları içerisinde siber caydırıcılık alanında yapılan çalışmaların neler olduğu konuları incelenmiştir. Bu kapsamda; siber caydırıcılığın, maliyet ve kullanım kolaylıkları yanında sağladığı üstünlükler nedeniyle üzerinde çalışılması, stratejiler geliştirilmesi ve gecikmeksizin uygulamaya konulması gereken çok önemli bir konu olduğuna dikkat çekilmiş ve bazı önerilerde bulunulmuştur.

Anahtar Kelimeler

Caydırıcılık, Siber Güç, Siber Caydırıcılık, Siber Saldırı, Siber Savaş, Siber Güvenlik.

Abstract

In this study, information is given on the importance of cyber security, concepts of cyber power, cyber-attacks, cyber warfare and cyber deterrence while it is underlined that cyber-attacks can also be countered by providing deterrence. Additionally, actions carried out in the fields of cyber security strategies and politics in Turkey up until today were analysed. In this context, it is emphasized that due to the advantages it offers in addition to cost and ease of use, cyber deterrence is a crucial subject that must be studied, strategies and policies must be developed on and be implemented without delay.

Keywords

Deterrence, Cyber Power, Cyber Deterrence, Cyber Attacks, Cyber War, Cyber Security.

I.GİRİŞ

Teknolojinin, özellikle bilgisayar ve iletişim sistemlerinin hızla gelişmesi ve internetin de yaygınlaşmasıyla, bilişim sistemleri ve altyapılarının sağladığı kolaylıklar ve kazanımlar bilişim sistemlerini ve hizmetlerini hayatın vazgeçilmezleri yapmıştır.

İnsanlık için tarihin başlangıcından bugüne en önemli varlık olan bilginin, elektronik ve bilişim sistemlerinin sağladığı imkânlarla, işlenmesinde, iletiminde, korunmasında ve kullanılmasında sağlanan etkinlik her geçen gün daha da artmış ve artmaya da devam etmektedir. Bu gelişmelere paralel olarak devletlerin özellikle ekonomik, politik ve askeri güçlerindeki kısa sürede meydana gelen olumlu yükselişler, kara, deniz, hava ve uzay ortamlarından sonra ortaya çıkan ve 5'inci Harekât Alanı olarak da adlandırılan 'Siber Ortam'ın önemini daha da artırmıştır.

Siber ortamın önemi artarken, bilgilere ve bilişim sistemlerine yönelik olarak başlayan kötü niyetli hareketler ve saldırılar günümüzde de artarak devam etmektedir. Teknoloji değerlendirmeleri ve geleceğe yönelik öngörüleriyle tanınan ABD'li yazar ve gelecek bilimci Alvin Toffler'ın "Teknolojik gücümüz artıyor ancak, yan etkileri ve olası tehlikeleri bundan çok daha hızlı büyüyor" [1] sözü bu durumu çok iyi açıklamaktadır.

Siber ortamda karşı tarafın bilgilerine ve bilgi sistemlerine yönelik zarar verme veya olumsuz etkileme istek ve ihtiyaçları 'Siber saldırı - Siber taarruz', bilgi ve bilişim sistemlerinin kötü niyetli hareketlere ve saldırılara karşı korunması ihtiyacı ise 'Siber güvenlik - Siber savunma' kavramlarını ortaya çıkarmıştır. Devletler siber savunma ve siber taarruz konularında strateji ve politikalar geliştirmeye ve bunları etkinlikle uygulamaya başlamışlar, bunlarla birlikte de 'Siber savaş' kavramı ortaya çıkmıştır.

Siber savaşın başlatılması ve sürdürülmesi için gerekli olan, siber ortamda sahip olunan bilgi sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği, 'Siber Güç' olarak tanımlanmaktadır [2]. Siber güç imkânları kullanılarak yapılan siber saldırıları ve siber saldırıların oluşturduğu savaşları önlemek, siber saldırıyı veya savaşı düşünenleri bu düşüncelerinden ve eylemlerinden vazgeçirmek, kısaca siber saldırganları caydırmak için siber güç imkânları tek başına kullanılabileceği gibi, yeterli olmadığında başka güçlerle birlikte kullanılmasına yönelik stratejiler geliştirilerek uygulanabilmektedir. Savaşlarda en mükemmeli hep kazanmak olmayabilir. M.Ö. 500'lü yıllarda yaşamış olan ünlü Çinli filozof ve savaş stratejisti Sun Tzu'nun dediği gibi "En iyisi savaşmadan baş eğdirmektir" [3]. Yani bir anlamda saldırganı isteğinden, saldırıdan veya savaştan caydırmak, söz konusu siber savaş olduğuna göre "Siber caydırıcılık" en iyisi olabilir.

Kişi, kurum, kuruluş, toplum veya devletlerin günümüzde en değerli varlıklarını oluşturan bilgi ve bilişim sistemleri ile altyapılarına yönelik kötü niyetli hareket ve tehlikeler olan tehditler ve saldırılar nelerdir? Bu saldırıların sonuçları veya oluşturabileceği hasar ve zararlar neler olabilir? Bunlara karşı korunmak için neler yapılmalı, hangi güvenlik veya savunma tedbirleri alınmalıdır? Saldırganları caydırarak kötü niyetli hareketlere ve saldırılara engel olmak, bu kapsamdaki risk ve tehditleri ortadan kaldırmak veya azaltmak mümkün olabilir

mi? Bu kapsamda caydırıcılık nasıl sağlanabilir? Türkiye'nin resmi belgelerinde siber güvenlik ve caydırıcılık konusunda belirlenen ve uygulanması öngörülen tedbirler ve planlamalar ile yapılan çalışmalar nelerdir? Siber saldırılara karşı caydırıcılık sağlamak için nasıl bir strateji geliştirilerek uygulanmalıdır?

Bu çalışmada, yukarıda kısaca sıralanan soruların cevapları ortaya konulurken, siber saldırılara karşı siber güvenliğin öneminin vurgulanması ve caydırıcılık sağlayarak siber güvenliğin nasıl sağlanabileceği konusunun açıklanması, bu konuda dikkate alınmasının uygun olacağı düşünülen esas ve prensiplerin ortaya konulması hedeflenmiştir. Yöntem olarak; 2'nci bölümde 'Siber saldırılar ve güvenlik', 3'ncü bölümde 'Caydırıcılık ve siber caydırıcılık', 4'üncü bölümde 'Resmi belgelerde siber güvenlik ve caydırıcılık", 5'inci bölümde 'Siber saldırılara karşı caydırıcılık stratejisi' konularında araştırmalar sonucu derlenen bilgiler verilmeye çalışılmış ve 6'ncı ve son bölümde konuyla ilgili ulaşılan "Sonuç ve değerlendirmeler" sunulmuştur.

II.SİBER SALDIRILAR VE GÜVENLİK

A.Siber saldırılar

Kazanç sağlamak veya zarar vermek maksatlarıyla siber ortamda belirlenecek hedef ya da hedeflere yönelik gerçekleştirilecek faaliyetler siber saldırıları oluşturmaktadır. ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırılar; "Bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler" [4] olarak tanımlanmıştır.

Saldırganlar siber saldırılarla, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken, temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir. Türkiye 2016-2019 Siber Güvenlik Stratejisi Belgesinde, bu üç prensipten hareketle siber saldırıların tanımı; "Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" [5] şeklinde yapılmıştır.

Bilgisayar ve iletişim teknolojilerinde ve özellikle 1990'lar sonrası internette yaşanan hızlı gelişmeler siber gücün etkisini daha da artırmış, siber gücün sağladığı imkânlar hayatı kolaylaştırmanın yanında, aynı zamanda siber saldırılarla sonuç almaya çalışan birer tehdit ve yaptırım aracı olarak da kullanılmaya başlanmıştır.

Çeşitli niyet ve maksatlarla gerçekleştirilen çok çeşitli tip ve büyüklükteki siber saldırılarla siber savaşların başlayıp devam ettiği dünyada, internet medyası ile yazılı ve görsel basın gibi açık kaynaklara da yansıyan ve siber gücün etkisini de ortaya koyan önemli siber olaylar ve siber saldırıların bazıları aşağıda sunulmuştur [6].

- 2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve kanalizasyon sularının şehre bırakılması,
- 2003'te ABD'nin sekiz eyaletinde 2 gün süren, ölümlere ve 6 milyar dolar zarara yol açan elektrik kesintisi,
- 2007'de Rus bilgisayar korsanlarının Estonya bilgi sistemlerine saldırısı ve ülke çapında faaliyetlerini durma noktasına getirmesi,
- 007'de İsrail savaş uçaklarının Suriye topraklarına girmesi ve nükleer tesisini imha ederek zayiatsız dönmesi, bu sırada Suriye hava savunmasının hiçbir hedef görememesi,
- 2008'de Rusya - Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu finans, haberleşme ve elektrik sistemlerinde ciddi sıkıntılar yaşanması,
- 2010'da İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı,
- 2010'da WikiLeaks'in yayınladığı belgeler ile diplomaside sanal bomba etkisi yaratması,
- 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi,
- 2014'te Sony Şirketinin yoğun siber saldırılar sonucu Kuzey Kore Lideriyle ilgili 44 milyon dolara mal olan filmi gösterimden kaldırması.
- 2016'da ABD'nin doğu yakasına hizmet sunan sistem altyapılarına yönelik olarak başlayan siber saldırıların ülke geneline yayılarak internet bağlantısını engellemesi ve ciddi ekonomik zarara sebep olması.

Dünyada yaşanan bu siber olaylara benzer şekilde, Türkiye'de yaşanmış önemli siber saldırı ve olayların bazıları da aşağıda sıralanmıştır [6].

- 2008'de Bakü-Tiflis-Ceyhan boru hattına siber saldırı sonrası patlama meydana gelmesi,
- 2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi,
- 2011'de saldırılar sonrasında Telekomünikasyon İletişim Başkanlığı'nın sitesinin devre dışı kalması,
- 2015'te elektriğini İran'dan alan Van ve Hakkâri hariç 79 ili etkileyen elektrik kesintisi,
- 2015'te, 10 gün süreli saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalara erişim sağlanamaması,
- 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi.

Henüz farkına varılmayan veya gizlilik, saygınlık kaybı vb nedenlerle açıklanmayan ve açık kaynaklara yansımayanlarla birlikte, yaşanan binlerce önemli siber olay ve saldırının arasından sadece bunlara bakılarak, siber gücün sağladığı imkânlarla çeşitli teknik, taktik ve stratejilerin kullanılmasıy-

la gerçekleştirilecek siber saldırılarla ülke güvenliği için çok büyük tehlikeler, hasar ve zararlar yaratabileceği sonucuna kolaylıkla ulaşılabilir.

B.Siber güvenlik

Hassas ve değerli varlıklara gelecek herhangi bir kötülüğe, hasar veya zarara karşı korunma veya karşı koyma derecesi anlamında kullanılan 'Güvenlik' kavramı; TDK sözlüğünde "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" [7] şeklinde açıklanmaktadır.

Saldırılarda hedefin merkezinde bilginin olması nedeniyle, başlangıçta 'Bilgi Güvenliği' olarak kullanılan kavramın siber güvenliği de kapsadığına dair yaklaşımların olmasına karşın, günümüzde siber ortamın hızlı değişimi dolayısıyla yaşanan olayların da etkisiyle bunun tersinin yaygınlaştığı, siber güvenliğin bilgi güvenliğini de içerir şekilde kullanılmaya başlandığı görülmektedir. Bu durum, "Konuyla ilgili farklı terimlerin ve tanımların ortak temalarından hareketle, siber güvenliğin devlet sırlarının korunması ve ulusal savunmanın sağlaması için temel esas olduğu…" [8] şeklinde NATO Siber Güvenlik Çerçeve Kılavuzu'nda da açıkça vurgulanmıştır.

Türkiye Siber Güvenlik Stratejisi Belgesinde ise siber güvenliğin; "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" [5] ifade ettiği belirtilmiştir.

Strateji belgesindeki bu tanımlamada görüldüğü üzere, temel amaç bilgiyi korumak ve sistemlerin devamlılığını sağlamaktır. Bilgiyi, bilişim sistemlerini ve kullanıcılarını hedef alarak gerçekleştirilen siber saldırılarda kullanılan üç prensip (bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması) siber güvenliğin de temelini teşkil etmektedir. Siber saldırı ve olayların tespit edilerek engel olunması ve bilişim sistemlerinin saldırı/olay öncesi duruma döndürülmesi de, siber güvenliğin amaç ve hedefleri arasında yer almaktadır.

Siber ortamın tehlikelerinin farkında olan ülkeler siber güvenliği önemsemekte, siber tehditleri ulusal güvenliğe karşı en önemli tehdit unsurlarından biri olarak kabul etmekte ve başta ülkenin elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans sektörleri vb kritik altyapıları olmak üzere bireylerinin, kurum ve kuruluşlarının varlıklarını siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadırlar. Bu konuda gerekli adımları atmayan ülkeler ise geç kalmış demektir. Çünkü başlangıçta küçük çapta ve bir kısmı zararsız denebilecek seviyedeki riskler, tehditler ve saldırılar, teknolojinin gelişmesi ve internetin yaygınlaşmasıyla birlikte büyüyerek siber savaş halini almıştır.

ABD eski Savunma Bakanı Leon Panetta, 2012 yılında yaptığı konuşmasında, "ABD'nin Siber-Pearl Harbor ihtimali ile karşı karşıya olduğu" [9] sözüyle, benzer hususları belirtmiş ve siber savaşın ulusal güvenlik için büyük bir tehdit olduğunu vurgulamıştır. Bilgisayar ve iletişim sistemlerinde, insanların internetinden nesnelerin internetine, akıllı cihazlardan akıllı evlere/şehirlere, siber uzayda sınır tanımayan ve insanın hayalinde canlandırma sınırlarını zorlayan gelişmeler yaşanmaktadır.

İşte böyle bir ortamda, siber saldırı risk ve tehditleri gerçeği ve tehlike boyutu ortadayken, çoğu ülke siber savaşın hem taarruz ve hem de savunma boyutu ile ilgili yasa, politika ve stratejiler üreterek uygulamaya koyarken, siber savaşı küçümseyip bu konuda ciddi çalışmalar içerisinde olmayan ülkeleri çok zor bir gelecek beklemektedir. Çünkü siber savaş gerçektir ve saldırganlar şimdiye kadar gerçek yeteneklerini ortaya çıkmaması için en gelişmiş siber silahlarını yani bu konudaki gerçek yeteneklerini kullanmamışlardır. Tam ölçekli bir siber savaşın yani gerçek yeteneklerin kullanıldığı saldırıların yapıldığı bir savaşın sonuçlarının tahmin edilemeyeceği ve olabileceklerin modern bir ülkeyi mahvedebileceği [10] yorumları yapılmaktadır.

Bu kapsamda, bilgisayar ve iletişim teknolojilerinin sağladığı imkânlardan ve kolaylıklardan etkinlikle yararlanabilmek için bilgi ve iletişim sistemleri ile altyapılarının; her geçen gün artarak ve çeşitlenerek devam eden siber suçlara, siber saldırılara, hasar ve yıkım miktarı korkutucu seviyelere ulaşan veya belirsiz olan siber savaşa karşı korunmasının, yani siber güvenliğin sağlanmasının yolları aranmakta ve bu konuda stratejiler geliştirilmektedir.

Siber savaş stratejileri geliştirilirken dikkate alınması gereken en önemli hususların başında caydırıcılık gelmekle birlikte, sır gibi saklanmaları nedeniyle siber silahların caydırıcılık sağlanmasında etkilerinin olmadığı iddia edilmektedir [10]. Ancak, ayrı ve geniş kapsamlı bir konu olması nedeniyle bu çalışmada değinilmeyen, konuyla ilgili önde gelen ülkelerin siber güvenlik ve savaşla ilgili stratejileri incelendiğinde, genel olarak caydırıcılık sağlanması açıkça ifade edilmese de, siber caydırıcılık sağlanmasına katkı sağlayan esas ve prensiplerin sıkça yer aldığı görülmektedir. Bu esas ve prensiplerin başında ise; güçlü siber savunmayı sağlayacak teşkilat ve güçlü yapılanmaların oluşturulması, askeri kabiliyetleri bütünleyecek siber kabiliyetlerin geliştirilmesi, siber suçlarla mücadele ve bu kapsamda caydırıcı yasaların çıkarılması vb önemli konular gelmektedir [11].

/II.CAYDIRICILIK VE SİBER CAYDIRICILIK

A.Caydırıcılık

*T*ürkçede genellikle "korkutarak cesaret kırmak ve vazgeçirmek" anlamlarında kullanılan 'caydırmak' sözcüğünden türetilen 'Caydırıcılık' kavramı, TDK Sözlüğünde "Bir saldırganlığı önlemek ve engellemek için önlem alma işi" [7] olarak açıklanmaktadır.

'Caydırıcılık'; hukuksal alanda "ceza veya hapis korkusuyla suç işlemekten alıkoyma" [12], uluslararası ilişkilerde yani diplomasi alanında "karşıdaki devleti emellerinden vazgeçirme davranışı veya belirli davranışlara yönlendirme" [13], askeri

alanda ise "düşmanı çok yüksek bedel ödeyeceğine inandırarak bir hareketten vazgeçirmek için askeri güç, yaptırım ve tehditlerin kullanımı" [14] olarak tanımlanmaktadır.

Geçmişe ve günümüze bakarak, hukuk alanında bireylerin çeşitli cezalar ile suç işlemelerinin önlenmesine, diplomasi alanında devletlerin çeşitli yaptırımlarla ilişkilerinin yönlendirilmesine ve askeri alanda savaşmadan karşı tarafın farklı davranmasının sağlanmasına, yani bu alanlarda caydırıcılık uygulamasına yönelik, pek çok örnek sıralanabilir. Adli olaylarda para ya da mahkûmiyet cezaları, uluslararası ortamda devletlere çeşitli yaptırımların uygulanması, klasik savaşta güçlü ordularla karşı tarafa güç gösterisi, tatbikatlar vb.

Caydırıcılığın yaygın olarak kullanılan genel tanımı ise, bir düşmanın, belirli bir eylemi gerçekleştirmek için maliyet/fayda hesaplamasına yönelik tahmini üzerinde yönlendirilmesidir [15]. Diğer bir ifadeyle, potansiyel faydaları azaltarak ya da olası masrafları arttırarak (ya da her ikisini de birden), düşmanı eylemi yapmaktan kaçınmaya ikna etmektir. Bu maksatla varlık ve çıkarların korunması için gerekli bütün olanak ve yeteneklerin kullanılacağına yönelik niyet ve kararlılık gösterilir. Caydırıcılığın sağlanması için 'Saldırganın eylemini boşa çıkarma' ve 'Cezalandırma (misilleme tehdidi)' yoluyla saldırıdan vazgeçirilmesine dayanan iki yöntem uygulanır.

Bu yöntemlerden özellikle soğuk savaş döneminde ön planda kullanılan ve nükleer caydırıcılığın esasını teşkil eden cezalandırma yoluyla caydırıcılığın başarıyla sağlanması için üç temel koşul bulunmaktadır [16]. Bunlar caydırıcının yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesidir. Nükleer caydırıcılıkta başarıyı olumlu yönde etkileyen bu temel koşullar, siber caydırıcılığın sağlanmasında da dikkate alınmalıdır.

B.Siber caydırıcılık

Caydırıcılık ile ilgili yukarıdaki açıklamalardan hareketle 'Siber caydırıcılık' nasıl tanımlanabilir?

Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" [3] özdeyişinden de hareketle siber caydırıcılık; 'siber ortamda bilişim sistem ve altyapılarına saldırı başlatacak saldırganı saldırıdan vazgeçirmektir' şeklinde de tanımlanabilir.

Caydırıcılığı genel anlamda "karşı tarafa düşmanca eylemleri yapmama konusunda gözdağı verme" şeklinde açıklayan ABD'li siber savaş araştırmalarıyla ünlü bilim adamı Martin C. Libicki siber caydırıcılığı, siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vaz geçirme olarak tanımlamaktadır. Bu kapsamda misillemenin etkisini de, nükleer ve konvansiyonel caydırıcılıktan sonra, diplomatik ve ekonomik yaptırımlarla sağlanan caydırıcılıktan ise önce geldiğinin kabul edilebileceğini belirtmektedir [17],

ABD eski Genelkurmay Başkan Yardımcılarından olan Orgeneral James Cartwright siber caydırıcılığı; "Siber ortamda başkalarının bize yapmak istediklerinin aynısını onlara yapma yeteneği" [17] olarak tanımlamıştır. Bu tanımlamanın nükleer veya konvansiyonel caydırıcılık için karşılık bulduğu kabul edilmekle birlikte, siber gücün ve kullanılmasının özellikleri dolayısıyla, siber caydırıcılık için yeterli olup olmayacağı tartışılmaktadır.

Siber saldırılara ve savaşa karşı caydırıcılık stratejisini analiz eden çalışmaların çoğu soğuk savaş teorilerine dayanmaktadır. Bu kapsamda başarılı bir caydırıcılık için yerine getirilmesi gereken tarafların yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesi koşullarının, siber saldırıların yarattığı tehditlere uygulandığında başarısız olunmasının beklendiği iddia edilmektedir [16].

İstihbarat yetenekleri bu sorunun çözümünü kolaylaştırsa da, genelde saldırıya karşılık verileceği zaman daha geniş bir potansiyel tehdidi kapsayacak şekilde değerlendirilmelidir. Soğuk savaş döneminde her iki tarafın da yetenekleri açıkça bilinirken, bilgi çağında olası saldırganların sayısının artması ve güçlerinin de belirsizliği, caydırıcılık mesajının kime ve nasıl ileteceğinin zorlukları istikrarlı ve inanılır caydırıcılık sunma olasılığını düşürmüştür.

Siber saldırılara karşı caydırıcılığın zorlukları nedeniyle; nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılık kuramının, günümüzde siber savaşı durdurmakta önemli bir rol oynayamadığı ve ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, tüm çabasına rağmen siber alanda sağlayamayacağı ileri sürülmektedir [10]. Bu tez, 2011 yılında ABD Savunma Bakanlığınca hazırlanan raporlardan sızan bilgilerden, 'siber saldırıların savaş sebebi sayılacağının ve askeri operasyonlarla karşılık verilebileceğinin açıklanması' [18] ile desteklenmektedir.

Libicki'ye göre ise, siber caydırıcılık işe yarayabilir. Ancak bunun için, siber caydırıcılığı nükleer ve klasik askeri caydırıcılıktan ayıran, siber caydırıcılığın aleyhinde olan ve problemli yanlarını ortaya koyan üçü asıl, altısı yardımcı olmak üzere dokuz soruyu cevaplamak gerekmektedir [17].

Asıl sorular:

- Kimin yaptığı biliniyor mu?
- Onların değerli varlıkları risk altında tutulabilir mi?
- Aynı şey art arda tekrarlanabilir mi?

Yardımcı sorular:

- Eğer misilleme caydırıcılığı sağlamazsa, en azından silahsızlandırmayı sağlayabilir mi?
- Üçüncü gruplar mücadeleye katılır mı?
- Misilleme kendi tarafımıza doğru mesajı verir mi?
- Saldırıya karşılık vermek için bir eşik var mıdır?
- Tırmanmadan kaçınılabilir mi?
- Saldırgan tarafa vurmaya değmediği durumda ne olur?

Nükleer caydırıcılıkta cevaplanması kolay olan bu soruların, siber caydırıcılık söz konusu olduğunda cevaplanması zorlaşmakta ve bazen de imkânsızlaştığı görülmektedir. Ancak siber ortamda siber güç kullanılarak caydırıcılık sağlanması düşünülüyorsa bu soruların cevaplanması ve bu cevaplar doğrultusunda planlamaların yapılması ve eyleme dönüştürülmesi gerekmektedir.

IV.RESMİ BELGELERDE SİBER GÜVENLİK VE CAYDIRICILIK

*T*ürkiye'de siber güvenlikle ilgili faaliyet ve çalışmalar 17 Şubat 2003 tarihinde yayımlanan '2003/10 Sayılı Başbakanlık Genelgesi' ile başlamıştır. Söz konusu genelgede, Güvenlik Kültürünü oluşturmayı amaçlayan ve OECD üyesi ülkelerin ortak tutumunu yansıtan rehber ilkelerin bilgi sistem ve ağlarına yönelik tehditler karşısında, her düzeydeki kullanıcılar tarafından benimsenip uygulanmasının yararlı olacağı belirtilerek, öncelikle ve başta kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda göz önünde bulundurulması istenmiştir.

Bu genelgeyi, Devlet Planlama Teşkilatı tarafından 'E-Dönüşüm Türkiye Projesi (2003)', Kalkınma Bakanlığı koordinasyonunda 'Bilgi Toplumu Stratejisi ve Eylem Planı (2006)', TÜBİTAK koordinasyonunda hazırlanan 'Ulusal Sanal Ortam Güvenlik Politikası (2009)' takip etmiştir. Bu çalışmaların içeriğinde, siber güvenlikle ilgili tespitler ve yol haritaları ortaya konmakla birlikte siber caydırıcılıkla ilgili dikkat çekici hususların bulunmadığı görülmektedir.

Daha sonra, 27 Ekim 2010 tarihli MGK Bildirisinde; "Siber tehdidin küresel düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri kapsamlı surette ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi için milli düzeyde yürütülen çalışmalar değerlendirilmiştir. Siber tehditlere karşı önlem almaya yönelik kararlılık ve irade ortaya konmuştur" [19] ifadeleri yer almıştır. Ülkenin en üst ulusal güvenlik kurulunun bildirisinde yer alan bu ifadeler, siber tehditlere karşı önlem alınmasına yönelik kararlılık ve iradenin ortaya konduğunun vurgulanması ve bunun duyurulması, caydırıcılık açısından önemlidir.

Bilgi toplumu politika, hedef ve stratejileri çerçevesinde, 26 Eylül 2011'de '655 Sayılı KHK' ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)'nın teşkilat ve görevleri yeniden düzenlenmiş, 'Siber güvenlik faaliyetleri ve hizmetlerine ilişkin kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonun sağlanmasına ilişkin usul ve esasları belirlemek ve gerekli düzenlemelerin yapılması' görevi UDHB'ye verilmiştir [20]. Siber güvenlikten sorumlu bir makamın belirlenmesinin, bu konularda eksikliklerin giderileceğine yönelik umut vermesi açısından caydırıcılık özelliği taşıdığı söylenebilir. Müteakiben siber güvenlik konusunda çalıştay ve tatbikatların yapılması, kamu kurumlarında yapılanmaya gidilmesi ve 2012 yılında siber güvenlik yol haritasının ortaya konması bu tespiti destekler niteliktedir.

Bakanlar Kurulunun 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin' 20 Ekim 2012 tarihli kararı ile UDHB başkanlığında 'Siber Güvenlik Koordinasyon Kurulu' kurulmuş, siber güvenliğe yönelik ilkeler, teşkilat, görev ve sorumluluklar resmi olarak belirlenmiştir. Siber güvenliğe yönelik en önemli stratejik adımlardan birisi olan bu adımla ilgili bakanlık ve kamu kurumlarının üst düzey yöneticilerinden 12 kişilik Siber Güvenlik Kurulu oluşturulmuştur. Siber Güvenlik Kurulu tarafından 'Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı' [21] kabul edilerek yayımlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı;

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır.
- Plan içeriğinde ve eylemlerde siber caydırıcılık açıkça yer almamakla birlikte, eylemlerden güdülen niyet ve maksatlarla ulaşılması öngörülen hedeflerin kısmen de olsa siber caydırıcılık sağlama sonucuna götürebileceği açıktır.
- Siber güvenlik konusunda yasal düzenlemelerin yapılması ve adli süreçlere yardımcı olacak çalışmaların yürütülmesi siber saldırganların siber ortamda işledikleri suçlar nedeniyle cezalandırılacak olmaları,
- Ulual Siber Olaylara Müdahale Merkezi (USOM)'nin oluşturulması ile Siber Olaylara Müdahale Ekipleri (SOME)'nin faaliyete başlaması, siber olayların tespitini, duyurulmasını, gerekli tedbirlerin alınarak saldırganlarla ilgili gerekli yasal işlemlerin de kısa sürede başlatılmasın sağlanabilecek olması,
- Ulusal siber güvenlik altyapısının güçlendirilmesinin siber saldırıların başarılı olmasını zorlaştırması ve daha masraflı hale getirmesi,
- Siber güvenlik alanında insan kaynağının yetiştirilmesi ile başta kullanıcıları siber güvenlik farkındalığının artırılmasıyla güvenlikte ihmallerin ve yanlışların azalması, bu konuda strateji ve politikaların geliştirilmesi,
- Siber güvenlikte yerli teknolojilerin geliştirilmesi ile daha güvenli donanım ve yazılımların kullanılmaya başlanması,
- Ulusal güvenlik mekanizmalarının kapsamının genişletilmesi ile koordinasyon ve işbirliğin artırılması siber caydırıcılık sağlanmasında temel yapı taşlarını oluşturan çok önemli eylem ve faaliyetlerdir.

Ülkemizin 2015-2018 döneminde takip edeceği ve Kalkınma Bakanlığının koordinasyonunda hayata geçirilecek olan 6 Mart 2015 tarihli 'Bilgi Toplumu Stratejisi ve Eylem Planı' [22] bilişim teknolojileri alt yapılarının geliştirilmesi, kullanıcıların eğitimlerinin artırılması, sektörlerin desteklenmesi vb nedenlerle siber caydırıcılığa önemli katkılar sağlayacaktır.

Türkiye '2016 - 2019 Ulusal Siber Güvelik Strateji ve Eylem Planı' 09 Eylül 2016'da açıklanmıştır. Türkiye'nin siber güvenlik konusunda izleyeceği yolu belirleyen Strateji ve Eylem Planında, siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber

uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması amacıyla, 5 ana eylem ve 41 alt eylemin gerçekleştirilmesi öngörülmektedir. Dört yıllık siber güvenlik yol haritasını oluşturan ana eylem maddeleri aşağıda sunulmuştur [5].

- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması,
- Siber Suçlarla Mücadele,
- Farkındalık ve İnsan Kaynağı Geliştirme,
- Siber Güvenlik Ekosisteminin Geliştirilmesi,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu.

Bu strateji ve eylem planının ana metin ve ana eylem maddelerinde siber caydırıcılık konusunda açık ifadeler bulunmamakla birlikte, ana eylem maddelerinde planlanmakta olduğu belirtilen hususların doğru planlanarak zamanında da uygulamaya konulmasının siber caydırıcılık konusunda ciddi ilerlemeler sağlayabileceği ortadadır. Caydırıcılık konusundaki bu öngörü ve beklentinin 'Siber suçlarla mücadele' eyleminin alt maddelerinde siber saldırganların tespiti ve suçlarının kanıtlanması sağlanarak caydırıcılık sağlanmasının hedeflenen kazanımlar arasında yer aldığının vurgulandığı görülmektedir.

V.SİBER SALDIRILARA KARŞI CAYDIRICILIK STRATEJİSİ

Türkiye'de siber güvenlik strateji ve politikalarıyla ilgili bu güne kadar hazırlanan ve uygulamaya konulan belgeler incelendiğinde siber caydırıcılık konusuna, siber suçlarla yasal olarak mücadele edilerek caydırıcılık sağlanması konusu hariç, yer verilmediği görülmektedir. Siber güvenliğin sağlanarak saldırıların engellenmesi ve saldırıların boşa çıkarılması açısından bakıldığında dolaylı olarak kısmen caydırıcılık sağlanabilecek olsa da, yeterli olmadıkları düşünülmektedir. Yapılması gereken siber caydırıcılık stratejisinin, siber güvenlik stratejisi ile birlikte ele alınarak açık ve ayrıntılı olarak oluşturulmasıdır.

Siber saldırılara karşı başarılı olacak ve siber güvenliğin artırılmasına da katkı sağlayacak caydırıcılık stratejisinin temel bileşenleri neler olmalıdır? Bu bileşenlerin, başarılı bir caydırıcılık için asgari koşulları karşılamasının ve Libicki tarafından ortaya konulan (III'üncü bölümde değinilen) dokuz soruya cevap verecek şekilde belirlenmesinin uygun olacağı düşünülmektedir. Bu tespit çerçevesinde başarılı bir siber caydırıcılık stratejisinin temel unsurları aşağıda sunularak kısaca açıklanmaya çalışılmıştır.

• Ülkenin öncelikle kritik altyapılarını koruyan etkin bir siber savunma:

Siber saldırılara karşı korunmak için her türlü saldırıya karşı koymada temel esas olan değerli varlıkların savunmasının güçlendirilmesi, saldırıyı boşa çıkartmak veya etkisini azaltarak karşı saldırıyı başlatmak için en öncelikli kural olmalıdır. Bu maksatla karşı tarafın saldırı yeteneklerini dikkate alarak ülkenin öncelikle kritik altyapıları olmak üzere bilgi ve bilişim sistemlerinin güvenliğinin sağlanması maliyeti yüksek olmakla birlikte caydırıcılık da sağlayacaktır. Çünkü bu durumda saldırgan tarafın saldırıları zorlaşacak ve maliyetleri de artacaktır.

• Siber saldırı yapması olası hedeflere yönelik etkin siber istihbarat:

Siber ortamda siber tehditlerin ortaya konması ve gelecekte saldırıları yapması mümkün görülen hedeflerin belirlenerek bunların yeteneklerinin öğrenilmesi siber savunma tedbirlerinin alınması yanında saldırı durumunda saldırganın kimliğinin tespiti, caydırıcılık tehdidinin duyurulması, başarılı misillemenin yapılarak hedeflenen sonuca ulaşılması vb pek çok eylem için çok önemli bir unsurdur.

• Olası siber saldırılara karşı etkin misilleme sağlayacak siber taarruz yeteneği:

Gerekli savunma tedbirlerinin alınmış olduğu bir siber ortamda, mutlak güvenlik mümkün olmadığı için savunmanın mutlaka aşılabileceği düşünülmeli ve karşı saldırılarla misilleme yapılması mutlaka planlanmalıdır. Bunun için da siber saldırı/taarruz yetenekleri olası hedeflerin durumları da dikkate alınarak kazanılmalı ve kullanılmaya hazır olunmalıdır. Bu kapsamdaki yeteneklerin maliyeti siber savunmadan daha düşük ve daha kullanılmadan bile karşı tarafta misilleme korkusu yaratarak siber savunmaya da katkı sağlayacaktır

• Siber güvenlik konusunda ulusal ve uluslararası alanda etkin koordinasyon ve işbirliği:

Ülkede bilişim sitem ve altyapılarını kullanan kişi, kurum ve kuruluş bütün kademelerin koordinasyon ve işbirliği içerisinde olması siber gücün etkisini artıracaktır. Siber ortamda saldırıların tespiti ve karşı konulmasında uluslararası işbirliğine ve koordineli hareket edilmesine de büyük ihtiyaç duyulmaktadır. Bu konudaki planlama ve uygulamalar siber savunmayı güçlendirirken siber caydırıcılığın etkinliğini de her bakımdan artıracaktır.

• Siber tehditlere ve saldırılara karşı bütün yeteneklerin kullanılması, koordinasyon ve işbirliğinin sağlanması için etkili komuta ve kontrol:

Siber ortamda bilişim sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği olan siber güç unsurlarının kendi içerisinde birlikteliği yanında, diğer ulusal güç unsurları (insan, coğrafi, ekonomik, politik, psiko sosyal, bilimsel ve teknolojik ve askeri güç) ile de koordinasyon ve işbirliği içerisinde kullanımı planlanmalıdır. Siber ortamda savunma, taarruz ve istihbarat yeteneklerinin koordinesi ve işbirliğinde başarı içinse şüphesiz etkili bir komuta kontrol sitemi kurulmalıdır.

• Siber tehditlere ve saldırılara karşı caydırıcılık niyet ve kararlılığının karşı tarafa bildirilmesi için etkin duyuru ve açıklama politikası:

Karşı taraf tarafından bilinmeyen gücün ve yeteneğin, karşı tarafa etkisi ancak kullanıldığında anlaşılabilir. Fakat önemli olan ve istenilen, bunun önceden bilinmesi ve caydırıcılığından yararlanılmasıdır. Gücün ve yeteneğin baskın etkisi yaratması için gizli kalmasının da faydaları bulunmaktadır. Saldırı öncesinde olası hedeflere gücün ve yeteneklerin duyurulması, saldırı girişimine karşı veya saldırı sırasında caydırıcılık sağ-

layacak tehditle ilgili niyet ve kararlılığın içeriği ve duyurulma şekli ile vasıtalarının önceden belirlenmesi gerekir. Bu konudaki eksik ve yetersizliklerin başka sorunlara ve istenmeyen etkilere sebep olabileceği unutulmamalıdır.

• Siber güvenlik ve caydırıcılık stratejilerinin uygulanmasına yönelik ortaya çıkabilecek olası durumlara ve koşullara da uyarlı yüksek durumsal farkındalık:

Siber güvenlik ve caydırıcılık stratejilerinin uygulanmasının başarısı, bu stratejilerin uygulanmasında veya uygulanması sonrasında beklenen hedeflere ulaşılmaması durumunda, bilişim sistem ve altyapılarının bütün seviyelerindeki kullanıcıların bilgi ve eğitim seviyeleri ile farkındalıkları çok önemlidir. Bu konuda analizler, eğitimler, tatbikatlar vb çalışmaların yapılmasına yönelik planlamalar uygulamaya konmalıdır.

• Siber güvenlik ve caydırıcılık stratejilerinin güncellenmesi ve geliştirilmesi:

Bilişim sistemleri ve altyapılarında çok hızlı yaşanan gelişmelere paralel olarak çeşitleri ve şiddeti de artan siber tehdit ve saldırıların takip edilmesi, her geçen gün değişik kimliklere bürünen saldırganların (kişi, grup, kurum, ülke vb) yeteneklerinin tespit, analiz ve değerlendirme sonuçlarına göre siber güvenlik ve caydırıcılık stratejileri güncellenmeli ve geliştirilmelidir. Bu kapsamda araştırma, seminer, çalıştay, tatbikat vb faaliyetler düzenlenerek sonuçları stratejilere yansıtılmalıdır.

• Siber güvenlik ve caydırıcılık stratejilerinin güçlü ve merkezi bir otorite tarafından oluşturulması ve uygulanması:

Siber güvenlik ve caydırıcılıkta başarı sağlanmasında en önemli faktörlerden birisi şüphesiz bu konuda doğru ve ayrıntılı strateji ve politikaların hazırlanması ve kararlılıkla uygulanmasıdır. Tarihsel gelişim ve dünya üzerinde yaşananlardan öğrenilen en önemli koşul ise bu strateji ve politikaların güçlü ve merkezi bir otorite tarafından oluşturulması ve uygulanmasıdır.

VI.SONUÇ VE DEĞERLENDİRME

Bilişim teknolojilerinin geliştiği ve hızla gelişmeye de devam ettiği günümüzde, bilgisayar ve iletişim teknolojilerinin sağladığı imkân ve kolaylıklardan etkin şekilde yararlanmak için siber güvenliğin önemi her geçen gün daha iyi anlaşılmakta, siber güvenlik ve savunmanın daha etkin şekilde sağlanması için de çalışmalar aralıksız sürdürülmektedir.

Siber saldırı olayları analiz edildiğinde, başarılarının, etkilerinin ve verilen zararların yüksek olmasında temel nedenlerinin başında savunmaya yönelik ulusal veya yerel strateji ve politikaların bulunmaması ya da bulunsa bile bunların yeterli olmaması veya etkin uygulanmaması gelmektedir.

Her şeyden önce, ülkenin haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans gibi kritik altyapı sektörlerine yönelik siber saldırılara karşı korunması için siber gücün öncelikle savunma maksatlı olarak artırılması ve kritik altyapılar başta olmak üzere, ülkenin bilişim varlıklarının etkinlikle savunulması gerekmektedir.

Tarihte sadece savunmayla hiçbir zafer kazanılmamış, karşı saldırı ve taarruz yeteneğinin de kazanılmasının ve kullanılmasının gerekli ve kaçınılmaz bir zorunluluk olduğu anlaşılmıştır. Siber ortamda savunma veya taarruz şeklinde icra edilecek mücadele ve savaşlarda, maksat istek veya istekleri karşı tarafa zorla kabul ettirmek ve temel amaç kazanmak olsa da, Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" özdeyişinden de hareketle, siber savaşta saldırganı saldırıdan veya savaştan caydırmak, yani 'siber caydırıcılık' en iyisi olabilir.

Türkiye'de geçmişten bugüne siber güvenlik strateji ve politikaları incelendiğinde, siber caydırıcılık konusuna gereken önemin verilmediği ve siber saldırılara karşı doğrudan veya dolaylı olarak caydırıcılık sağlanması için yapılan çalışmaların da yetersizliği de ortadır.

09 Kasım 2016 tarihli ve 6757 numaralı Kanun Hükmünde Kararname ile 5 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 60'ıncı maddesinde değişiklik yapılarak Bilgi Teknolojileri ve İletişim Kurumuna; "Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma" [23] görevi verilmiştir.

Türkiye Cumhuriyeti Başbakanının, 22 Kasım 2016 günü Bilişim Zirvesi'nde, siber güvenlikle ilgili yaptığı ve basına da yansıyan açıklamasında "Siber saldırılarda caydırıcılığın arttırılacağını, saldırılardan sadece korunulmayacağını ayrıca caydırıcılık için ek önlemler alınacağını…" [24] ifade etmesi Türkiye'de siber güvenlik yanında siber caydırıcılık konusunda da umut verici çalışmaların başladığını göstermektedir.

Siber saldırılarda caydırıcılığı sağlamak için; saldırılara karşı önceden etkili bir siber savunmaya hazır olarak karşı konulmalı, etkin bir karşı saldırı ve taarruzla hedefe ulaşma gücüne, ancak savunma için de, taarruz için de, kısaca savaşta başarının vazgeçilmezi olan etkin siber istihbarat yeteneğine sahip olunmalıdır.

Siber ortamda savunma, taarruz, caydırıcılık ve istihbarat yetenekleri bilgi, bilgisayar ve iletişim konularında milli teknolojilere sahip olunarak desteklenmeli, milli teknolojilere sahip olunamayan alanlarda sahip olunan teknolojilere hâkim olunmalıdır.

Siber gücün geliştirilerek artırılması ve her maksatla etkin şekilde kullanılması için uygulayıcıların yetiştirilmesi ve farkındalıklarını artıracak eğitimler verilmesi, bu maksatla özellikle siber güvenlik konularında uzman kadroların oluşturulması, her seviyede eğitim ve öğretimin planlanması ve yaygınlaştırılması gerekmektedir.

Siber gücün artırılması ve siber saldırılara karşı caydırıcılık da sağlayarak etkin güvenlik ve korunma için her alanda koordinasyon ve işbirliği gerekir. Bunun için bütün devlet kurum ve kuruluşları ile özel sektör arasında etkin iş birliği ve koordinasyon sağlanmalıdır.

Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi, gerekli yasal mevzuatın mutlaka oluşturulması ve

etkinlikle uygulanması gerekmektedir. Bilişim teknolojileri ve özellikle internet sayesinde ülkeler arası etkileşimin boyutunun da derinleşmesi nedeniyle, diğer ülkelerle siber saldırılara karşı işbirliği yapılması, suçluların yakalanması ve haklarında gecikmeksizin yasal işlem yapılarak cezalandırılması, aynı zamanda caydırıcılık sağlaması yanında saldırıların azalmasını da sağlayacaktır.

Siber güvenlik başta olmak üzere, siber gücün artırılması, etkin bir yönetim ve denetim sağlanması için teşkilatlanmaya gidilmesi, 2016-2019 Ulusal Siber Güvenlik Stratejisinde belirtildiği gibi "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması" [5] ve siber gücü kullanma yetkilerinin tek bir merkezde toplanması kısa sürede olumsuzlukların en aza indirilerek başarının artırılmasını da sağlayacaktır. Siber güvenlik stratejisini oluşturarak uygulayacak teşkilatın, dünyadaki örneklerinden de yararlanılarak, bir ordu yapılanması gibi düşünülerek hayata geçirilmesi teşkilatın etkinliğini ve başarısını daha da artıracaktır.

Siyasi, askeri, ekonomik, coğrafik, demografik, bilimsel, teknolojik, sosyal ve kültürel güçten oluşan Milli Güç unsurlarının her biri uluslararası ortamda ve ilişkilerde aynı zamanda birer caydırıcılık unsuru oluşturmaktadır. Bilimsel ve Teknolojik Güç içerisinde kabul edilen 'Siber Güç (siber savunma, taarruz ve caydırıcılık gücü)' ile de, tek başına veya diğer milli güç unsurlarıyla birlikte siber alanda, uluslararası hukuk ilkelerine bağlı kalarak, kendine özgü kural, esas ve stratejiler doğrultusunda yaptırım uygulamak ve belirlenecek amaçlar doğrultusunda tespit edilecek talep ve isteklerin gerçekleştirilmesi için strateji ve politikalar geliştirerek daha güçlü ve etkin 'caydırıcılık' sağlamak mümkündür. Bu amacın başarısı ise ulusal ve yerli üretim sektörüne gereken önem verilerek caydırıcılık sağlayacak şekilde yönlendirilmesi ve desteklenmesinden geçmektedir.

Siber caydırıcılıkta temel esas ve önemli olan siber saldırıların/savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle yapılmasıdır. Bu kapsamda, 'Siber Güçle Caydırıcılık'; üzerinde düşünülmesi, daha fazla önem verilmesi, diğer alanlardaki caydırıcı gücün bu alanda da oluşturulması için ciddi ve ayrıntılı olarak çalışılması, konuyla ilgili doktrinler üretilmesi, mevcut stratejilerin bu yönde güncellenmesi, yeni stratejiler geliştirilmesi ve geleceğe dönük planlamalar yapılarak gecikmeksizin uygulamaya konulması gereken çok önemli bir konu olduğu değerlendirilmektedir.

TEŞEKKÜR

Makalenin hazırlanması aşamasında destek ve katkıları dolayısıyla, Prof. Dr. Şeref SAĞIROĞLU'na teşekkür ederim.

KAYNAKLAR

[1] Goodman, M., Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü, TİMAŞ Yayınları, İstanbul, 2016.

[2] Nye, J. S., Cyber Power, http://belfercenter. ksg.harvard.edu / files/ cyber-power.pdf, (Erişim: 18 Şubat 2017).

[3] Tzu, Sun, Savaş Sanatı, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2014.

[4] Singer, P.W. ve Friedman, A., Siber Güvenlik ve Savaş, Buzdağı Yayınları, Ankara, 2015.

[5] T.C. UDHB , 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, T.C. UDHB Yay. Ankara, 2016.

[6] Şenol, M., Siber Güçle Caydırıcılık Ama Nasıl? Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Ankara, 2016.

[7] TDK, Büyük Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_bts, (Erişim: 25 Şubat 2017).

[8] Klimburg, A., National Cyber Security Framework Manual, NATO Yayını, Talinn, 2012.

[9] Yayla, M., Hukuki Bir Terim Olarak Siber Savaş, Türkiye Barolar Birliği Dergisi, Sayı 104, Ankara, 2013.

[10] Clarke, R.A.ve Knake, R.K., Siber Savaş, İKÜ Yayınları, İstanbul, 2010.

[11] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim: 18 Şubat 2017).

[12] Kızmaz, Z., Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, Cilt:7, Afyonkarahisar, 2005.

[13] Özdemir, H., Uluslararası İlişkilerde Güç-Çok Boyutlu Bir Değerlendirme, Cilt:63, Sayı:3, Ankara Üniversitesi SBF Dergisi, Ankara, 2008.

[14] Akad, M. T., Modern savaşın Temel Kavramları, Kitap Yayınevi, Ankara, 2011.

[15] Long, A., Deterrence From Cold War to Long War, RAND Corporation, ABD, 2008.

[16] Lupovici, A, Cyber warfare and deterrence. Military and Strategic Affairs, Volume:3, No:3, İsrail, 2011.

[17] Libicki, M. C., Cyberdeterrence and Cyberwar, RAND Corporation, ABD, 2009.

[18] Gorman, S. ve Barnes, J. E., Cyber Combat: Act of War, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718, (Erişim: 25 Şubat 2017).

[19] T.C. MGK Sekreterliği, 27 Ekim 2010 Tarihli Toplantı, http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti, (Erişim: 25 Şubat 2017).

[20] Resmi Gazete, UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, http://www.resmigazete.gov.tr/eskiler /2011/11/20111101M1-1.htm, (Erişim: 01 Şubat 2017).

[21] T.C. UDHB, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. UDHB Yay. Ankara, 2016.

[22] T.C. Kalkınma Bakanlığı, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Bilgi Toplumu D.Yay., 2015.

[23] Resmi Gazete, Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında KHK Değiştirilerek Kabul Edilmesine Dair Kanun, http://www. resmigazete.gov.tr/eskiler/2016/11/20161124-4..htm, (Erişim: 01 Şubat 2017).

[24] Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Zirvesi'16 "No Way Out!" Dedi, https://www.btk.gov.tr/tr-TR/Ulusal-Etkinlik/BILISIM- ZIRVESI16-NO-WAY-OUT-DEDI, (Erişim: 01 Şubat 2017).

Siber Güvenlik Ekosisteminin Geliştirilmesi Modeli: Siber Güvenlik Kümelenmesi

Model for Cyber Security Ecosystems: Cyber Security Clusters

Hasan Hüseyin ÖZBENLİ
STM A.Ş.
Ankara, Turkey
hhuseyin.ozbenli@stm.com.tr

Mustafa ÖZLÜ
STM A.Ş.
Ankara, Turkey
mustafa.ozlu@stm.com.tr

Abstract

Today, rapid developments in the field of information and communication technologies are seen as an element that paves the way for social and economic development. It is inevitable that the transformation in the digital world is parallel to the increase in the welfare of the citizens. However, it is accepted that cyber security and its developments are an integral and indivisible part of this transformation. It is clear that there is a direct causality principle between the growth of information technologies and the illegal and malicious use of these technologies. To counteract this, cyber security is increasingly on the agenda of countries' decision-making bodies. In this document, we propose the establishment of a cyber security cluster in our country, together with the skills needed for these clusters, by developing a cyber security ecosystem in our country and exploring examples of cyber security clusters in the world that have been established to dissipate the sector.

Index Terms

Cyber security, industrial clustering, cyber security ecosystem, cyber security clusters. (key words)

I.GİRİŞ

Günümüzde, bilgi ve iletişim teknolojileri alanındaki hızlı gelişmeler sosyal ve ekonomik kalkınmanın önünü açan bir unsur olarak görülmektedir. Dijital dünyada gerçekleşen dönüşüme paralel olarak vatandaşların refah düzeyinde de artış olduğu kaçınılmaz bir gerçektir. Bununla birlikte, siber güvenlik ve alanındaki gelişmelerin de bu dönüşümün ayrılmaz ve bölünmez bir parçası olduğu kabul edilmektedir.

Bilgi ve iletişim teknolojileri ağları, cihazları ve hizmetleri gün geçtikçe daha da önem kazanmaktadır. 2016 yılında, dünya nüfusunun neredeyse yarısı interneti (3,5 milyar kullanıcı) kullanmıştır (1). Bir araştırmaya göre, 2020 yılına kadar internete bağlı 12 milyardan fazla makineden-makineye bağlı cihaz olacağı tahmin edilmektedir (2). 2016 yılında yapılan diğer bir istatistiğe göre, gönderilen tüm e-postaların neredeyse yüzde birinin kötü niyetli saldırılara ait olduğu tespit edilmiştir ve bu son yılların en yüksek oranıdır. Fidyecilik (Ransomware) saldırıları, işletmeleri ve tüketicileri giderek etkilemektedir. Saldırganların, fidye talebinin ortalama miktarı 2016'da 1000 USD'nin üzerine çıkmıştır. Mayıs 2017'de gerçekleşen WannaCry saldırısı, 150'den fazla ülkedeki şirket ve hastanede büyük ölçüde aksamalara neden olarak büyük yankı uyandırmıştır (3).

Bilgi teknolojilerinin büyümesi ile bu teknolojilerin yasadışı ve kötü niyetli kullanımı arasında doğrudan bir nedensellik ilkesinin bulunduğu açıktır. Bu etkiyi gidermek için, siber güvenlik, ülkelerin karar organlarının gündeminde giderek daha fazla ön plana çıkmaktadır. Bu amaçla her geçen gün ülkelerin siber güvenliği ile ilgili doktrinler ve stratejiler önem kazanmaktadır. Bununla birlikte, bilgi ve iletişim teknolojilerinin güvenli bir şekilde kullanılmasını sağlamak için uygun stratejileri, yetenekleri ve programları sunma kapasiteleri açısından ülkedeki paydaşlar arasında belirgin bir boşluk ve dağınıklık bulunmaktadır.

Bu makalede, ülkemizde siber güvenlik ekosistemini geliştirmek ve sektördeki dağınıklığı gidermek amacıyla kurulan dünyadaki siber güvenlik kümelenmeleri örneklerinin araştırılmasıyla bu kümelenmeler için ihtiyaç duyulan yeteneklerle beraber ülkemizde siber güvenlik kümelenmesi kurulması önerisi getirilmektedir.

II.SİBER GÜVENLİK EKOSİSTEMİ

Genel olarak, siber güvenlik ekosistemi; müşteriler, üreticiler, tedarikçiler, kullanıcılar ve düzenleyici ve denetleyicilerin de içine dâhil olduğu siber güvenlik teknolojisi ürün ve hizmetlerinin oluşturulmasını ve uygulanmasını sağlayan şahıs ve kurumların ağı olarak tanımlanmıştır (4).

Benzer şekilde, siber güvenlik ekosistemi; içerisinde bilgi güvenliği ürünleri ve servislerini yönlendiren kuruluşlarını, bilgi güvenliği donanım ve yazılım tedarikçilerinin, danışman ve uzmanları, dijital adli bilişim uzmanlarının, standardizasyon ajanslarının, akreditasyon ve eğitim tesislerinin, akademik konferanslar ve yayınların, kitap ve dergilerin, bilgisayar korsanları ve onların araç gereçlerinin de olduğu ağ olarak tanımlanmaktadır (5). Siber güvenlik için ekosistem, güçlü bir yasal mevzuat, proaktif devlet girişimleri, sektörün aktif katılımı ve katkısı ile etkin siber kuvvet mekanizmasını gerektirmektedir.

Bu dokümanda, sürdürülebilir ve etkin bir siber ekosistem için geniş bir alanda birlikte çalışabilir, dağınık bir ortamda etkili iş birliği yapabilen endüstriyel siber kümelenme modeli sunulmaktadır. Siber güvenlik alanında kurulacak bu ortaklık ağı ile teknolojik ve ekonomik gelişmelerin önü açılarak, sağlıklı katılımcı ve paydaşların ve uygulanabilir strateji ve politikaların desteğiyle milli/yerli siber güvenlik teknolojileri geliştirerek ülke olarak daha güvenli ve dünya pazarında rekabet edebilecek bir sektör oluşması hedeflenmektedir.

III.ENDÜSTRİYEL KÜMELENMELER

Belirli bir alanda faaliyet gösteren bir grup firmanın ve iş dünyasına direkt ya da dolaylı etki eden iş dışı kurumların (Kamu kurumlan, sivil toplum kuruluşları, üniversiteler gibi) belli bir coğrafi alanda oluşturduğu, her bir firmanın rekabet edebilirliğine olumlu etkisi olan gruplara küme denir. Kümeler, özellikle de aynı faaliyet alanında hem rekabet içinde olan, hem de birbiriyle iş birliği yapan şirketlerin, belli bir alanda uzmanlaşmış tedarikçilerin, hizmet sağlayıcıların, ilgili sektördeki firmaların ve ilgili kurumların coğrafi yoğunlaşmalarıdır (6). Kümeler, birbirlerine katma değer sağlayan bir üretim zincirinde, birbirlerine güçlü bir şekilde bağlı olan firmaların, bilgi üreten ajansların ve müşterilerin üretim ağıdır (7). Diğer bir anlatımla kümeler, birbiriyle katma değer yaratan üretim zinciri içerisinde bağlantılı, güçlü bir şekilde bağımlı olan firmaların (uzmanlaşmış tedarikçiler dâhil) ve üreticilerin ağı olarak tanımlanabilir (8). Kümelenme ise, birbirleri ile ilişkili veya birbirlerinin tamamlayıcısı olan ürünleri üreten ve satan kuruluşların sektörel ve coğrafi temelde yoğunlaşması olarak tanımlanabilir.

Rekabetin artması ile firmalar sadece kendi durumunu değil, bulundukları bölgenin ve sektörün dinamiklerini de inceleyerek karar vermeye başlamışlardır. Ayrıca ihtiyaç duyulan insan gücü, ham madde ve sermaye gibi kaynakların azalması ya da maliyetlerinin artması, firmaları ortak hareket etmeye zorlamaktadır. Stratejilerini birlikte ya da diğerlerinin durumuna göre belirlemeye çalışan firmalar, belli bir süre sonra aynı mekânları ve kaynakları paylaşmanın maliyetleri azalttığının farkına vararak bölgesel olarak yakınlaşmışlardır. Buna bağlı olarak teknoloji, iş gücü ve kaynak paylaşımları sağlanarak, iş birliği kararlarının tüm paydaşların çıkarına olacak biçimde verilmesi sağlanabilir. Firmaların tek başlarına pazarda yeterli paya sahip olmalarının zor olduğu göz önüne alındığında, sektör içindeki diğer firmalar ile aynı kümede yer almaları sonucunda, önemli kazanımlar elde edebilirler. Örneğin firmalar farklı konulardaki tedariklerini küme içinden sağlayıp, maliyet avantajı elde edecek bunun sonucunda da pazar payları ile rekabet güçlerinde artış olması sağlanacaktır.

Kümelenme, firmaların kendi karlılıklarını ya da kazançlarının önüne geçmez ve bunlar için bir engel teşkil etmez, aksine küme içi firmalar arası rekabet devam eder. Bu rekabet firmaların sürekli kendilerini yenilemelerini ve küresel rekabetçi ortama ayak uydurmalarını sağlar. Kümelenme oluşumlarının başlangıcında firmalar herhangi bir yönlendirme olmadan şartların kendilerine sunduğu olanaklar ile bir bölgede yoğunlaşmaya başlarlar. Bunun için firmaların bölgede özellikle dikkat ettiği bazı olanaklar;

- Gerekli altyapı ve tesislerin varlığı,
- Pazar koşullarının uygunluğu,
- Teknolojik imkânların olması,
- Yetişmiş iş gücünün varlığı,
- Sosyal ve kültürel ortamın uygunluğu,
- Yasal ve mevzuat düzenlemelerinin yapılmış olması,
- Kamu kurumları ile sivil toplum kuruluşlarının desteği,
- Üniversiteler ve eğitim kurumlarının varlığı,

olarak sıralanabilir (9).

Genel anlamda kümelenme oluşumları sayesinde, ulusal ya da bölgesel düzeyde, rekabetçiliğin arttırılması, yenilikçiliğin ve Ar-Ge faaliyetlerinin teşvik edilmesi amaçlanmaktadır. Bunun yanında, bölgesel kalkınmanın hızlandırılması, yabancı yatırımların çoğaltılması ile KOBİ'lerin desteklenmesi, beklenen faydalar arasında ilk sıralarda gelmektedir. Küme içinde yer alan firmalar, yürütülen yenilikçilik faaliyetlerinden haberdar olup, öğrenme ve uygulama süreçlerini çok hızlı biçimde yerine getirebilirler. Kümelenme içinde yer alarak bilgiye kolay ulaşım, teknolojik gelişmelerden haberdar olma, teşviklerden yararlanma ve önemli kurumlar ile koordineli çalışma olanaklarına sahip olunması firmalar açısından önemlidir. Bununla beraber yetişmiş iş gücü, altyapı, lojistik, araştırma ve eğitim kurumları, üniversiteler ve risk sermayesi konularında da küme içinden destek sağlanarak, maliyet azaltıcı çeşitli faydaların elde edileceği ifade edilmektedir (10).

A.Kümelerin Faydaları

İhtiyaç duyulan üretim faktörlerinin daha uygun koşullarda temin edilmesine olanak sağlayarak firmalara maliyet avantajı kazandırır

- Ölçek ekonomisinden faydalanılarak maliyetlerin düşürülmesini sağlar
- İşgücü ve ürün kalitesi, verimlilik ve istihdamı arttırır
- Firmaların ihracat ve satışlarının artmasını sağlar
- Yenilik ve teknolojilerin hızla yaygınlaşmasını sağlar
- Yerel rakiplerle yarışmayı öğretir
- Ar-Ge, pazarlama, finansal kaynaklara ulaşım gibi kaynakların daha etkin kullanılmasını sağlar
- Taklit edilmesi güç rekabet avantajı ile bölgesel kalkınmayı destekler
- Bölge ekonomisini güçlendirir
- Yerel ortak gereksinim ve menfaatler için çalışılmasını sağlar
- Bölgeyi yatırımcılar için ilgi merkezi haline getirir
- Üniversite- sanayi iş birliğini destekleyerek, Ar-Ge ve yenilik çalışmalarının güçlenmesini sağlar

- Yeni iş ve girişim sayısını arttırır
- Teşvik almayı kolaylaştırır
- Eğitim ve danışmanlık faaliyetlerini geliştirir (11).

IV.TÜRKİYE'DEN KÜMELENME ÖRNEKLERİ

Türkiye son yıllarda kümelenme konusunda önemli gelişmeler kaydedilmektedir. Birçok sanayi kolunda kümelenme desteklenmiş ve bu destekler kümelenme sayılarında artışlar gerçekleşmesini sağlamıştır. Kümelemeyi bir arada tutan şey, yasal bir zorunluluk değil, bu kurumlar arası oluşan güven ve iş birliğidir. Alıcı-tedarikçi ilişkileri, ortak dağıtım kanalları, ortak iş gücü havuzları, üniversitenin firmalarla gerçekleştirdiği araştırma geliştirme çalışmaları gibi bu güven ve iş birliği sonucu oluşan aktiviteler, bu grubun ortak güçlüklere göğüs germesini ve ortak fırsatları değerlendirmesini sağlar. Ortak ekonomik çıkarlar, kümedeki firmaların, tek başına hareket eden şirketlere göre daha verimli, daha yenilikçi ve dolayısıyla daha rekabetçi olmalarını sağlar. Her alanda olduğu gibi savunma sanayinde de kümeler oluşmuş ve faaliyetlerini sürdürmektedirler. Savunma sanayi kümelenmelerinin en önde gelenlerine aşağıda yer verilmiştir.

A.OSSA: OSTİM Savunma ve Havacılık Kümelenmesi

OSSA, Savunma Sanayinin yerlileştirilmesine yönelik çalışmaları desteklemek ve Türk Savunma Sanayinin uluslararası pazardaki rekabet gücünü arttırmak adına Aselsan, Havelsan, TAI, TEI, Roketsan, FNSS, Boeing, Sikorsky vb. ana sanayi firmalarının onaylı alt tedarikçisi olarak kümede yer alan 164 nitelikli KOBİ ve 7.500'den fazla personel kapasitesi ile 1 Temmuz 2008 tarihinde kurulmuştur ve faaliyetlerine devam etmektedir (12).

B.SAHA İstanbul: Savunma, Havacılık ve Uzay Kümelenmesi

SAHA İstanbul, SSM, İTO, THY Teknik, İTÜ, İSO, DTO, TİM ve Üniversitelerimizin destekleri ile Türkiye'nin milli gelirinin yarısını üreten İstanbul Sanayisinin, Katma Değeri yüksek, teknolojik ürünler üretmesi amacı ile, Edirne'den başlayarak, Tekirdağ, İstanbul, İzmit, Yalova, Adapazarı ve Düzce'ye uzanan Kuzey Marmara koridorunda faaliyet gösteren 65.000 sanayici firmamızın gücünü, kümelenerek, ortak bir sinerji yakalanması hedefi doğrultusunda, 2015 yılı Mart ayı içinde, 27 kurucu üyenin girişimleri ile kurulmuştur (13).

C.TSSK: Teknokent Savunma Sanayii Kümelenmesi

ODTÜ TEKNOKENT, aktif olarak Ar-Ge yapan ve 90'ı aşkını savunma sanayii şirketi olmak üzere, 300'den fazla firma ile beraber ODTÜ içinde yer alan birçok araştırma merkezi ve laboratuvarı bünyesinde barındırmakta olup, 2010 senesi itibariyle Teknokent Savunma Sanayi Kümelenmesi (TSSK) adı altında savunma sanayii alanında faaliyet gösteren firmaları kümelemiştir. Bu şirketler, birbirlerini tamamlayıcı ve birbirlerinin kabiliyetlerine katma değer ekleyen ve savunma, havacılık ve güvenlik alanları için yeni ürün ve hizmetler geliştiren dikey uzmanlıklara sahiptirler (14).

D.İzmir Havacılık ve Uzay Kümelenmesi

Havacılık ve Uzay Kümelenmesi, ülkemiz havacılık ve uzay sanayinin gelişimi için sektöre ihtiyaç duyduğu desteği sağlamak, sektörde yerli katkı payının ve ihracat imkânlarının artırılmasında katkıda bulunmak, ulusal ve uluslararası alanda iş birlikleri kurmak ve sektörün yenilikçi ürünler ve süreçler geliştirmesine destek olmak amacıyla 2015 yılında kurulmuş bir kümelenmedir. 14'ü akademik olmak üzere toplam 60 üyeye sahiptir (15).

Yukarıda belirtilen kümeler dışında Eskişehir Havacılık Kümelenmesi ve Bursa Havacılık ve Uzay Kümelenmesi de savunma sanayi için çalışmalarına devam etmektedirler. Bahsi geçen kümelerde yer alan firmalar önemli işbirliklerine ve başarılara imza atmaktadırlar. Ülkemizde savunma sanayi kümelerinde kazanılan bu ilerlemelerin yurtdışı boyutuna bakıldığında, bazı ülkelerde kümelenme çalışmalarının daha da özelleştiği, siber güvenlik alanında kümeler var olduğu görülmektedir.

V.DÜNYADA SİBER GÜVENLİK KÜMELENMELERİ

Siber güvenlik kümelenmeleri, kurulduğu bölgedeki siber güvenlik alanındaki yetenekleri ve uzmanlığı bir araya getirerek, yapılan çalışmaların belirli bir strateji ve yol haritası ekseninde ilerlemesini böylece eğitim, araştırma ve teknoloji becerilerinin geliştirilmesiyle sektördeki ekonomik kalkınmayı da hedeflemektedir. Dünyada farklı endüstri alanlarında olduğu gibi siber güvenlik endüstrisinde de kümelenme örnekleri mevcuttur. Kümelenmelerin kuruluş hedefleri ve gerçekleştirilen faaliyetler incelendiğinde bunlar arasında siber güvenlik teknolojilerini geliştirerek yatırım faaliyetlerini artırmak, kamu-özel sektör ortaklıklarını geliştirmek, yeni pazar araştırmaları yapmak, akademik ve eğitim faaliyetleri belirli bir standarda getirmek ve ulusal/uluslararası düzenleyici kurumlarla diyalog kurmak olduğu anlaşılmaktadır. Genel olarak siber güvenlik alanındaki çalışmaların bir araya getirilerek teknolojik ve ekonomik anlamda bir sinerji yaratılması konusunda ortak bir hedefe sahip olan bu kümelenme dünyadaki örnekleri aşağıda olduğu gibi incelenmiştir.

A.The Hague Security Delta (HSD)

Hague (Lahey) Güvenlik Deltası (HSD), Avrupa'nın önde gelen siber güvenlik kümelenmesidir. Lahey, Twente ve Brabant'daki önemli bölgesel merkezlere sahip bu Hollanda kümesinde; siber güvenlik, ulusal ve kentsel güvenlik, kritik altyapının korunması, adli bilişim alanlarındaki yenilikler konusunda işletmeler, kamu kurumları ve bilişim kurumları birlikte çalışmaktadır. Yalnızca Lahey bölgesindeki 400 güvenlik şirketi, ulusal cironun %25'inden fazlasını güvenlik alanında gerçekleştirmekte ve bu şirketler 15.200 kişiye istihdam sağlamaktadır. Ülke çapında ise siber güvenlik sektöründe elde edilen 7,2 milyar avro ciroyla beraber 61,600 kişi istihdam edilmektedir (16).

B. The Pôle d'Excellence Cyber (Cyber Cluster)

Pôle Siber Güvenlik Kümelenmesi (Pôle d'Excellence Cyber), Fransa Rennes Bölgesinde Şubat 2014'de Fransız Savunma Bakanlığınca kurulmuş bir siber kümelenmesidir. Kümede; Airbus Defence and Space, Thales, Orange Labs, Cap Gemini, Alcatel Lucent, Sopra Group gibi liderlerle bölgede siber güvenlik alanında çalışan yaklaşık 75 şirket bulunmaktadır. Ayrıca siber güvenlik alanında faaliyet gösteren 7 araştırma derneği (IRISA, Lab-STICC, IRMAR, IETR vb.) ve akademik kurumlar (Université de Rennes 1, Telecom Bretagne, INSA Rennes, ENSIBS, IUT de Bretagne, ENSSAT, vb.) kümeye destek vermektedir (17).

C.UK Cyber Security Forum

Birleşik Krallık Siber Güvenlik Forumu, siber güvenlik alanında aktif olarak çalışan küçük ve orta ölçekli şirketleri (KOBİ'ler) temsil eden bir sosyal kuruluştur. Foruma katılmak tamamen ücretsizdir ve ülkede 500'den fazla ana üye bulunmaktadır. Forum altında Malvern Siber Güvenlik Kümelenmesi (18) örneğine benzer şekilde 18 farklı siber güvenlik kümesi bulunmaktadır. Siber Güvenlik Kümeleri, siber güvenlik alanında aktif olarak çalışan küçük şirket gruplarıdır. UK Siber Güvenlik Forumu gönüllü olarak oluşturulan bir çatı kuruluştur. Kümelenmelerin üyeliği ücretsizdir ve tüm üyeler, konuşmacıları dinlemek, ağ kurma ve ilgili tartışmalara katılmak için düzenli toplantılara davet edilir. Kümeler bağımsız olarak yönetilir, ancak tüm üyelerin ulusal düzeyde temsil edilmesi ayrıca fırsatların ve en iyi uygulamaların tüm kümeler arasında paylaşılmasını sağlamak için UK Siber Güvenlik Forumu aracılığıyla işbirliği yapmakta ve iletişim kurmaktadır (19).

D.Finish Information Security Cluster

Finlandiya Bilgi Güvenliği Kümelenmesi (FISC), Finlandiya'nın önde gelen bilgi güvenlik şirketleri tarafından siber güvenlik çalışmalarını ve operasyonlarını ulusal/uluslararası alanda geliştirmek amacıyla 2012'de kurulmuş bir kuruluştur. FISC, yaklaşık 50 üye organizasyona sahiptir ve bunlar tamamen bilgi ve siber güvenlik teknolojilerine odaklanan küçük veya orta ölçekli şirketler olmakla birlikte, ülkede bilgi güvenliği ile ilgili operasyonları gerçekleştiren çok uluslu şirketlerdir. FISC'nin ana hedefi, siber güvenliği geliştirmek ve aşağıdaki alanlarda üye kuruluşların faaliyetlerini desteklemektir: yatırım faaliyetlerini artırmak, kamu-özel sektör ortaklıklarını geliştirmek, pazar araştırmaları yapmak, üst düzey eğitimin ulusal derinliğini ve genişliğini sağlamak ve ulusal/uluslararası düzenleyici kurumlarla diyalog kurmaktır (20).

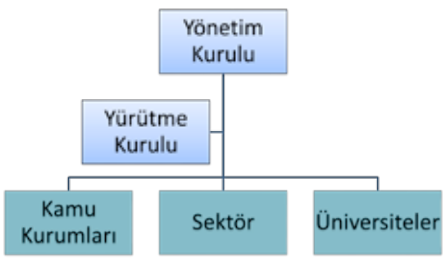
Dünyada bunlara ek olarak, üniversiteler ya da enstitüler bünyesinde siber güvenlikteki teknoloji farkındalığını teşvik etmek için endüstri, akademik ve devlet kurumları arasında etkileşimi artırmak amacıyla konsorsiyum, merkez, enstitü ya da forum çatısı altında kurulan siber güvenlik kümelenmeleri faaliyet göstermektedir.

- Kanada - The Canadian Institute for Cybersecurity at the University of New Brunswick (UNB)
- [https://www.cybernb.ca]
- Singapur - The Singapore Cybersecurity Consortium [http://sgcsc.sg]
- ABD - University of Central Florida Faculty Cluster Initiative (Cyber Security and Privacy Research) [https://www.ucf.edu/faculty/cluster/cyber-security-and-privacy/]
- ABD - Cyber & Information Security Consortium (CISC) [https://www.cyberinfosec.org/about-us/]
- ABD - The National Cybersecurity Preparedness Consortium [http://nationalcpc.org/about.html]
- ABD - The Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA)

[http://cias.utsa.edu]

VI.ÜLKEMİZDE SİBER GÜVENLİK KÜMELENMESİ MODELİ

Dünyadaki siber güvenlik alanındaki tematik endüstriyel kümelenme örneklerini incelediğimizde bu oluşumların küme, konsorsiyum, forum, merkez veya mükemmeliyet merkezi adı altında farklı isimlerle oluşturulan platformlar olduğu görülmektedir. Oluşturulacak platformun daha önce bahsedilen kümelenme amaçlarını da gözeterek bütün ekosistemi içine alacak ve sektörel ekosistemin merkezine oturacak şekilde çatı ya şemsiye bir kuruluş olması öngörülmektedir. Oluşturulacak kümeden en önemli beklenti, Ar-Ge faaliyetlerinin, yenilikçiliğin ve yerli/milli teknolojik üretimin desteklendiği, bunların da doğrudan girişimciliği ve ekonomiyi tetiklediği bir ekosisteme katkı sunmasıdır. Bu platformun başarılı olması ve sürekliliği, ekosistem içerisinde yer alan her bir unsura bir şekilde dokunmasına bağlıdır. Kamu ya da özel sektörde yer alan ihtiyaç ve talep sahipleriyle buna cevap verecek arz sahiplerinin yani sektörün etkileşim içerisinde kümeye destek vermeleri beklenmektedir. Kümenin dünyadaki diğer modeller de örnek alınarak, ülkemiz şart ve ihtiyaçlarına ve çağın gereklerine uygun bir şekilde özgün bir model olması amaçlanmaktadır. Oluşturacak platform, üç temel ve önemli paydaş olan kamu, sektör ve üniversite temsilcilerinin oluşturduğu bir Yönetim Kurulu vasıtasıyla yönetilmeli; organizasyon faaliyetleri ise Yürütme Kurulu vasıtasıyla yürütülmelidir.



Şekil 1. Kümelenme Genel Organizasyon Yapısı

Bununla birlikte kümelenmenin alt paydaşları olarak aşağıda

sıralanan unsurların kümeye katkı sağlayacak şekilde modele dâhil olması beklenmektedir:

- Yerli ve yabancı yatırımcılar, girişimciler ve KOBİ'ler
- Teknokent/Teknoparklar
- Enstitüler

Herhangi bir alanda endüstriyel kümelenme oluşturulması için üç temel şart uzmanlık, yakınlık ve ağ oluşturma söylenebilir. Bu amaçla küme içerisinde yer alacak işletmeler, siber güvenlik yetkinlik ve uzmanlık alanına göre sınıflandırılarak gruplandırılacaktır. Üyeler; coğrafi ve finansal durumlarına göre kurucu, fiziksel ve uydu/uzak üyeler olarak kategorilere ayrılacak; her kategoriye farklı görev ve sorumluluklar atanacaktır. Böylece küme hem fiziksel hem de ağsal olarak geniş bir bölgeyi kapsayacak şekilde faaliyetlerini yürütebilecektir.

Şekil 2. Siber Güvenlik Kümelenmesi Genel Faaliyetleri

Kümelenmede düzenlenecek olan bölgesel, ulusal ve uluslararası etkinliklerin kümeye olan ilgiyi artırması planlanmaktadır. Kümelenme çatısı altında düzenlenecek haftalık, aylık ve belirli periyotta uzak üyelerin de katılacağı yıllık etkinlikler, siber güvenlik kümelenmesi paydaş ve üyelerinin ortak bir sinerji ve birliktelik oluşturması önemlidir. Yılda bir kez düzenlenecek bir haftalık Siber Güvenlik Haftası Etkinliği ile bir hafta süresince eğitimler, seminerler ve sempozyumlar düzenlenerek bölgesel ve küresel düzeyde kümenin cazibesinin artırılması hedeflenmektedir. Bununla beraber düzenlenecek çalıştaylar ve uluslararası konferanslar ile kümenin etkinliğinin üst seviyelere çıkması planlanmaktadır.

Araştırma ve geliştirme faaliyetleri kümelenme oluşumunun en temel gayeleri arasında yer almaktadır. Kurulacak siber güvenlik araştırma laboratuvarları ve kuluçka merkezleri, yeni girişimcilere yönelik finansal ve teknik destekler ve iş ortaklıkları, üniversitelerle yapılacak iş birlikteliği ve danışmanlık faaliyetleri bu kapsamda değerlendirilmelidir. Oluşturulacak kümelenmenin yürüteceği faaliyetler içerisinde en önemlilerinden biri eğitim-öğretim faaliyetleridir. Küme, hem kamu hem özel sektör hem de üniversitelerin siber güvenlik alanındaki uzmanlık ihtiyaçlarına cevap verecek şekilde düzenlenmelidir. Bu amaçla kümede yer alacak Siber Güvenlik Akademisi, küme çatısı altında olmakla beraber ihtiyaçlara yönelik farklı konumlarda buna ek olarak da sanal eğitim platformuyla faaliyetlerini yürütecektir. Eğitim platformuna küme üyeleri ile birlikte üniversiteler ve enstitüler de destek verebilecektir.

Kümelenmenin finansal olarak kendini idame edebilmesi, hem kamunun hem de sektörün verecekleri desteklere bağlıdır. Siber güvenlik alanında milli kritik ihtiyaçların karşılanması için kamuda yürütülen projeler kapsamında kümeyle entegre olmalı ve oluşturulacak platforma fon akışı sağlanmalıdır. Ayrıca kümede elde edilen ürünlerin küme çatısı altında ulusal ve uluslararası pazara çıkmasıyla bölgesel ve küresel bir sinerji ve ticaret merkezi olması hedeflenmektedir. Böylece kümelenme siber güvenlik alanına yatırım yapmayı planlayan, sektör için bir finansal yatırımcı buluşma noktası haline gelmesi öngörülmektedir.

VII. SONUÇ

Ülkemizin siber güvenlik alanında yapılan çalışmaların verimliliğinin yükseltilerek, rekabet edebilirliğinin artırılması için, konuya odaklı çalışan, nitelikli iş gücüne sahip, güç birliği ile ileri teknoloji ürünler üretebilen, bunları uluslararası arenada satabilen, ulusal ve bölgesel girişimler ile bunları destekleyecek yapılara, şiddetle ihtiyacı vardır. Siber Güvenlikle ilgili firmaların sahip olduğu sınai ve ticari gücü ortaya çıkarmak ve küresel rekabet ortamında hak ettiği yere ulaşmalarını hızlandırmak için tüm kurumların iş birliği içinde ilerlemesi ve mevcut kaynakların etkin biçimde kullanılması gerekmektedir.

Söz konusu amaca ulaşmak için Siber Güvenlik alanında etkili bir araç olarak önerilen model doğrultusunda kümelenme yaklaşımından yararlanılması isabetli olacaktır. Kümelenme ile şirketler, birbirlerini tamamlayıcı ve birbirlerinin kabiliyetlerine katma değer ekleyen siber güvenlik alanı için yeni ürün ve hizmetler geliştiren dikey uzmanlıklara sahip olabileceklerdir. Model ile siber güvenlik alanında kümelenme yoluyla dışa bağımlılığı ortadan kaldırmak amacı ile hem imal ettirecek kurumları hem de sanayicilerimizi milli üretim ve yazılıma yönlendirecek, devletimizin yerli sanayini geliştirme hedeflerinde yardımcı olacak bir eko sistem kurulmuş olacaktır.

Milli olması zorunlu ve kritik ihtiyaçlarının, üniversiteler ile ar-ge odaklı iş birlikleri çerçevesinde yerli şirketlerce geliştirilmesi; yerli savunma sanayii şirketleri, üniversiteler ve diğer şirketler ile ar-ge odaklı iş birlikleri çerçevesinde uluslararası pazarlara teknoloji üretmeyi hedeflemesi de model ile önerilen kümelenmenin başka bir kazanımı olacaktır.

Siber güvenlik kümelenmesi modelimiz; siber güvenlik alanında çalışan firmaları yönlendirmek, bilgilendirmek ve onlara rehberlik etmek suretiyle milli üretim yetenek ve kapasitemizi artırma idealine hizmet edecek bir kümelenme olarak planlanmalıdır. Kümelenmenin hem ülke güvenliğine hem de ülke ekonomisine önemli katkılar sağlayacağı aşikârdır.

KAYNAKLAR

[1] ITU Statistics, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[3] Wannacry Campaign Ppotential Sstate Involvement Could Have Serious Consequences, https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html

[4] Enabling Distributed Security in Cyberspace, Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, U.S. Department of Homeland Security, 2011, http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf]

[5] Jatinder N. D. Gupta (The University of Alabama in Huntsville, USA) and Sushil Sharma (Ball State University, USA), "Handbook of Research on Information Security and Assurance", 2009

[6] Porter M., "Clusters and the New Economics of Competition", Harvard Business Review, 1998

[7] OECD, Reviews of Regional Innovation Competitive Regional Clusters, 2007

[8] Roeland T., Hertog P., OECD Summary Report of the Focus Group On Clusters, 1998

[9] Xiangwei, 2008: s. 377

[10] Morosini, 2004: s. 309

[11] İzmir Atatürk Organize Sanayi Bölgesi, Kümelenme Nedir? http://www.iaosb.org.tr/icerik/kumelenme/kumelenme-nedir

[12] OSSA: OSTİM Savunma ve Havacılık Kümelenmesi, http://www.ostimsavunma.org/tr/content/kume-hakkinda/281

[13] SAHA İstanbul: Savunma, Havacılık ve Uzay Kümelenmesi, http://sahaistanbul.org.tr/sahaistanbul/

[14] TSSK: Teknokent Savunma Sanayii Kümelenmesi, http://tssk.org.tr/

[15] İzmir Havacılık ve Uzay Kümelenmesi, http://www.hukd.org.tr/baskanin-mesaji

[16] The Hague Security Delta (HSD), https://www.thehaguesecuritydelta.com]

[17] Pôle d'Excellence Cyber, https://www.univ-rennes1.fr/actualites/pole-dexcellence-cyber-des-industriels-lirisa

[18] Malvern Cyber Security Cluster, http://www.malvern-cybersecurity.com

[19] UK Cyber Security Forum, http://www.ukcybersecurityforum.com

[20] Finish Information Security Cluster, http://www.fisc.fi/en/

Blok Zinciri Tabanlı Siber Güvenlik Sistemleri

Blockchain Based Cyber Security Systems

Enis Karaarslan
Bilgisayar Mühendisliği
Muğla Sıtkı Koçman Üniversitesi
Muğla, Türkiye
enis.karaarslan@mu.edu.tr

Muhammet Fatih Akbaş
Bilgi İşlem Daire Başkanlığı
İzmir Kâtip Çelebi Üniversitesi
İzmir, Türkiye
mfatih.akbas@ikc.edu.tr

Özet

Kripto paralar (cryptocurrency), eşler arası (Peer-to-Peer, P2P) mimaride birbirine bağlı madenci düğümü adı verilen bilgisayarlara ve blok zinciri yapısında tutulan kayıt sistemine dayanmaktadır. Bu sistemler sadece bir para birimi sağlamamakta, bu altyapılar üzerinde çeşitli 'merkezi olmayan' (decentralized), dağıtık (distributed) sistemler/yazılımlar tasarlanmaktadır. Bu çalışmada blok zinciri sisteminin nasıl çalıştığı, sağladığı veri bütünlüğü, kullanılabilirlik, mahremiyet gibi güvenlik servisleri ve hata toleransı incelenmektedir. Blok zinciri yapısının; nesnelerin interneti (Internet of Things, IoT), akıllı şehirler, kişisel verilerin korunması, bilgisayar ağları için kullanımı gibi siber güvenlik konularındaki çalışmalar ele alınmaktadır. Blok zinciri uygulamalarındaki temel sorunlara ve olası çözümlere değinilmektedir. Bu tür çözümlerin ağ güvenliğinde kullanımına dair fikirler ele alınmaktadır.

Anahtar Kelimeler

Blok Zinciri, Siber Güvenlik, Kripto Para

Abstract

Cryptocurrency relies on the computers called miner nodes which are interconnected with Peer-to-Peer (P2P) architecture and the record system that is held in a blockchain structure. These systems do not only provide a currency; various decentralized, distributed systems/softwares can be designed on these infrastructures. This study examines how blockchain system works, investigates the provided security services like data integrity, availability, privacy and fault-tolerance. The studies of using blockchain structure in cyber security issues like protecting the Internet of Things (IoT), smart cities, computer networks and the privacy of the personal data is covered. Basic problems in the blockchain applications and possible solutions are discussed. Ideas for the use of such solutions in the network security are addressed.

Index Terms

Blockchain, Cyber Security, Cryptocurrency

I. Giriş

Bitcoin (BTC), bilindiği üzere P2P protokolünü kullanan ve merkezi olmayan bir dijital paradır. 2008 senesinde duyurulmuş ve 2009 senesinden beri aktiftir. Protokol çalışması [1] Satoshi Nakamoto adıyla yayınlanmasına rağmen, bu çalışmanın bilinmeyen kişi(ler) tarafından geliştirildiğine inanılmaktadır. Hiçbir finans kurumunun yönetmediği Bitcoin'in başarısı, alternatif bozukluk (altcoin) adı verilen türevleri ile devam etmiştir. Bildirinin hazırlandığı anda; bu tür paraların geçerli olduğu Coin Market Cap [2] borsasında işlemde olan 865 farklı kripto para bulunmaktaydı.

Kripto paralar, yapılan işlemleri P2P protokolü ile birbirine bağlı bilgisayarlar üzerinde blok zinciri yapısında tutmaktadır. Ethereum gibi birçok kripto para, sağladıkları API'ler aracılığı ile kendi altyapı ve para birimlerini kullanan başka yazılımların da geliştirilmesi için ortamlar sağlamaktadır. Ethereum [3] projesi kendisini bir blok zinciri uygulama platformu olarak tanımlamakta ve durdurulamaz uygulamalar geliştirilebileceğini öne sürmektedir.

Bu bildiride, ikinci bölümde P2P ve blok zinciri temelli bu mimarinin nasıl çalıştığı ve öğeleri ele alınacaktır. Üçüncü bölümde, sistemin güvenilirliği ele alınacaktır. Dördüncü bölümde, bu mimarinin hangi güvenlik servislerini sağladığı belirtilecektir. Beşinci bölümde, bu yapının siber güvenlik için kullanımına dair akademik çalışmalardan örnekler verilecektir. Altıncı bölümde, blok zinciri sistemlerindeki sorunlar ele alınacak ve bunları çözmeye yönelik yeni yaklaşımlara değinilecektir.

II. Blok zinciri sistemleri

Bazı sistemlerde farklılıklar olmakla birlikte, BTC Mimarisi [1] yaygın olarak diğer alternatif bozukluk sistemlerde de kullanılmaktadır. Temel kavramlar aşağıda tanımlanmıştır:

- ***Blok zinciri:*** Blok zinciri, zamana göre sıralanmış ve sürekli büyüyen bir veri yapısıdır. Bloklar, yapılan işlem(ler)i ve bir önceki blokun adresini tutarlar. Blok zinciri, işlemlerin değiştirilemez listesinin tutulduğu bir kayıt defteridir (ledger). Ethereum'un kullandığı bloklarda çalıştırılabilir kod da bu blok içerisinde tutulmaktadır.
- ***Akıllı Anlaşma (Smart Contract):*** Ethereum projesi

ile blok zincirinde akıllı anlaşmalar yapmak mümkündür. Bu anlaşmalarla; değer tutan, veri kaydeden ve çeşitli hesaplama görevleri için bloklara çalıştırabilir kod ekleyen uygulamaların geliştirilmesi mümkün olmaktadır.

- ***Madenci Düğüm (Mining Node):*** İşlemlerin gerçekleşmesini sağlayan bilgisayarlardır. Önceleri işlemci gücü kullanılırken, ekran kartlarındaki işlemcilerin veya bu iş için üretilmiş özel kartların kullanılması söz konusu olmuştur.
- ***Madencilik Gücü:*** Hash işlemleri çoğunlukla ekran kartlarının işlemcileri üzerinde GPU hesaplama gerçekleştirilmekte ve H/s (saniyede hash hesaplama) birimi ile Kilo-Mega-Giga (bin, milyon, milyar) biriminden güçleri tanımlanmaktadır. Bir ekran kartı Mh/s güçlerinde çalışmakta, makinelere takılan çoklu kartlarla yüksek madencilik güçlerine ulaşılabilmektedir.
- ***Konsensus Protokolleri:*** Blok zincirlerinin bütün düğümlerde aynı olabilmesi için kimin değişiklik yapacağını belirleyen kurallar bütünüdür. PoW ve PoS yaklaşımlarından söz etmek mümkündür. Çalıştığının Kanıtı (Proof of Work, PoW), her düğümün değişiklik önerisi yapabilme hakkı kazanmak için öncelikle çözmesi gereken bir bulmaca gibidir. Başkalarının çözmesinin zor olduğu ama işleyen tarafından kolaylıkla doğrulanabilecek bir değerdir. PoS (Proof of Stake), PoW'deki hesaplama yerine, sisteminde sahip olduğu zenginliğe (kripto para) göre bloğu yaratacak olanın seçildiği bir yaklaşımdır.
- ***Hesap:*** Her makine veya kullanıcıya özgü o kripto para birimini tutmaya yarayan tekil (unique) bir hesaptır.

Örneğin: a94f5374fce5edbc8e2a8697c15331677e6ebf0b

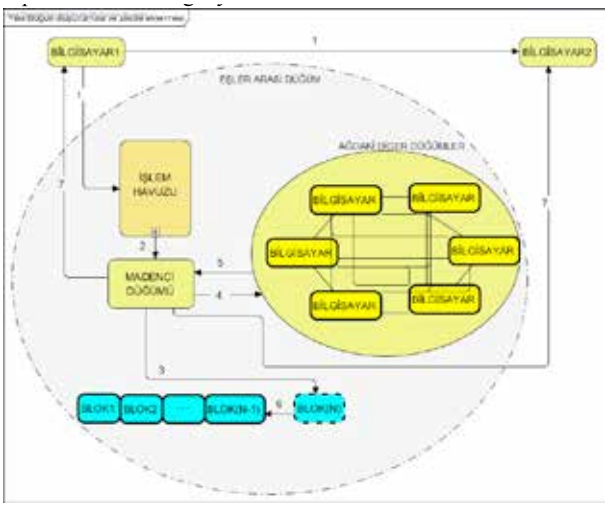
Sistemin temel özellikleri:

- İşlemler merkezi değildir,
- İşlemler P2P ağda tüm düğümlere yayınlanır (broadcast),
- İşlemler birden fazla düğüm tarafından onaylanır ve sonunda blok zincire eklenir,
- Sistemdeki bütün hesaplar halka açıktır (public) ama anonimdir. Hesap ID'si aynı zamanda açık anahtar (public key) olarak kullanılır,
- Madenci düğümler, işlemleri bloklar olarak toparlar.

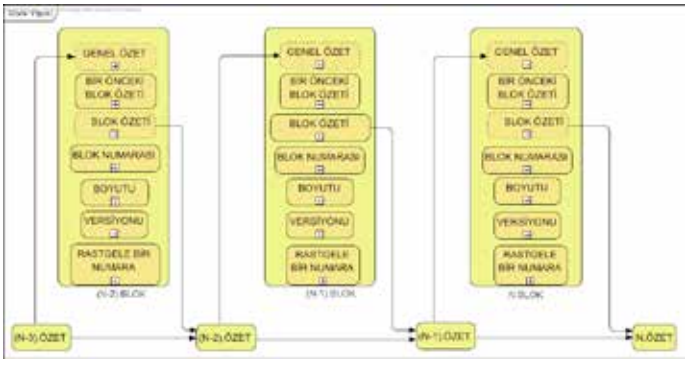
Blok zinciri uygulamasında madenci adı verilen sistemler, şu ana kadarki bütün işlemleri içeren bütün blok zincirini tutarlar. Bloğu oluşturacak düğümün seçimi konsensus protokolü ile gerçekleştirilir. Blok zinciri yapısı kullanan bir uygulama aracılığı ile Bilgisayar1 ve Bilgisayar2 makineleri arasında bir işlem yapılacağı bir senaryodaki yeni bloğun oluşturulması ve blok zincirine eklenmesi Şekil 1'de gösterilmiştir. İşlem aşamaları şekilde gösterilen numaralarla aşağıdaki gibidir:

1. Bilgisayar1 yapılacak işlemi Bilgisayar2 de dâhil olmak üzere eşler arası ağda yayınlar,
2. Sistemde işlem havuzunun (mining pool) kullanımı seçimli olabilmekte, işlemler yayınla öğrenilebilmektedir. Doğrulanmamış işlemler, düğümler tarafından çağırılır,
3. Ağda kullanılan protokole göre, n adet işlem toplu olarak bir bloğa yazılabilir. Düğümler yeni blok oluşturulur,
4. Doğrulama için eşler arası ağdaki bilgisayarlara yayın yapılır,
5. Doğrulama bilgisinin tamamlandığı bilgisi ağ içerisinde iletilir,
6. Eşler arası ağda konsensus protokolü ile bir madenci düğümü seçilir. Seçilen madenci düğümü, yeni bloğu blok zincirine ekler,
7. Talep edilen işlemin tamamlandığı bilgisi, işlemi gerçekleştiren makinelere iletilir.

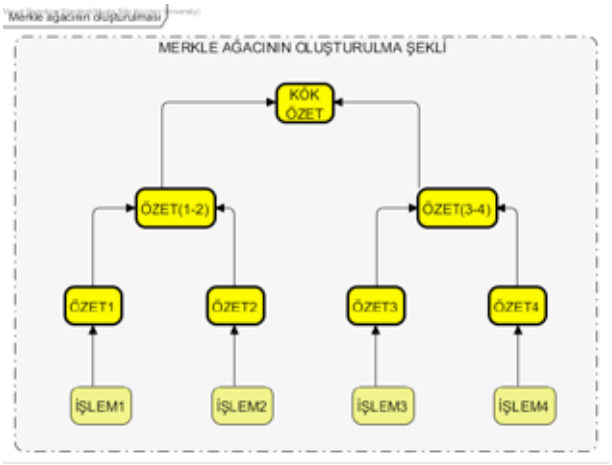
Bloklar, hash(özet) değeri ile önceki bloklara bağlanmaktadır. Bu süreçte önceki bloklardaki özet değerinden genel özet değeri oluşturulmaktadır. Aynı zamanda bir önceki bloğun özeti de tutulmaktadır. Blok içerisinde ise; 4 işlemin toplanarak bir bloğa yazılması durumunda alınan özetlerden kök özet (Merkle ağacının) oluşturulması Şekil 3'de gösterilmiştir.



Şekil 1. Blok zinciri tabanlı uygulamada yeni bloğun zincire eklenme süreci



Şekil 2. Blok zinciri yapısı



Şekil 3. Merkle Ağacının Oluşturulması

Blok zinciri tabanlı uygulamaların geliştirilmesi için çeşitli altyapı çalışmaları bulunmaktadır. Linux Foundation tarafından yürütülen Hyperledger [4], 27 organizasyonun destek verdiği bir açık kaynak projesidir. Bunun yanı sıra farklı kripto paraları altyapıları da çeşitli API'ler sağlamaktadır. Örneğin; Ethereum blok zinciri platformu, akıllı anlaşmalar ile altyapıları üzerinde çeşitli uygulamaların çalıştırılmasına izin vermektedir. Solidity [5] gibi yüksek düzeyli dillerle Ethereum Sanal Makinesi (Ethereum Virtual Machine) üzerinde akıllı anlaşmalar geliştirmek mümkündür.

III. Sistemin güvenilirliği

Saldırganların sistemi ele geçirmesi için, ağdaki düğümlerin çoğunluğunu ele geçirmesi gerekmektedir. Düğümlerin dağıtık olması, bu olasılığı da oldukça düşürmektedir.

Blok zinciri yapısında hash fonksiyonları aktif olarak kullanılmaktadır. Her blok, bir önceki bloğun sağlamasını (hash) tutar. Hash fonksiyonu olarak farklı algoritmalar da kullanılmakla birlikte, BTC SHA256 algoritmasını kullanmaktadır. Sistemdeki bir işlemi değiştirmek, zincirdeki tüm blokları da hesaplamayı gerektirecektir ki bu da muazzam bir işlem gücüne gereksinim duyacaktır. Zincirdeki her değiştireceği blok için diğer düğümleri de ikna etmesi ve bunun için de PoW hesaplamalarını gerçekleştirebilmesi gerekecektir. Bu da %51 saldırısı olarak tanımlanmaktadır, çünkü bunun için ağdaki bütün düğümlerin madencilik işlemci gücünün en az %51'ine sahip olması gerekecektir. Saldırı teorik olarak mümkün olsa da pratikte bu tür bir saldırı olası değildir ve etkisinin kısa süreceği ifade edilmektedir [6]. PoS kullanıldığında ise, saldırganın bütün kripto paranın en az %51'ine sahip olması gerekecektir ki Ethereum'da sadece konsorsiyumun elinde bulunan bir güçtür.

IV. Güvenlik servisleri

Güvenlik servisleri açısından blok zincirinin, merkezi ve dağıtık veritabanlarından farkı Tablo 1'de [7] verilmiştir. Blok zinciri ile veri bütünlüğü (data integrity), kullanılabilirliği (availability) servisleri ve hata toleransı (fault tolerance) en iyi şekilde verilebilmektedir. Blok zinciri tabanlı sistemler, gizlilik (confidentiality) servisini hedeflememektedir.

Tablo 1. Blok zinciri ile Merkezi / Dağıtık Veritabanlarındaki Güvenlik Servislerinin Kıyaslanması [7]

	Blok Zinciri	Merkezi Veritabanı	Dağıtık Veritabanı
Bütünlük	Yüksek	Orta	Orta
Kullanılabilirlik	Yüksek	Düşük	Orta
Hata Toleransı	Yüksek	Düşük	Yüksek
Gizlilik	Düşük	Yüksek	Orta

İşlemi gerçekleştiren makinelerin bütün kayıtları ortada olsa da kime ait olduklarının belirli olmamasından dolayı mahremiyet (privacy) tabanlı servisler de verilebilmektedir.

V. Siber güvenlik için kullanımı

Yeni teknolojiler beraberinde yeni güvenlik tehditlerini getirmektedir. IoT, akıllı şehirler gibi popüler kavramların sağladığı yararların yanı sıra bilgi güvenliği konusunun iyi bir şekilde gözden geçirilmesi gerekmektedir. P2P tabanlı ve dağıtık blok zinciri mimarisi ile siber güvenlik için mahremiyet ve bütünlük başta olmak üzere çeşitli güvenlik servisleri sağlayacak çözümler yapmak mümkündür. Blok zinciri, kriptografik algoritmalar, dijital imzalar ve özet fonksiyonları gibi güvenlik yöntemlerini kullanmaktadır. Bankacılık sektörü, finans kuruluşları, sağlık hizmetleri, elektronik oylama, IoT ve bilgisayar ağları için kullanımı söz konusudur. Güvenlik ve mahremiyet alanı üzerine yapılan çalışmalarda blok zinciri tabanlı yaklaşımların kullanımı gelecek vaat etmektedir [8].

Conoscenti ve arkadaşlarının literatür çalışmasında [9], blok zinciri teknolojisinin kullanıldığı durumlar incelenmektedir. Blok zinciri teknolojisinin bütünlük (integrity), anonimlik (anonymity) ve uyarlanabilirlik (adaptability) özelliklerini etkileyen unsurlar ele alınmaktadır. Blok zinciri teknolojisinin veri depolama yönetimi, malların ve verilerin ticareti, kimlik denetimi ve değerlendirme sistemleri gibi kategorilerde kullanıldığı belirtilmektedir.

Huh ve arkadaşlarının çalışmasında [10], IoT cihazlarının yönetimi için blok zinciri teknolojisinin kullanımı önerilmektedir. Platform olarak Ethereum'un seçildiği bu çalışmada, Ethereum'un akıllı anlaşması kullanılarak IoT cihazlarının davranışlarını belirleyen kodlar yazılmaktadır. Kimlik doğrulama amaçlı (authentication) kullanılan açık anahtarlı altyapı (Public Key Infrastructure, PKI) ile saldırganların Ethereum platformu üzerinde bulunan yönetim sistemini kontrol altına almasının önüne geçilmektedir. Anahtarların yönetimi için RSA kripto sistemi kullanılmaktadır. Açık anahtarlar (public keys) Ethereum'da, gizli anahtarlar (private keys) uçlardaki IoT cihazlarda saklanmaktadır.

Birçok nesnenin/cihazın birbirleriyle etkileşim halinde olduğu bir IoT ortamında hassas veriler söz konusu olmaktadır. Böylesine bir ortamda cihazlar arasındaki iletişimin ve hassas verilerin korunması gerekmektedir. Bu yüzden IoT güvenliği konusunun önemi her geçen gün artmaktadır. Dorri ve arkadaşlarının çalışmasında [11], IoT güvenliği ve mahremiyet için blok zinciri yaklaşımı önerilmekte ve akıllı evler için durum çalışması sunulmaktadır. Çalışmada önerilen çözümün DDoS ve Linking saldırılarına karşı etkinliği de analiz edilmektedir.

Biswas ve arkadaşlarının çalışmasında [12], akıllı şehirlerdeki güvenlik tehditlerine karşı koruma sağlamak ve akıllı şehirleri daha güvenli bir hale getirmek için blok zinciri teknolojisinin kullanımı ele alınmıştır. Akıllı şehirlerde bulunan cihazlarla blok zinciri teknolojisinin entegrasyonunun dağıtık bir ortamda güvenli veri iletişimini sağlayacağı ifade edilmektedir.

Blok zinciri teknolojisi işlemsel olarak maliyetlidir ve yüksek bant genişliğine gereksinim duyulmaktadır. Bu gereksinimler birçok IoT cihazı için uygun değildir. IoT'de blok zinciri teknolojisinin uygulanması; yüksek enerji tüketimi, ölçeklenebilirlik ve işleme zamanı gibi nedenlerden çok kolay değildir. Dorri ve arkadaşlarının bir diğer çalışmasında [13], IoT için iyileştirilmiş yeni bir blok zinciri mimarisi önerilmektedir. Bu çalışmada, Bitcoin'in altyapısını oluşturan klasik blok zinciri kullanımının getirdiği yükleri ortadan kaldırmak için hafif (lightweight) bir blok zinciri mimarisi kullanımından bahsedilmektedir. Önerilen çözüm, merkezi konumda ve özel olan değiştirilemez bir kayıt defterinden (Immutable Ledger, IL) ve merkezi olmayan konumda ve herkese açık (public) blok zincirinden oluşan hiyerarşik bir mimariye sahiptir. IL, ek yükü azaltmak için IoT'nin yerel ağ seviyesinde çalışmaktadır. Blok zinciri ise daha güçlü bir güven için daha üst seviyedeki uç cihazlarda bulunmaktadır. IoT için iyileştirilmiş bu blok zinciri mimarisi, güvenlik ve mahremiyet özelliklerini içinde barındırmakta olup blok onayı işleme zamanını azaltmak için PoW yerine dağıtık güven yöntemini kullanmaktadır. Madencilik süreci yoktur, bu da bazı gecikmeleri ortadan kaldırmaktadır. Simülasyon sonuçları, önerilen yöntemin düşük oranda paket ve işlem yükü getirdiğini göstermektedir. Servis reddi saldırısı (Denial of Service, DoS), modifikasyon saldırısı (modification attack), düşürme saldırısı (dropping attack) ve ekleme saldırısı (appending attack) gibi bazı saldırı türlerine karşı da yöntemin başarısı ölçülmüştür.

Kişisel verilerin korunması ve mahremiyet amacıyla da blok zincirinin kullanımı mümkündür. Bilindiği üzere, üçüncü parti yazılımları veya servisleri çok fazla miktarda kişisel ve hassas verileri toplamaktadır. Zyskind ve arkadaşlarının çalışmasında [14], blok zinciri tabanlı ve blok zinciri tabanlı olmayan depolama alanlarının birleştirildiği mahremiyet odaklı bir kişisel veri yönetimi platformu sunulmuştur.

Kişisel sağlık verilerinin tutulduğu elektronik sağlık kayıtlarına erişim denetim altında tutulmalıdır. Azaria ve arkadaşlarının çalışmasında [15], MedRec adını verdikleri blok zinciri çözümü tabanlı kayıt yönetim sistemi önerilmiştir. Hastaların, geniş kapsamlı ve değiştirilemez bir sağlık kaydına sahip olması ve bu kayda farklı sağlık kurumlarından kolaylıkla erişebilmesi hedeflenmiştir. Sistem, araştırmacı ve sağlık otoriterilerinin madenci olarak sisteme katkıda bulunması için anonim verileri bir ödül olarak vermeyi öngörmektedir. Madenci makineleri PoW ile sistemin güvenilirliğini sağlayacaktır.

Watanabe ve arkadaşlarının çalışmasında [16], dijital haklar gibi sözleşmelerin yönetiminin daha güvenli hale getirilmesi için yeni bir mekanizma önerilmektedir. Bu mekanizma, güvenilirlik skorunu (credibility score) kullanan yeni bir konsensus metoduna sahiptir. Bu yöntem ile birlikte proof-of-stake (PoS) yöntemi bir arada kullanılarak hibrit bir blok zinciri yapısı ortaya çıkmaktadır. Saldırganın kaynakları ele geçirmesinin önüne geçmesini sağlamakta ve blok zincirini daha güvenli bir hale getirmektedir.

Bilgisayar ağları için kullanımına dair bazı çalışmalardan da söz etmek mümkündür. Gelecekte blok zinciri tabanlı DNS ve blok zinciri tabanlı internet söz konusu olabilecektir. DNSChain [17]; özgür, güvenli ve dağıtık bir DNS çözümü olarak ortaya atılmıştır. SecureChain [18], ağ cihazlarının yapılandırma dosyalarının ve log kayıtlarının saklanmasına yönelik bir yaklaşımdır. Log kayıtlarının daha güvenli bir mimaride tutulması; değiştirilemezlik ve inkâr edilemezlik ilkesinin sağlanması hedeflenmektedir.

İlgi çekici bir başka çalışmada, Barnas [19]; yeni bir siber savunma yaklaşımı modelinin gerektiğini belirtmiş ve ülke ulusal güvenliği için blok zincirinin kullanımına dair çeşitli önerilerde bulunmuştur. Blok zinciri ile değiştirilemez kayıtların oluşturulabileceği ve sistemde zayıflık takibi yerine değişikliklerin izlemenin daha etkin olacağı belirtilmiştir. Tedarik zinciri yönetiminde kullanımı ile aygıt yazılımlarının (firmware) takip edilebileceği belirtilmiştir. İletişim altyapısına saldırı yapıldığında, dağıtık mimarisinin ve güvenlik protokollerinin sayesinde iletişimin devamını sağlayabilen altyapıların kurulabileceğine değinilmiştir.

VI. Sorunlar ve yeni yaklaşımlar

Blok zinciri sistemlerinde, işlemlerin kayıtlarının tutulduğu blokların büyümesi ve bunun sonucunda yaşanan performans sorunları, büyük miktarlarda madenci düğümü kuran ve bir nevi fabrikalara dönüşen şirketlerin sistemi domine etme riski ve yüksek elektrik harcamaları gibi sorunlardan söz etmek mümkündür. O'Dwyer ve arkadaşlarının 2014'deki çalışmasında [20], Bitcoin altyapısının elektrik harcamasının İrlanda'nın elektrik tüketimi olan 3 GW'a yaklaştığı tahmin edilmiştir. Blok zinciri sistemlerinin yaygın kullanımında çok daha fazla elektrik harcamasının olacağı ve 4000 GW'ı aşabileceği tahmin edilmektedir. Bu da Amerika'nın toplam elektrik

harcamasının iki katıdır [21].

Bu sistemlerdeki sorunlara farklı yaklaşımlarla çözüm bulunmaya çalışılmaktadır. Daha hızlı ve ölçeklenebilir bir çözüm olan Lightning Network [22] çözümü önerilmiştir. Dağıtık konsensusun sağlanması için PoW yaklaşımı yerine PoS yaklaşımı tartışılmakta ve bazı kripto paralar tarafından kullanılmaktadır. Böylece matematiksel problem çözmek için harcanan işlemci gücü yerine rastsal seçim [23] veya madencilerin sistemde bulundurduğu kripto para değerinin kullanımı [24] söz konusu olabilecektir. PoS ile sistemin çok daha az elektrik harcaması ve çok daha hızlı çalışmasının söz konusu olacağı iddia edilmektedir [23].

VII. Sonuç

Kripto paralar sadece farklı bir ekonomi yaratmakla kalmamakta, aynı zamanda kullandıkları P2P ağları ve blok zinciri yapısına dayalı mimarileri ile siber güvenlik için yeni çözüm önerilerine ilham olmaktadır. Blok zinciri yapısına dayanan bu mimari ile veri bütünlüğü, mahremiyeti, kullanılabilirliği güvenlik servislerinin ve hata toleransının sağlandığı etkin çözümler geliştirilebilmektedir.

Blok zinciri sistemleri ile siber güvenlik çözümlerinin etkinleştirilmesine yönelik çalışmalar gerçekleştirilebilir. Bu sistemlerin; IoT, akıllı şehirler ve bilgisayar ağlarının siber güvenliği için ve kişisel verilerin korunmasında kullanımına dair çalışmaların belli başlıları bu bildiride sunulmuştur.

Blok zinciri tabanlı siber güvenlik sistemlerinin ele geçirilmesinin diğer çözümlere göre daha zor olduğunu da söylemek mümkündür. Saldırganın ağdaki madencilik gücünün en az %51'ini elinde tutması veya yazılım değişikliği için madenci düğümlerinin çoğunluğunu ikna etmesinin gerekmesi bu teknolojinin siber güvenlik sistemlerinde kullanımının önemini ortaya koymaktadır.

Blok zinciri sistemlerinde aşılması gereken sorunlar bulunmaktadır. Bunlardan en önemlisi; işlemlerin kayıtlarının tutulduğu blokların büyümesi ve bunun sonucunda yaşanan performans sorunlarıdır. Bunun yanı sıra, bu sistemlerin ihtiyaç duyduğu yüksek işlemci gücü ve yüksek elektrik sarfiyatı da önemli bir etmendir. Büyük miktarlarda madenci düğümü kuran kurumların sistemi domine etme riski de bulunmaktadır.

Lightning Network gibi daha hızlı ve ölçeklenebilir yeni ağların kurulması, P2P ağında hangi düğümün kaydı yapacağının seçiminde daha az enerji gerektiren PoS yaklaşımının kullanımı gibi yeni yaklaşımlar ortaya çıkmaktadır.

Blok zinciri teknolojisine dayanan siber güvenlik önlemlerinin çalışılması ve geliştirilmesi gerektiğini düşünüyoruz. MSKÜ NetSecLab (http://wiki.netseclab.mu.edu.tr) bünyesinde bu tür blok zinciri tabanlı sistemlerin simülasyonu ve denemelerinin gerçekleştirilmesi hedeflenmektedir.

Teşekkürler:

MSKÜ NetSecLab ağ güvenliği grubundan lisans öğrencimiz Fatih Teke'ye katkılarından ve yaptığı test çalışmalarından dolayı teşekkür ederiz.

Kaynaklar

[1] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008. https://bitcoin.org/bitcoin.pdf (Türkçesi: http://bitcoin-turkiye.net/bitcoin-makale.pdf) (Erişim Tarihi: 30.08.2017).

[2] CryptoCurrency Market Capitalizations. https://coinmarketcap.com/currencies/views/all (Erişim Tarihi: 30.08.2017).

[3] Ethereum. https://www.ethereum.org (Erişim Tarihi: 30.08.2017).

[4] Hyperledger. https://www.hyperledger.org (Erişim Tarihi: 30.08.2017).

[5] Solidity Tutorial. http://solidity.readthedocs.io/en/latest (Erişim Tarihi: 30.08.2017).

[6] 51% Attack. https://learncryptography.com/cryptocurrency/51-attack (Erişim Tarihi: 30.08.2017).

[7] N. Bozic, G. Pujolle and S. Secci. "A Tutorial on Blockchain and Applications to Secure Network Control-Planes". IEEE 3rd Smart Cloud Networks & Systems (SCNS), pp. 1-8, 2016.

[8] H. Halpin and M. Piekarska. "Introduction to Security and Privacy on the Blockchain". IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 1-3, 2017.

[9] M. Conoscenti, A. Vetro and J.C. De Martin. "Blockchain for the Internet of Things: a Systematic Literature Review". IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1-6, 2016.

[10] S. Huh, S. Cho and S. Kim. "Managing IoT Devices using Blockchain Platform". IEEE 19th International Conference on Advanced Communication Technology (ICACT), pp. 464-467, 2017.

[11] A. Dorri, S.S. Kanhere, R. Jurdak and P. Gauravaram. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home". IEEE 2nd PERCOM Workshop On Security Privacy And Trust In The Internet of Things, 2017.

[12] K. Biswas and V. Muthukkumarasamy. "Securing Smart Cities Using Blockchain Technology". IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems

(HPCC-SmartCity-DSS), pp. 1392-1393, 2016.

[13] A. Dorri, S.S. Kanhere and R. Jurdak. "Towards an Optimized BlockChain for IoT". ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17), pp. 173-178, 2017.

[14] G. Zyskind, O. Nathan and A.S. Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data". IEEE Security and Privacy Workshops (SPW), pp. 180-184, 2015.

[15] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management". IEEE 2nd International Conference on Open and Big Data (OBD), pp. 25-30, 2016.

[16] H. Watanbe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami. "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts". IEEE International Conference on Consumer Electronics (ICCE), pp. 467-468, 2016.

[17] S. Singh and N. Singh. "Blockchain: Future of Financial and Cyber Security". IEEE 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 463-467, 2016.

[18] SecureChain: A Blockchain Security Gateway for SDN. http://www.reply.com/en/content/securechain (Erişim Tarihi: 30.08.2017).

[19] N.B. Barnas. "Blockchains in National Defense: Trustworthy Systems in a Trustless World". A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Air University, 2016.

[20] K.J. O'Dwyer and D. Malone. "Bitcoin Mining and its Energy Footprint". 25th IET Irish Signals & Systems Conference and China - Ireland International Conference on Information and Communications Technologies (ISSC 2014 / CIICT 2014), 2014.

[21] The Bitcoin and Blockchain: Energy Hogs. https://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761 (Erişim Tarihi: 30.08.2017).

[22] J. Poon and T. Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". 2016. DRAFT Version 0.5.9.2. https://lightning.network/lightning-network-paper.pdf (Erişim Tarihi:30.08.2017).

[23] Could a Blockchain-based Electricity Network Change the Energy Market? https://www.theguardian.com/sustainable-business/2017/jul/13/could-a-blockchain-based-electricity-network-change-the-energy-market (Erişim Tarihi: 30.08.2017).

[24] Proof of Work vs Proof of Stake: Basic Mining Guide. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake (Erişim Tarihi: 30.08.2017).

Android Kötücül Yazılım Tespiti Yaklaşımları

Android Malware Detection Approaches

Ceren ASLANALP DİNÇER
Bilişim Enstitüsü Adli Bilişim Anabilim Dalı
Gazi Üniversitesi, Ankara, Türkiye
ceren.aslanalp@gmail.com

İbrahim Alper DOĞRU
Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü
Gazi Üniversitesi, Ankara, Türkiye
iadogru@gazi.edu.tr

Özet

Mobil cihazlar, mobil uygulamaların işlevselliklerinin gelişmesiyle birlikte hem iş hem günlük hayatta vazgeçilmez cihazlar olmaya başlamıştır. Kendi cihazını getir iş modeli ile beraber bu cihazlar iş ve kamu kurumlarının ağlarına bağlanarak, beraberinde kötücül yazılımların tüm risklerini organizasyona taşımaktadır. Kötücül davranış, bilgiye ve cihaza yetkisiz erişim dolayısıyla hem kurum hem kişiye karşı ciddi ölçüde tehdit oluşturmaya başlamıştır. Android, açık kaynak çekirdek politikası sebebiyle bu tehditlere çok daha fazla açık bir platformdur. Bu kötücül yazılımları tespit edip önlem almak için tespit mekanizmaları geliştirilmekte, buna karşılık olarak kötücül yazılım geliştiricileri dönüşüm gibi güçlü tekniklerle bu tespit tekniklerinden kaçmayı amaçlamaktadır. Bu çalışmada, Android kötücül yazılım tespiti yaklaşımları sunan farklı çalışmalar incelenmiştir ve bu çalışmalar çeşitli ölçütler bakımından karşılaştırılmıştır.

Anahtar kelimeler

Android malware, kötücül yazılım, kötücül yazılım tespiti, dinamik yaklaşım, statik yaklaşım, imza tabanlı yaklaşım, hibrit yaklaşım

Abstract

With the development of the functionality of mobile applications, mobile devices have become essential in both business and daily life. Bring your own device business model permits the employees to connect their own devices to the networks of business and public institutions and carry all the risks of malware together with the organization. Malicious behavior via unprivileged access to information and device has been a serious threat to both organizations and individuals. Android has open source kernel policy, so it is more vulnerable to these threats. Detection approaches have been developed for the mitigation and detection of malware by time. In response to this, malware developers aim to hide from these detection techniques by developing complicated techniques like obfuscation. In this study, various studies presenting Android malware detection approaches have been reviewed and compared in terms of various criteria.

Index Terms

Android malware, malware detection, dynamic approach, static approach, signature-based approach, hybrid approach

I. GİRİŞ

Günümüzde mobil sistemlerin gelişmesi ve yaygınlaşması ile birlikte geçmişte kullanılan geleneksel cep telefonları artık yerini akıllı telefonlara bırakmıştır. Akıllı telefon marketinin dünya çapındaki hızlı büyümesinin sebeplerinden biri de akıllı telefonların iş amacıyla kullanımının yaygınlaşmasıdır. Kendi Cihazını Getir iş modeli günden güne kabul görmeye başlamıştır. Akıllı telefonların en farklı özelliklerinden biri genellikle 'apps' olarak anılan üçüncü parti uygulama programlarının kullanıcılar tarafından telefona yüklenebilmesi ve çalıştırılabilmesidir. Bu uygulamalar genellikle resmi olarak çevrimiçi mağazalardan dağıtılmaktadır. Apple Store IOS platformu ve Google Play Store Android platformu için kullanılmaktadır. Bu mağazalar kullanıcıların yeni uygulamaları keşfetmesi ve yüklemesi için uygulama geliştiricilerine uygun bir mekân sağlamaktadır [1].

Android'in açık kaynak çekirdek politikası sebebiyle kötücül yazılım geliştiricileri bu mobil platform hakkında daha derin bilgi sahibi olabilmektedir. Google Market'in stratejisi dolayısıyla üçüncü parti uygulamaların geliştirilmesi teşvik edilmektedir [1]. 3. parti uygulama marketleri ise kapsamlı bir güvenlik taraması olmadan uygulama dağıtılmasına olanak sunmaktadır [2]. Android kötücül yazılım konusu hem kurumsal hem bireysel kullanıcılar için artan bir problem haline gelmektedir. Android işletim sistemini hedef alan zararlı uygulamaların sayısı dramatik bir biçimde atmaktadır. G DATA şirketinin 2016 birinci yarı mobil kötücül yazılım raporuna göre; G DATA güvenlik uzmanları 2016'nın ilk yarısında 1.723.265 adet yeni Android kötücül yazılım örneği tespit etmiştir. Ek olarak, Android kullanıcılarının sadece %13'ünün resmi Play Store'u kullandığı ve Android 6.0 sürümünde olduğu; %30'undan fazlasının ise hala eski Android sürümlerden biri olan Kitkat (4.4)'ı kullandığı ifade edilmiştir [3].

Android kötücül yazılıma karşı önlem almak için mevcut endüstri yaklaşımı telefona virüs tarayıcısı yüklemektir. Bu virüs tarayıcılar tipik olarak Dalvik sanal makinesinde çalışır ve bilinen kötücül yazılım imzalarıyla yüklenen uygulamaları karşılaştırır. Bu "kara liste" tekniği kötücül yazılım dağıtıcıları tarafından istismar edilebilen bir zayıflıktır. Bir sıfır-gün kötücül uygulaması kritik sistem dosyalarını değiştirerek ayrıcalık yükseltebilmekte ve telefonun davranışını değiştirebilmektedir. Bu sebeple virüs tarama motorları bu saldırıları gözden kaçırmaktadır [4].

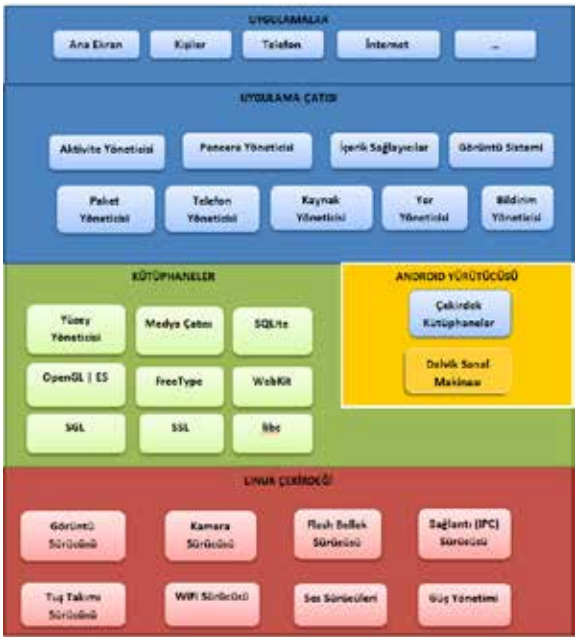
Akıllı telefonlar çoğunlukla kurum sınırları dışında da aktif olduğu için ağ seviyesindeki izleme araçları da etkili olmamaktadır. Bu yüzden, cihazların zararlı uygulamalara karşı kendilerini izleyebileceği sağlam yöntemler gereklidir [4]. Bu kötücül yazılımları tespit edip önlem almak için tespit mekanizmaları geliştirilmekte, buna karşılık olarak kötücül yazılım yazarları güçlü tekniklerle bu tespit tekniklerinden kaçmayı amaçlamaktadır.

Bu çalışmada, ikinci bölümde Android'in mimarisi anlatılmıştır. Üçüncü bölümde kötücül yazılımlara yer verilmiştir. Dördüncü bölümde kötücül yazılım (malware) tespiti için önerilen farklı yaklaşımlar incelenmiştir. Beşinci bölümde incelenen sistemlerin karşılaştırması yapılmış ve altıncı bölümde çalışmanın sonuçlarına yer verilmiştir.

II. ANDROID MİMARİSİ

Android işletim sistemi, Şekil 1'de gösterildiği gibi katmanlardan oluşan bir yazılım bileşenleri yığınıdır [5].

Katmanların en altı Linux 3.6'dır. Bu katman işlem yönetimi, bellek yönetimi, cihaz yönetimi, kamera, tuş takımı, görüntü vb. temel sistem fonksiyonlarını sağlar. Linux çekirdeğinin üstünde çatı (framework) kütüphaneleri ve veri tabanı erişimi, grafik çizimi gibi işlevlere olanak sağlayan bir kütüphane kümesi bulunur. Android Yürütücüsü, kilit bir bileşen olan Dalvik Sanal Makinası'nı sağlar. Bu bileşen, her Android uygulamasının kendi sürecinde ve kendi Dalvik Sanal Makinası üzerinde çalışmasını sağlar. Uygulama Çatısı Android uygulamalarına servisleri sağlar. Uygulama geliştiriciler bu servislerden faydalanırlar. Uygulamalar sadece uygulama katmanına yüklenmek üzere yazılır [5].



Şekil 1. Android mimarisi [5]

Android uygulamaları ".apk" uzantılı sıkıştırılmış dosyalardır. Android Application Programming Interface (API) kullanılarak geliştirilmektedir ve 4 tip bileşenden oluşur: aktiviteler, servisler, yayın alıcıları ve içerik sağlayıcılar. Android yazılımı uygulamalarla bu bileşenler aracılığıyla etkileşimde bulunur. Uygulama paketlerinde çoklu sınıf dosyaları yerine tüm sınıflar tek bir .dex uzantılı dosya içine paketlenir. Android uygulama paketleri uygulama bayt kodunu, yerel kod kütüphanelerini, uygulama kaynaklarını ve AndroidManifest'i içeren jar dosyalarıdır. AndroidManifest uygulama paket adını, uygulama izinleri vb. bilgileri içeren XML dosyasıdır. İnsan tarafından okunabilir XML formatında yazılır ve uygulama inşası sırasında binary XML'e dönüştürülür [6].

III. MOBİL KÖTÜCÜL YAZILIM

Bir kötücül yazılım akıllı telefona yüklendikten sonra cihazdaki veriye erişmeye çalışacak, normal işlevlerine müdahale edecek ya da uzaktan erişim açmak gibi telefonu daha savunmasız hale getirecektir [1]. Cabir, 2004 yılında tespit edilmiş Dünya'nın ilk mobil solucanıdır. Nokia 60 serisine zarar vermek için tasarlanmıştır. Saldırısı sonucunda ekranda 'Cabire' yazısı çıkmaktadır. Daha sonra solucan kendi kendini kopyalayarak telefonun bluetooth bağlantısını kullanarak yakınındaki diğer cihazlara bulaşmaktadır [7]. Genel olarak, çok çeşitli saldırı tipi kötücül yazılım aracılığıyla başlatılabilir. Bunların bazıları şunlardır:

•Casus Yazılım: Akıllı telefonlardan gizlice kullanıcı bilgilerini toplayan kötücül yazılımlardır [1].

•Gözetim Saldırıları: Kullanıcının telefonundaki GPS, mikrofon, kamera gibi sensörler aracılığıyla takip edilmesidir [1].

•Çevirici (Diallerware) Saldırıları: Kullanıcılar farkında olmadan yüksek oranlı arama ya da SMS servisleri ile yüksek ücretlere maruz bırakılabilirler [1].

•Finansal Kötücül Yazılım: Kredi kartı bilgilerini toplayan bir keylogger ya da gerçek bankacılık uygulamasını taklit eden bir uygulama olabilir [1].

•Botnetler: Uzaktan yönetilebilen kötücül yazılım bulaşmış zombi cihazlar topluluğudur. Organize bir biçimde saldırı başlatırlar [1].

•Solucan: Kendi kendini çoğaltır ve ağ üzerinde kullanıcı müdahalesi olmadan bir cihazdan başka cihaza bulaşabilir [1].

•Fidyecilik: Şifreleme ile kullanıcı verisi şifrelenmekte ya da ekranı kilitlemektedir ve şifre çözme anahtarı saldırganın elinde tutulmaktadır. Saldırgan, bir miktar para karşılığı veriyi ya da cihazı serbest bırakacağını iddia etmektedir.[3].

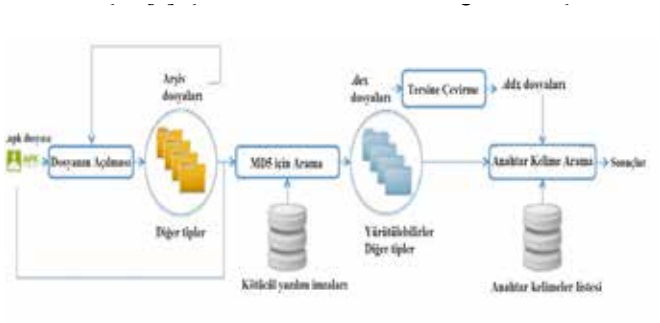
IV. VERİ SETLERİ ÜZERİNDEN KÖTÜCÜL YAZILIM TESPİTİ YAKLAŞIMLARI

Android kötücül yazılımlarının her geçen gün artmasıyla birlikte tespit yöntemleri de araştırılmakta ve geliştirilmektedir. Yapılan çalışmada bu yöntemlerden statik, dinamik, hibrit ve imza tabanlı çalışmalar incelenmiştir.

A.Statik Analiz Yaklaşımı

Bu yaklaşım, kötücül yazılım tespitinin uygulamalar cihaza yüklenmeden yapılmasını sağlar. Böylelikle mobil cihaz uygulamanın kötücül işlevinden etkilenmemektedir. Bu yaklaşım, uygulama çalıştırılmadan onun kötücül karakteristiklerini ve kötü kod parçalarını tespit eden hızlı ve pahalı olmayan bir yaklaşımdır [8–9].

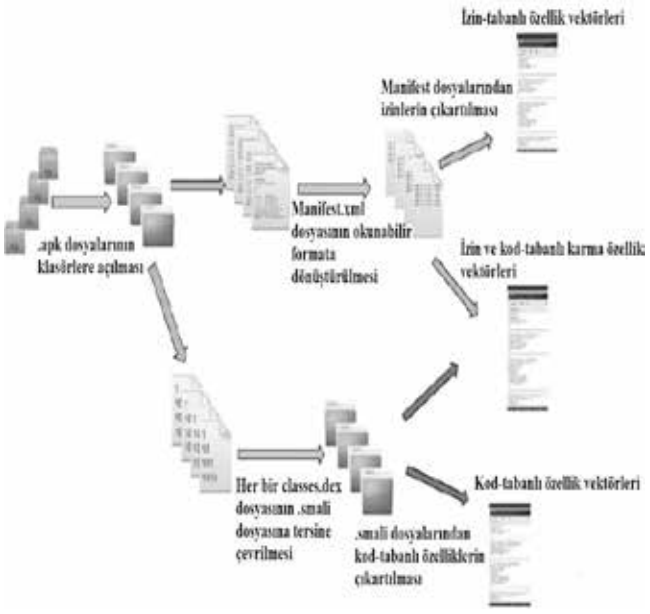
DroidAnalyzer, Android uygulamalarının potansiyel zafiyetlerini ve root ayrıcalığı istismarı varlığını tanımlayan bir statik analiz aracıdır. Çalışmada uygulama izinleri, riskli API'ler ve root ayrıcalığı istismarının varlığını gösteren anahtar kelimeler incelenmiştir. Riskli izinler ve anahtar kelimeler öncelikle veri seti üzerinde tespit edilmiş, daha sonra hedef uygulamalar incelenmiştir. Uygulamaların MD5 kriptografik özet değerleri ve anahtar kelimelere atanan şüphe seviyelerinin karşılaştırmasına dayalı bir algoritma kullanılmıştır [2]. Şekil 2'de aracın mimarisi gösterilmiştir.



Şekil 2. DriodAnalyzer mimarisi [2]

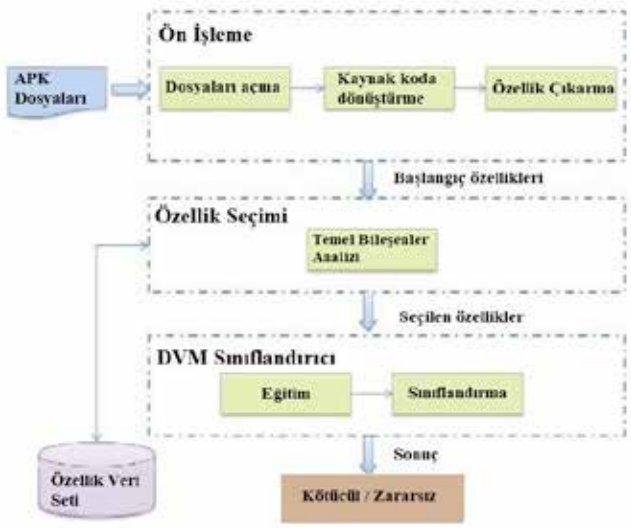
Xing Liu ve Jiqiang Liu izin tabanlı iki katmanlı bir tespit şeması önermişlerdir. İlk katman ilk iki aşamayı, ikinci katman üçüncü aşamayı içermektedir. Uygulama yükleme esnasında talep edilen izinler 'istenen izinler' olarak ve uygulama çalışması sırasında kullanılan izinler 'kullanılan izinler' adlandırılmıştır. Sistem tasarımında zararsız ve kötücül veri setindeki her uygulama için: istenen izinler açılan APK dosyasından alınan AndroidManifest.xml dosyası normal bir xml dosyasına çevrilerek ve daha sonra Python'daki xml.dom.minidom paketiyle ayrıştırılarak çıkartılmış ve boolean değerlere çevrilmiştir. Kullanılan izinleri elde etmek için Dex dosyasının analiz edilmesi gerekmektedir. Bunun için APK dosyası apktools ile geri derlenerek uygulamanın istenen izinleri ve smali kodu elde edilmiştir. Daha sonra her istenen izin için ilgili API çağrıları, içerik sağlayıcı URI'ları, ve intent action dizgilerine bakılmıştır. İlk aşamada istenen izinler ve C4.5'un WEKA uygulaması olan J48 sınıflandırıcı kullanılarak uygulamalar sınıflandırılmıştır. İkinci aşamada aynı kümedeki uygulamalar istenen izin çiftleri ve J48 sınıflandırıcı kullanılarak sınıflandırılmıştır. Eğer bir uygulama ilk iki aşamada zararsız olarak sınıflandırıldıysa o zararsız olarak kabul edilmektedir ya da kötücül olarak sınıflandırıldıysa kötücül olarak kabul edilmektedir. Eğer ilk iki aşamada farklı kümelerde sınıflandırıldıysa, üçüncü aşamada, başka bir kümeye konmakta ve kullanılan izinler çifti ve J48 sınıflandırıcı kullanılarak sınıflandırılmaktadır [10].

Yerima ve arkadaşları proaktif Android kötücül yazılım tespiti için statik analiz uygulayan Bayes sınıflandırması tabanlı makine öğrenmesi yaklaşımları önermiştir. Bu yaklaşımlarda izin tabanlı özellikler, kod tabanlı özellikler ve her ikisinden oluşan karma özellikli modeller incelenmiştir. İzin-tabanlı Bayes sınıflandırıcıda APK Analyser her uygulamanın manifest dosyasından izinleri çıkarmış ve izin detektörünü kullanarak standart Android izinleriyle eşleşme yapmıştır. Bir izin tespit edildiğinde onun sayısı yükseltilmiş ve kaydedilmiştir. Her izin için kaydedilen toplam Bilgi Kazancı'nı kullanan izin seçimi fonksiyonu tarafından derecelendirme ve en ilgili izinleri seçme için kullanılmıştır. Kod tabanlı Bayes sınıflandırıcıda, Bir miktar kod tabanlı özellik bir özellik detektörü setinin eşleşme kriteri olarak ayrıştırılmış ve APK analyser'da uygulanmıştır. Detektörler .smali dosyalarını ve varsa ek olarak dış kütüphaneleri, asset dosyalarını ve kaynak klasörlerini inceleyip ayrıştırmıştır. Bunlar daha sonra Bilgi Kazancı kriteriyle en ilgili özellikler seçilerek azaltılan büyük bir özellik seti sağlamıştır. Özellik seçimi aşamasından sonra en yüksek dereceli kod tabanlı özellik, eğitimde kullanılan her uygulamayı karakterize eden girdi özellik vektörlerini oluşturmak için kullanılmıştır. Derecelendirilmiş izinler ve kod tabanlı özelliklerden karma sınıflandırıcıda, özellik seçimi fonksiyonu aynı anda izinleri ve kodları derecelendirmek için kullanılmıştır. Daha sonra her ikisinden de en yüksek derecelendirilmiş olanlar Bayesian sınıflandırma modeli için girdi özellik vektörü olarak seçilmiştir. Şekil 3'te modelleri oluşturmak üzere otomatikleştirilmiş tersine mühendislik ve veri madenciliği için inşa edilen APK Analyser'ın yapısı gösterilmiştir. Yapılan sınıflandırma performansı değerlendirmeleri sonucunda bileşik tabanlı ve kod özelliği tabanlı modellerin izin tabanlı modellere göre daha iyi bir seçim olduğu görülmüştür [11].



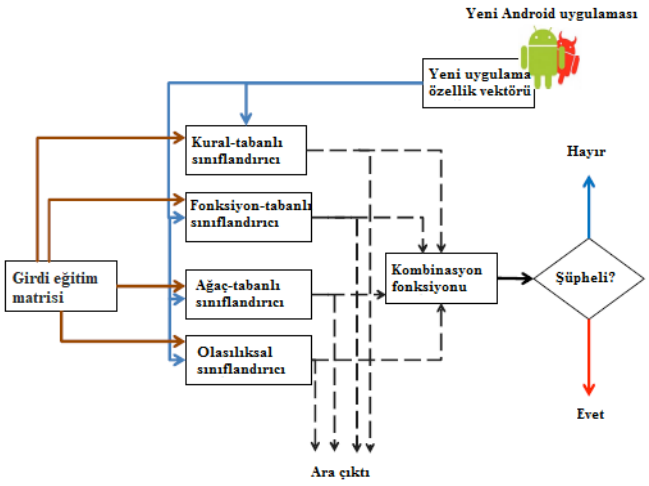
Şekil 3. APK Analyser tarafından yapılan otomatikleştirilmiş tersine mühendislik ve veri madenciliği [11]

Zhao Xiaoyan ve arkadaşları, izin tabanlı hafif bir statik kötücül yazılım tespit sistemi önermişlerdir. Şekil 4'te çatı modülleri gösterilmektedir. Ön İşleme Modülünde, AndroidManifest.xml dosyasından APK'ların izin listesi alınmıştır ve başlangıç özellik seti oluşturulmuştur. Manifest dosyasını okunabilir XML dosyasına çevirebilmek için AXMLPrinter2.Jar kullanılmıştır. Her uygulama için izin listesi Android sistem izinlerinin toplam setiyle karşılaştırılmıştır ve özellik değerleri 0 ya da 1 olarak kaydedilmiştir. Özellik Seçme Modülünde, orijinal özellik setinden Temel Bileşenler Analizi algoritmasıyla temel bileşen çıkartılmıştır. Destek Vektör Makinesi (DVM) Sınıflandırma Modülünde, eğitim aşamasında, kötücül ve zararsız uygulama örneklerinin özellik vektörleriyle sınıflandırıcı eğitilmiştir. Tespit aşamasında, sınıflandırıcı bilinmeyen bir APK'yı sınıflandırmaktadır. Özellik Veri Seti, örneklerden çıkartılan özellikleri depolama ve güncelleme ile sorumludur. [12].



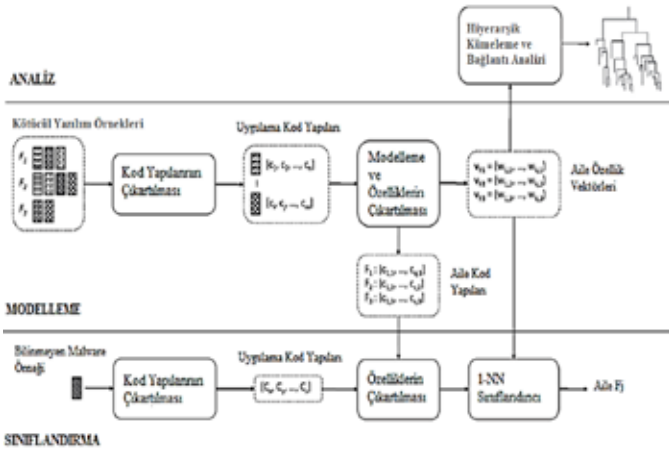
Şekil 4. Kötücül yazılım tespit çatısı [12]

Yerima ve arkadaşları statik özellikler kullanılarak paralel makine öğrenmesi sınıflandırıcıları vasıtasıyla kötücül yazılımın erken tespiti için bir metot önermişlerdir. Öğrenme aşaması için API ilişkin özellikler, uygulama izinleri, standart işletim sistemi ve Android çatı komutları kullanılmıştır. Çalışmada kullanılan algoritmalar şunlardır: Karar Ağacı (ağaç-tabanlı), Simple Logistic (fonksiyon-tabanlı), Naïve Bayes (olasılıksal), PART (kural-tabanlı), ve RIDOR (kural-tabanlı). Deneylerin ilk kısmı her bir aday sınıflandırma algoritmasıyla yapılmıştır. Naive Bayes sınıflandırıcının en düşük, PART'ın en yüksek doğruluk oranına sahip olduğu görülmüştür. Deneylerin ikinci kısmında her ayrı sınıflandırıcıdan elde edilmiş sınıflandırma kararlarının; olasılıklarının ortalaması, olasılıklarının çarpımı, maksimum olasılık, çoğunluk oylamasının sonucuna dayanan kombine sınıflandırma yaklaşımı incelenmiştir. En iyi doğruluk oranının olasılıkların çarpımı şemasından geldiği görülmüştür. Şemanın tüm performans sonuçlarının tek sınıflandırıcılardan daha iyi olduğu görülmüştür [13]. Şekil 5'te bu yaklaşımın mimarisi gösterilmiştir.



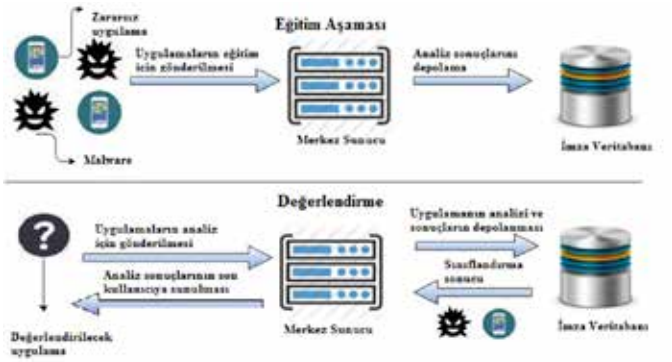
Şekil 5. Bileşik paralel sınıflandırıcı yaklaşımı [13]

Suarez-Tangil ve arkadaşları metin madenciliği ve bilgi alma tekniklerine dayalı bir sistem olan Dendroid'i önermişlerdir. Bu çalışmada, akıllı telefon kötücül yazılım örnekleri ve ailelerinin onların yazılım bileşenlerinde mevcut olan kod yapılarına dayanarak otomatik olarak analiz edilmesi için metin madenciliği yaklaşımlarının kullanımları araştırılmıştır. Dendroid'in ana yapı blokları Şekil 6'da sunulmuştur. Veri setinde bulunan her kötücül yazılım örneği için öncelikle Dalvik komutları tersine çevrilmiştir. Daha sonra Androguard kullanılarak kötücül uygulamaların kod parçaları çıkartılmış ve yapıları işlenmiştir. Vektör Uzay Modeli adapte edilerek her aileden aile özellik vektörü elde edilebilmesi için veri setindeki tüm aileler üzerinde uygulanmıştır ve bilinmeyen örnekleri bilinen aileler içine sınıflandırmadaki uygunluğu araştırılmıştır. Daha sonra, kötücül yazılım aileleri için filogenetik ağaçlar olarak anlaşılabilecek dendogramları türetmek için hiyerarşik kümeleme kullanımı üzerinde çalışılmıştır. Bu, aileler arasındaki ilişkileri, ortak soyların varlığını, belli kod özelliklerinin yaygınlığını analiz etmek için bir aracı analist olmuştur. Çalışmada yapılan deney sonuçlarında yaklaşımın önemli ölçüde kesin olduğunu ve kötücül yazılım örneklerinin büyük veri tabanları ile verimli biçimde baş ettiğini gösterdiği ifade edilmiştir [14].



Şekil 6. Dendroid'in yapısı [14]

Kabakuş ve arkadaşları izin tabanlı statik analiz yapan öğrenmeye dayalı bir sistem olan APK Auditor'ü önermişlerdir. Sistem mimarisi Şekil 7'de gösterilmiştir. Mobil cihaza yüklenen istemci uygulaması hem yereldeki uygulamaları hem de Play Store'da uygulamaları taramaktadır ve kullanıcılar uygulama izinleri ve güvenlik seviyeleri hakkında bilgi alabilmektedir. Uygulamanın talep ettiği izinler, hafıza yönetimi ve istemcinin koruma seviyesi istatistiği ara yüzde görsel olarak sunulmaktadır. Merkez sunucunun iki ana işlevi vardır: Play Store'dan düzenli olarak en popüler uygulamaların sisteme yüklenmesi, incelenmesi ve kötücül yazılım puanı hesaplanması ve Android uygulamalarının anlık olarak kötücül içerik kontrolünden geçirilmesi. Merkez sunucuda uygulamalar incelenirken öğrenmeye dayalı bir mekanizma sunulmuştur. Öğrenme aşamasında uygulamanın karakteristiği çıkarılmakta ve veri tabanında depolanmaktadır. Eğitim veri seti kullanılarak uygulamaları sınıflandırmak için kötücül yazılım skor eşik değeri ve lojistik regresyon kullanılmıştır. Değerlendirme aşamasında ise incelenmek istenen uygulama öğrenme sonucunda üretilen profillerden hangisine yakınsa o gruba dâhil edilmektedir. İncelenen uygulamalar, inceleme sonuçları, izinler, servisler ve alıcılar ilişkisel bir veri tabanı halinde depolanmaktadır [15].



Şekil 7. APK Auditor mimarisi [15]

Arslan ve arkadaşları fazladan izin talebinde bulunarak şüpheli kaynak erişimi yapabilecek Android uygulamalarını tespit etmek için, veri setleri kullanarak daha önceden belirlenmiş seviyeler doğrultusunda uygulamaların izin ve kod yapılarını inceleyerek risk değerlerini belirleyen bir yöntem önermişlerdir. Uygulamalar apktool ile açılarak Manifest dosyası okunabilir formata dönüştürülmüştür. Uygulamaların kaynak koduna erişmek için Dex2jar aracı kullanılmıştır. Manifest dosyasında istenen izinler 135 adet Android izni ile karşılaştırılmış, varsa 1 yoksa 0 değeri kullanılarak kötücül ve zararsız veri setleri için birer çizelge oluşturulmuştur. Daha sonra metin arama metodu kullanılarak her bir iznin kaynak kodunda çağırılıp çağırılmadığı 0 veya 1 değeri kullanılarak belirlenmiştir. Her bir uygulama için, talep edilmiş fakat kullanılmamış tüm izinlerin kötücül uygulamalar içerisinde kullanılma sayısı toplanarak şüphe değeri hesaplanmıştır. Bu değer zararsız uygulama veri setinin şüphe değeri ortalamasından yüksek ise uygulama kötücül olarak belirlenmiştir. Çalışmanın uygulama kısmında kötücül veri seti Drebin veri setinden ve zararsız veri seti bankacılık uygulamalarından alınarak oluşturulmuştur. Çalışma sonucunda kötücül ve zararsız uygulamalar için hesaplanan şüphe değeri yaklaşımının belli bir seviyede ayırt edici değerler elde etmeye yardımcı olduğu ifade edilmiştir. Ayrıca bu yaklaşımın tek başına yeterli olmadığı ve dinamik analiz yaklaşımı ile birlikte kullanılarak daha etkili ve doğru sonuçlar üreteceği belirtilmiştir [16].

Kayabaşı ve Doğru, oluşturdukları zararsız ve kötücül veri setleri üzerinden mobil uygulamaların sınıflandırılmasında kullanılan çeşitli makine öğrenmesi algoritmalarını güvenirlilik bakımından değerlendirmiştir. Zararsız uygulamalar Google Play Store'dan Android Market API kullanılarak indirilmiştir ve zararsız veri seti oluşturulmuştur. Kötücül uygulama veri seti için ise Malgenome Projesi olarak da bilinen Android Malware Genome Project'ten uygulamalar alınmıştır. Uygulamalar apktool aracını kullanan bir program kodlanarak tersine derlenmiştir. Uygulamaların API çağrıları, bu çağrıların paket düzeyindeki bilgileri ve başlangıç modelini oluşturmak için istenen izinler çıkartılarak zararsız ve kötücül uygulamalar için özellik kümesi belirlenmiştir. Zararsız ve kötücül sınıflara ait veri setleri kullanılarak, bir makine öğrenmesi algoritmaları aracı olan Weka ile sistemin eğitim aşaması gerçekleştirilmiştir. Çalışmada, sınıflandırma işlemini uygulamada başarılı olanlar seçilerek 4 adet makine öğrenmesi algoritması kullanılmıştır: KNN, Naive Bayes, ID3 ve J48. Çalışmada yapılan değerlendirmelerde en güvenilir algoritmanın KNN ve en zayıf algoritmanın ise Naive Bayes olduğu belirtilmiştir [17].

B.Dinamik Analiz Yaklaşımı

Statik analiz yaklaşımından farklı olarak, mobil uygulama analizleri yürütme esnasında yapılır. Statik analiz yaklaşımıyla ortaya çıkartılamayacak karışıklıktaki eksiklik veya açıklıklar ortaya çıkartılabilmektedir [8].

Burguera ve arkadaşları Android Platformunda kötücül yazılım tespiti yapmak için yeterli kaynak ve mekanizmaları sağlayan bileşenlere sahip bir çatı olan Crowdroid'i önermişlerdir. Crowdroid'in yapısı Şekil 8'de sunulmuştur. Bu uygulama Linux çekirdek sistem çağrılarını gözlemlemekle ve onları ön işlenmiş bir şekilde merkezi bir sunucuya göndermekle yükümlüdür. Crowdsourcing felsefesine göre kullanıcılar kullandıkları her uygulama için kişisel olmayan ama davranışsal veriyi göndererek yardımcı olacaklardır. Daha sonra uzak sunucu veriyi ayrıştırmakla ve uygulamalardaki her kullanıcı etkileşimi için sistem çağrı vektörü oluşturma ile yükümlü olacaktır. Böylece, kullanılan her uygulama için davranış verisi veri seti oluşmuş olacaktır. Son olarak, her veri seti bir bölücü kümeleme algoritması kullanılarak kümelenir. Bu şekilde meşru uygulamalar ile kötücül uygulamalar –aynı ada ve tanımlayıcıya sahip olsalar bile- arasındaki çok küçük sistem çağrı örüntüleri ayırt edilebilmiştir. Normallik modelini oluşturmak ve Android uygulamalarındaki anormal davranışları tespit etmek için bir önceki aşamada elde edilen vektörler analiz edilir ve kümelenir. Crowdroid sistem çağrılarını toplamak için Linux'ta bulunan Strace aracını kullanmaktadır. Crowdroid'in yapısı Şekil 8'de gösterilmiştir. Yapılan testlerin sonucunda,

sistem çağrılarını gözlemlemenin kötücül yazılım tespiti için uygulanabilir bir yöntem olduğu belirtilmiştir. [18].

Şekil 8. Crowdroid'in yapısı [18]

Y lu ve arkadaşları, Android cihazında uygulama davranışlarını gözlemleyen ve makine öğrenmesi tekniklerini uygulayarak uygulamaların zararsız ya da kötücül olduğunu tespit eden bir teknoloji önermişlerdir. Analiz ettikleri davranışlar şunlardır: 1)Kullanıcılardan yetkisi olmadan mesaj gönderme ya da silme, 2) Kullanıcının telefonunun kötücül olarak ele geçirildiğini fark etmemesi için mesaj önleme 3)Kullanıcının haberi olmadan uygulama yükleme, indirme ya da silme, 4) Kullanıcının SD kart içeriğini ele geçirme, 5)ICCID, IMEI, IMSI ya da MSISDN gibi mobil terminal hakkında bilgi edinme, 6) Kullanıcının arama geçmişi, telefon rehberi, konumu vb. kişisel bilgilerini elde etme, 7)Kullanıcı farkında olmadan internet bağlantısı yaparak kötücül kullanım yapma. Kötücül davranışı tetikleyen aktiviteleri gözlemlemek için aktiviteler ve yayın alıcıları incelenmiştir. Ek olarak kötücül davranışın yapılabilmesi için gereken izinler de AndroidManifest.xml'den alınmıştır. Naive Bayes sınıflandırmayı uygulamadan önce, etkinliğini arttırmak için özellikler Chi-Square metotla filtrelenmiştir. Kötücül yazılım davranışının amacına ulaşması için bir seri eylemi sırasıyla gerçekleştirmesi gerekmektedir. Örneğin, kullanıcının rehberini elde etmek (davranış) istiyorsa, öce onu okumalı, daha sonra internet ya da mesaj yoluyla bilgiyi göndermelidir. Dolayısıyla, davranışlar özellikler ve eylemler kümeleri ile ifade edilmiş ve Chi-Square metotla filtrelenmiştir. Chi-Square metodu kullanılarak ve kullanılmadan aynı veri seti üzerinde Naive Bayes sınıflandırma test edilmiştir. Kombine metodun daha düşük yanlış pozitif ve daha yüksek doğruluk oranı olduğu görülmüştür [19].

M. K. Alzaylaee ve arkadaşları Android uygulamalarını otomatik olarak analiz etmek için dinamik analiz tabanlı bir yapı olan DynaLog'u önermişlerdir. DynaLog'un bileşenleri Şekil 9'da gösterilmiştir [20].

Emülator-tabanlı güvenli sanal ortamda analiz bileşeninde, uygulama bir Android emülatörü üzerinde çalıştırılarak DroidBox aracı ile bazı üst seviye davranışlar ve karakteristikler çıkartılmaktadır. APK enstrümantasyon modülünde, DroidBox tarafından ayrıştırılamayan ve loglanamayan API çağrıları izlenmiştir. Bunun için, derleyici/ayırıcı araçlarını içeren APIMonitor aracı kullanılmıştır. Enstrümantasyon işlemi, dex dosyasına tersine mühendislik yapmayı ve uygulama çalışırken emülatör logunun içine bir API çağrısı sınıfının veya metodunun varlığını izlemek için kullanılabilecek imzaları eklemeyi içermektedir. Davranış/özellik loglama ve çıkarma bileşeninde, DynaLog izlenen davranışlara ya da API çağrı imzalarına karşılık gelen belirli log girdilerini çıkarma yeteneğini sağlar. Tetikleyici/egzersiz modülünde, MonkeyRunner aracı kullanılarak uygulamalara ekran dokunuşları, kaydırma vb. rastgele olaylar gönderilmektedir ve uygulamada mevcut olan tüm aktivite ve servislerin çalışması sağlanmaktadır. Log ayrıştırma ve işleme modülünde, otomatikleştirilmiş yapı ile analiz edilen her uygulama için çıkartılan özellikler okunabilir çıktı raporlarına biçimlendirilmektedir. Önerilen yapıyı değerlendirmek için Malgenome Projesinden alınmış kötücül ve MCAfee laboratuvarında incelenmiş zararsız uygulamalar kullanılmıştır. Yapılan değerlendirmeler sonucunda önerilen yapının sofistike Android kötücül yazılımının kitlesel tespitinde kullanılabilecek yetenekte olduğu ifade edilmiştir [20]

C.İmza Tabanlı Yaklaşım

Bu tür yaklaşımda uygulamalar analiz edilerek bir imza veri tabanında saklanır. Merkezi bir sunucu analiz ve koruma süreçlerini gerçekleştirirken, veri tabanı sunucusu analizleri saklar ve sonraki analizlerde tekrar kullanılmasını sağlamaktadır [8].

Guido ve arkadaşları kurumsal olarak kullanılan Android cihazlara istenerek ya da istenmeyerek yüklenmiş zararlı uygulamaların tespiti için, Android telefonlarda yerel bir bileşenle koşan Tractor Beam adında özel bir servis önermişlerdir. Servis, periyodik olarak her blok cihaz için değişen bit dizilerinin ofsetlerini, bir SHA256 kriptografik özeti yerel bir SQLite veri tabanında saklanmış bir önceki ölçüm ile karşılaştırarak tespit eder. Akıllı telefon merkez sunucunun dinlediği servisle Wi-Fi üzerinden iletişim kurabilir durumda olduğunda Tractor Beam güvenli yetkilendirilmiş bağlantıları başlatır, depolama ve analiz için her değişmiş bit dizisini telefon blok cihazından okur ve kopyalar. Tractor Beam'in yerel depolama ihtiyacı küçüktür çünkü blok cihaz bit dizileri değil sadece onun SHA256 kriptografik özetleri tutulur [4]. Merkez sunucu HTTPS portunu dinler. Merkez sunucunun servisi gelen bit dizileri ve ofset değerleri için dinler ve bunları normalize edilmiş ilişkisel veri tabanında saklar. Merkez sunucu aynı zamanda hem temel imajı hem veri tabanındaki gelen bit dizileri ve ofset yerlerini kullanarak hedef telefonun blok cihazlarının imajlarını dosya sisteminin geçici alanında tekrar oluşturur [4]. Analiz uygulama çatısı Detektör ve loglayıcılar olarak adlandırılmış, otomatize edilmiş adli bilişim işlemleri serisini yeniden oluşturulmuş imajlar üzerinde dinamik bir biçimde çalıştırmaktadır. Detektörlerin içinde kötücül aktiviteyi tespit edecek teknikler geliştirilmiştir ve loglayıcılar şüpheli aktiviteleri kaydeder. Tractor Beam ve bileşenlerinin sık değişmemesi gereken dosya sistemi değişikliklerini tespit ettiği, cihaz yeniden başlatıldıktan sonra kötücül yazılımın tekrar başlamasına izin veren sürekli yapıları bulduğu, yeni yüklenmiş uygulamalar içinde dosya sistemine konulan kötücül dosyaları bulduğu ifade edilmiştir [4].

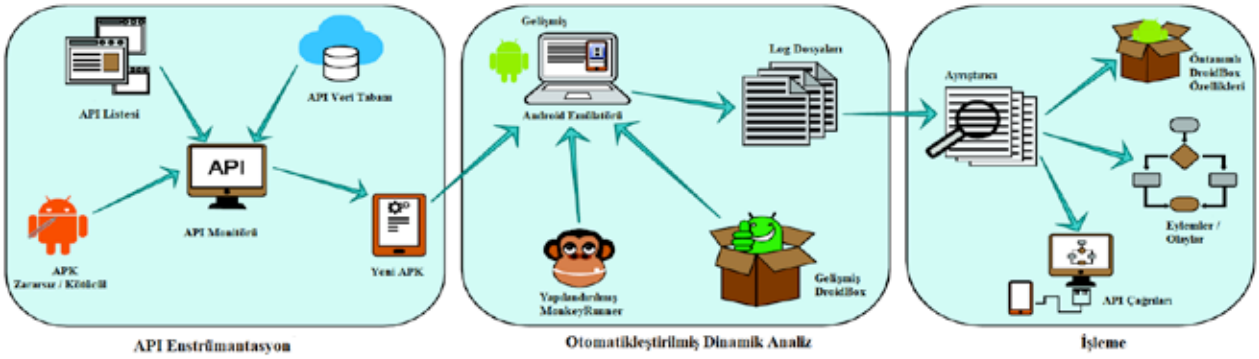
D.Hibrit Analiz Yaklaşımı

Bu yaklaşımda uygulamanın sahip olduğu hem statik hem

dinamik özellikler kullanılarak kötücül yazılım analizi yapılmaktadır.

Wang ve arkadaşları anomali tespiti ve suistimal tespitini entegre eden hem uygulama marketleri hem de kullanıcılara yönelik hibrit bir mobil kötücül yazılım tespit sistemi önermişlerdir [21].

Bu sistem iki ana kısımdan oluşmaktadır: suistimal detektörü statik ve dinamik analiz yaparak bilinen kötücül yazılım ya da yeni varyantlarını tespit etmek ve sınıflandırmakla sorumlu iken, dinamik analiz sonuçları kullanılarak anomali detektörü yeni ve bilinmeyen sıfır gün kötücül yazılımlarını tespit edebilmektedir. Hibrit analiz için gereken aşırı hesaplama kaynaklarından dolayı hem suistimal detektörü hem de anomali detektörünün cihaz dışında bulut gibi bir ortamda konuşlandırılması gerektiği ifade edilmiştir [21].



Şekil 9. DynaLog'un bileşenleri [20]

Suistimal tespitinde statik ve dinamik özellikler çıkartılmıştır. Statik analiz başlıca manifest dosyası ve tersine çevrilen dex kodlarından sağlanan özelliklere odaklanmıştır. Android Asset Packaging Tool adapte edilerek statik özellikler çıkartılmıştır. Dinamik analizde kullanılacak özellikleri çıkartmak için bir dinamik analiz çatısı olan CuckooDroid aracından yararlanılmıştır ve dosya erişimi ve operasyonları, alıcı kayıtları, çalıştırılan komutlar, içerik çözen sorgular, dinamik şüpheli aramalar, ağ operasyonları vb. olaylar izlenmiştir. Daha sonra bu statik ve dinamik özellik dizgilerini 0 ve 1 ile temsil eden numerik vektörlere dönüştürülmüştür. Çıkartılan çok sayıdaki özellik Chi2 puanlama fonksiyonu ile en yüksek puana sahip olanlar bulunarak azaltılmıştır ve özellik seçimi yapılmıştır. Daha sonra bir linearSVC sınıflandırıcı bu özellik vektörleri ile eğitilmiştir. Bilinmeyen bir uygulama sisteme verildiğinde onun özellik vektörü bu sınıflandırıcı tarafından işlenmektedir ve kötücül yazılım olup olmadığına karar verilmektedir. Eğer uygulama zararsız olarak tespit edildiyse anomali tespiti tetiklenmektedir. Değilse çoklu-aile sınıflandırıcısı kullanılarak belli bir kötücül yazılım ailesine sınıflandırılmaktadır. Anomali tespitinde dinamik özellikler kullanılmaktadır. Özellik seçimi için VarianceThreshold yaklaşımı kullanılmıştır. Anormal uygulamaları tespit etmek için, tek-sınıf DVM sınıflandırıcı zararsız uygulamalar kullanılarak inşa edilmiştir. Yeni uygulama, bu eğitilen sınıflandırıcı tarafından sıfır-gün kötücül ya da zararsız uygulama olarak etiketlenmektedir [21].

Tianda Yang ve arkadaşları etkili mobil kötücül yazılım analizi için statik bir madencilik algoritması ile dinamik bir kusur analizini kullanan hibrit bir yaklaşım önermişlerdir. Bu yaklaşımda, statik analiz ile öncelikle olası saldırı kritik yollar Android API'lerine ve mevcut saldırı desenlerine göre belirlenmekte ve dinamik analiz ile belirlenen yollar takip edilerek mevcut saldırı örnekleriyle uyumluluğu kontrol edilerek saldırı olasılığını tespit etmek için uygulama sınırlı ve odaklanmış bir kapsamda çalıştırılmaktadır. Statik analiz aşamasında; apktool kullanılarak uygulamalar açılarak kaynak dosyalarına ulaşılmaktadır. dex2jar kullanılarak .dex dosyası .class dosyalarına dönüştürülmektedir. Bir API seti oluşturmak için jd-gui kullanılarak API'ler okunmakta ve hassas olanları seçilmektedir. Apriori algoritması temel alınarak geliştirilmiş DApriori algoritması son kümeyi oluşturmak için çalıştırılmaktadır. Elde edilen küme daha önce oluşturulmuş kötücül kütüphanesiyle karşılaştırılmaktadır ve belirlenen orandaki benzerliğe göre karar verilmektedir. Çalışmada, zararlı kütüphanesi oluşturmak için popüler zararlı uygulamalar seçilmiş ve örnekler Androguard ve Contagio Mobile'dan toplanmıştır. Daha sonra 12 adet mobil uygulama üzerinde DApriori çalıştırılmıştır: WhatsApp, Facebook, Zitmo, Godwon, GoldDream, Pincer, Gazon, SMSGoogle, Tele, Samsapo, FakenotifyB and Mouabad. Uygulamaların tamamının şüpheli olarak tanımlanması statik analizin bir kısıtlaması olarak ifade edilmiştir. Dinamik analiz aşamasında: öncelikle uygulama simüle edilmiş bir ortamda çalıştırılmaktadır, ardından izleme için bir uygulama davranışları listesi seçilmektedir. Aktiviteler bir log dosyasında saklanmaktadır ve kötücül niyet için analiz edilmektedir. Çalışmada statik analiz aşamasına göre 3 adet davranış izlenmek üzere seçilmiştir: sistem çalıştırılabilir yolu /system/xbin gibi kritik dizin yoluna erişim, http sunucular için alan adı erişimi, yeterli açıklama olmadan ücretlendirme. Çalışmada dinamik kusur analizi için Droidbox aracı kullanılmıştır. Bu araç yürütme sırasında hedefi ve gönderilen veriyi takip etmek için hassas API'leri izlemektedir. Çalışmada dinamik analiz Godwon uygulaması üzerinde çalıştırılmıştır ve log dosyası ve davranış grafiklerine göre uygulamanın zararlı olduğu sonucuna varılmıştır [22].

V. SİSTEM KARŞILAŞTIRMALARI

Bu bölümde incelenen çalışmaların yaklaşımları, kullandığı

araçlar ve servisler, veri setleri ve kullanılan yöntem ve algoritmalar bakımından genel bir bakış sunulmuştur. Tablo 1'de bu karşılaştırmaya yer verilmiştir.

Statik analizde yaygın olarak izinler, API çağrıları ve kod özellikleri kullanılmaktayken dinamik analizde davranışlar, aktiviteler ve sistem çağrıları gözlemlemektedir. Kötücül uygulamalar için Android Malware Genome Project veri setinin yaygın olarak kullanıldığı ve Google Play Store ve 3. parti resmi olamayan marketlerden zararsız uygulamaların alındığı, zararsız olduğunun doğrulanması için Virustotal tarama servisinin kullanıldığı görülmektedir. Android Malware Genome Project (AMGP) veri seti Yajin Zhou ve Xuxian Jiang tarafından yapılan çalışma sonucunda ortaya çıkmıştır. 49 farklı kötücül yazılım ailesinden ve 1260 örnekten oluşan ilk büyük koleksiyondur. Örnekler resmi ve alternatif marketlerden toplanmıştır [23].

Sıkıştırılmış formata sahip apk uzantılı uygulama dosyalarını açmak ve izinler, kodlar gibi uygulama özelliklerini kullanabilmek için AXMLPrinter2.jar, Baksmali, apktools, dex2jar gibi çeşitli tersine mühendislik araçları kullanılmıştır. Bunun yanında dinamik özellikleri elde etmek için ve uygulama davranışlarını gözlemleyebilmek için Strace, CuckooDroid ve DroidBox araçları kullanılmıştır. Android kötücül yazılım tespitinde makine öğrenmesi algoritmalarının yaygın olarak kullanılmaya başlandığı görülmektedir. Ek olarak daha etkin sistemler geliştirmek için birden çok makine öğrenmesi algoritmasının birlikte kullanıldığı da görülmüştür.

VI. SONUÇ

Andriod tabanlı telefonların yaygınlaşmasıyla birlikte Android için geliştirilen kötücül yazılımlar artan bir problem haline gelmiştir. Bu kötücül yazılımlar kişisel, kurumsal ve ulusal güvenlik bakımından bir tehdit oluşturmaktadır. Bu çalışmada bu kötücül yazılımlara yönelik tespit mekanizmaları incelenmiştir.

Dinamik analiz sadece yürütme esnasındaki uygulama davranışlarını izleyebilmektedir ve potansiyel zafiyetleri tespit etme yeteneğinden yoksundur. Statik analiz uygulama cihaza yüklenmeden önce potansiyel zafiyetleri tespit edebilmektedir fakat uygulama davranışlarını gözlemlememektedir. Hibrit yaklaşımlar hem statik hem dinamik analiz yapabilmektedir fakat yüksek kaynak kullanımına ihtiyaç duymaktadır.

Mobil cihaz kullanıcıları 3. parti marketlerden uygulama indirmekten kaçınmalıdır. Bir uygulamanın 3. parti uygulama marketlerindeki sürümü resmi marketlerdekine göre farklılıklar gösterebilmektedir ya da buradaki uygulamalar kötücül niyetle geliştirilmiş uygulamalar olabilmektedir.

Resmi uygulama marketleri uygulamaları detaylı olarak incelemeli ve etkin tespit mekanizmaları kullanarak kötücül uygulamaların bu kaynaklardan dağılmasına karşı önlem almalıdır. Uygulama izinleri güvenlik açısından önemli bir role sahiptir. Kullanıcılar uygulamaların talep ettiği izinlere karşı dikkatli olmalıdır. Kullanıcıların bir anti-kötücül yazılım ürünü kullanmaları bilinen kötücül uygulamalara karşı önlem almayı sağlamaktadır.

Mevcut önleme yaklaşımları ve tespit araçları bazı saldırıları önlemeye yardımcı olsa da kötücül yazılım davranışı hızla değişmektedir ve kötücül yazılım geliştiricileri günden güne tespit mekanizmalarından kaçabilecek yeni kötücül uygula-

TABLO I. SİSTEM KARŞILAŞTIRMALARI

Çalışma	Yaklaşım	Araçlar / Servisler	Veri Seti Kaynağı	Yöntem / Algoritma
DroidAnalyzer [2]	Statik	Dedexer	AMGP, 3.parti marketler, Google Play Store.	Kelime ve kriptografik özet eşleşme algoritması
X. Liu ve J. Liu [10]	Statik	Apktools, xmldom.minidom	AppChina AMGP, Çin güvenlik şirketleri	Karar ağacı (C4.5)
Yerima ve arkadaşları [11]	Statik	AXML2jar, Baksmali, APKAnalyser, Virustotal	AMGP, 3.parti marketler	Naive Bayes, Bilgi Kazancı
Xiaoyan ve arkadaşları [12]	Statik	AXMLPrinter2.jar	AMGP, Google Play Store	DVM, Temel Bileşenler Analizi
Yerima ve arkadaşları [13]	Statik	APKAnalyser	MCAfee dahili kaynakları	Karar Ağacı, Simple Logistic, Naive Bayes, PART, RIDOR
Dendroid [14]	Statik	Androguard	AMGP	Vektör Uzay Modeli, 1-NN
APK Auditor [15]	Statik	APIfy ve 42matters web servisi,	Contagio mobile, Drebin, AMGP, Google Play Store	Lojistik regresyon
Arslan ve Arkadaşları [16]	Statik	Apktool, Dex2jar	Drebin, bankacılık uygulamaları	Şüphe değeri karşılaştırması
Kayabaşı ve Doğru [17]	Statik	Android Market API, apktool, Weka	Google Play Store, AMGP	KNN, Naive Bayes, ID3 ve J48
Crowdroid [18]	Dinamik	Strace	Crowdroid kullanıcıları, resmi ve resmi olmayan marketler	k-means
Y. lu ve arkadaşları [19]	Dinamik	Belirtilmemiş.	Belirtilmemiş.	Naive Bayes, Chi Square
DynaLog [20]	Dinamik	DroidBox, APIMonitor, MonkeyRunner	AMGP, MCAfee laboratuvarı	Davranış analizi
Guido ve arkadaşları [4]	İmza	Tractor Beam	AMGP	Bit dizilerinin karşılaştırılması
X. Wang ve arkadaşları [21]	Hibrit	CuckooDroid, Android Asset Packaging Tool, VirusTotal	Çin uygulama mağazaları, Drebin	LinearSVC, tek-sınıf DVM
T. Yang ve arkadaşları [22]	Hibrit	Apktool, dex2jar, jd-gui, DroidBox	Androguard, Contagio Mobile	DApriori, benzerlik, kusur analizi

malar geliştirmektedir. Bu nedenle, kötücül yazılım geliştikçe daha etkin araçların geliştirilmesine ihtiyaç vardır. Bu amaçla öğrenmeye dayalı makine öğrenmesi yaklaşımları günden güne önerilen sistemlerde kullanılmaya başlanmıştır. Mobil cihazlardaki kısıtlı kaynaklar kötücül yazılım tespitine yönelik araçlar geliştirilirken dikkate alınmalıdır.

KAYNAKLAR

[1]D. He, S. Chan, M. Guizani, "Mobile application security: malware threats and defenses," IEEE Wireless Communications, vol. 22(1), pp. 138-144, February 2015.

[2]S.- H. Seo, A. Gupta, A. M. Sallam, E. Bertino, K. Yim, "Detecting mobile malware threats to homeland security through static analysis," Journal of Network and Computer Applications, vol. 38, pp. 43-53, February 2014,

[3]G DATA Mobile Malware Report. (Visited July 2017) [Online]. Available: https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_Mobile_Malware_Report_H1_2016_EN.pdf.

[4]M. Guido, J. Ondricek, J. Grover, D. Wilburn, T. Nguyen, A. Hunt, "Automated identification of installed malicious Android applications," Digital Investigation, vol. 10, pp. 96-104, August 2013.

[5]Android – Architecture. (Visited July 2017) [Online]. Available: http://www.tutorialspoint.com/android/android_architecture.htm

[6]V. Rastogi, Y. Chen, X. Jiang, "DroidChameleon: evaluating Android anti-malware against transformation attacks," In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pp. 329-334, May 2013.

[7]A. Apvrille, "The evolution of mobile malware," Computer Fraud & Security, vol. 2014(8), pp. 18-20, August 2014.

[8]A. T. Kabakuş, İ. A. Doğru, A. Çetin, "Android kötücül yazılım tespit ve koruma sistemleri," Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, vol. 31(1), pp. 9-16, March 2015.

[9]M. Chandramohan, H. B. K. Tan, "Detection of mobile malware in the wild," IEEE Computer, vol. 45(9), pp. 65-71, January 2012,

[10]X. Liu, J. Liu, "A two-layered permission based android malware detection scheme," In 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 142-148, April 2014.

[11]S. Y. Yerima, S. Sezer, G. Mcwilliams, "Analysis of bayesian classification-based approaches for android malware detection," IET Information Security, vol. 8(1), pp. 25-36, January 2014.

[12]Z. Xiaoyan, F. Juan, W. Xiujuan, "Android malware detection based on permissions," In 2014 International Conference on Information and Communications Technologies (ICT 2014), pp. 1-5, May 2014.

[13]S. Y. Yerima, S. Sezer, I. Muttik, "Android malware detection using parallel machine learning classifiers," In 2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, pp. 37-42, September 2014.

[14]G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, J. Blasco, "Dendroid: a text mining approach to analyzing and classifying code structures in Android malware families," Expert Systems with Applications, vol. 41(4), pp. 1104-1117, March 2014.

[15]A. T. Kabakus, I. A. Doğru, A. Cetin, "APK Auditor: Permission-based Android malware detection system," Digital Investigation, vol. 13, pp. 1-14, June 2015.

[16]R. S. Arslan, I. A. Doğru, N. Barışçı, "Android Mobil Uygulamalar için İzin Karşılaştırma Tabanlı Kötücül Yazılım Tespiti," Politeknik Dergisi, vol. 20(1), pp. 175-189, Haziran 2016.

[17]G. Kayabaşı, I. A. Dogru, "Mobil Uygulamaların Sınıflandırmasında Kullanılan Makine Öğrenmesi Algoritmalarının Güvenirlilik Tespiti," ISCTurkey 2016 Bildiriler Kitabı, pp. 191-195, Ekim 2016.

[18]I. Burguera, U. Zurutuza, S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for Android," In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, pp. 15-26, October 2011.

[19]Y. Lu, P. Zulie, L. Jingju, S. Yi, "Android malware detection technology based on improved bayesian classification," In 2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC), pp. 1338-1341, September 2013.

[20]M. K. Alzaylee, S. Y. Yerima, S. Sezer, "Dynalog: an automated dynamic analysis framework for characterizing android applications," In Proceedings of the 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), pp. 1-8, June 2016.

[21]X. Wang, Y. Yang, Y. Zeng, C. Tang, J. Shi, K. Xu, "A novel hybrid mobile malware detection system integrating anomaly detection with misuse detection," In Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services, pp. 15-22, September 2015.

[22]T. Yang, K. Qian, L. Li, D. Lo, L. Tao, "Static Mining and Dynamic Taint for Mobile Security Threats Analysis," In IEEE International Conference on Smart Cloud (SmartCloud), pp. 234-240, November 2016.

[23]Y. Zhou, X. Jiang, "Dissecting android malware: characterization and evolution," In 2012 IEEE Symposium on Security and Privacy, pp. 95-109, May 2012.

Android Uygulama İzinlerinin Analizi ile Kötücül Yazılım Tespiti

DETECTING Malware using Android Application Permissions

Ahmet SUSAR
Bilişim Sistemleri Anabilim Dalı
Gazi Üniversitesi Bilişim Enstitüsü
Ankara, Türkiye
ahmet.susar@gazi.edu.tr

İbrahim Alper DOĞRU
Bilgisayar Mühendisliği Bölümü
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
iadogru@gazi.edu.tr

Murat DÖRTERLER
Bilgisayar Mühendisliği Bölümü
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
dorterler@gazi.edu.tr

Özet

Mobil cihazların kullanımı günden güne artarak devam etmiş ve mobil cihazlar sağladığı kolaylıklar sayesinde yaygınlaşmışlardır. İlerleyen yıllarda da mobil cihazların kullanımındaki artışın devam edeceğini araştırmalar göstermektedir. Mobil cihazların önemli, kişisel ve hassas bilgilere erişme özellikleri ile bu cihazlarda Android platformunun yaygın bir şekilde benimsenmesi; bu cihazları kötücül yazılım geliştiren kişilerce, potansiyel kazanç ve kişisel şöhret gibi amaçlarla, cazip bir hedef haline getirmiştir. Kullanıcıların hayati değere sahip bilgilerinin güvenliği için, Android cihazlarda bilgi güvenliğinin sağlanması kaçınılmaz derecede önemlidir. Hem kötücül yazılımların devamlı olarak kendini yenileyerek artması hem de kritik verileri korumak için kötücül yazılım geliştiren kişilerden bir adım önde olma gerekliliği, bu konuda yapılan çalışmaları sürekli hale getirmiştir. Android platformunda çeşitli analiz yöntemleri ile kötücül yazılım tespiti yapılmaktadır. Bu çalışmada Android platformunda uygulama izinlerine odaklanan statik analiz yöntemi ile kötücül yazılımların tespiti amaçlanmıştır.

Anahtar Kelimeler

Android, kötücül yazılım tespiti, mobil güvenlik, uygulama izinleri, mobil cihaz güvenliği.

Abstract

The use of mobile devices has been increasing day by day and the mobile devices have become widespread thanks to the conveniences they provide. The researches show that the increase in the use of mobile devices will continue in the upcoming years. The feature of the mobile devices that allows them to access important, personal and sensitive information and the Android platform being adopted widely have made these devices an inviting target for the malware developing people for aims such as potential gain and personal fame. Providing information safety in Android devices is inevitably significant for the safety of the vital information of the users. Both the continuous and self-renewing increase of the malware and the necessity to be one step ahead of the persons developing malware in order to protect the critical data have made the works concerning this matter continuous. A malware detection in the Android platform is being done via various analysis methods. In this study, the detection of malware via a static analysis method focusing on the application permissions in the Android platform is aimed.

Index Terms

Android, malware detection, mobile security, application permissions, mobile device security.

I. GİRİŞ

Sürekli artan mobil cihaz kullanımı, zamanla mobil cihazların hem kişisel hem de ticari alanda popüler olmasını sağlamıştır [1]. 2020 yılına kadar yaklaşık 6,1 milyar mobil cihaz kullanıcısı olacağı [2] ve internet erişiminin yaklaşık yarısının mobil cihazlar üzerinden sağlanacağı tahmin edilmektedir [3]. Mobil teknolojinin hızla gelişmesi ile ortaya çıkan mobil servisler yaşam kalitesini yükseltmektedir [4]. Akıllı telefonlar mobil cihazlar olarak ortaya çıkarak bilgisayarlardan çok daha etkili olmuşlardır [5]. Kullanıcılar akıllı telefonlardan yararlanmalarına rağmen, kötücül yazılımlar ile gizli ve hassas bilgiler çalınabilmektedir [6]. İletişim uygulamaları (örneğin, Whatsapp ve Facebook Messenger gibi) kişisel bilgileri, elektronik belgeleri, müzikleri, resimleri, e-postaları ve coğrafi konum bilgilerini saklamaktadır [7]. Mobil cihazlarda bulunan bu önemli bilgiler, bu cihazları potansiyel kazanç ve kişisel şöhret gibi amaçlarla kötücül yazılım geliştiren saldırganların hedefi haline getirmiştir.

Akıllı telefon işletim sistemleri arasında Android, 2016 yılının dördüncü çeyreğinde toplam pazarın %81.7'sini elinde tutmaktadır. 2016 yılında Android, pazar payını %3.2 oranında artırarak %84.8'lik pazar payına ulaşmıştır ve pazar payını yıllık olarak artıran tek işletim sistemi olmuştur [8]. Bütün mobil işletim sistemleri kötücül yazılım geliştiren kişiler tarafından potansiyel hedef sayılsa da genellikle en çok kullanılan işletim sistemi olan Android platformu daha cazip bir hedef konumundadır.

Mobil kötücül yazılım ile ilgili yapılan araştırmalar, Android platformundaki kötücül yazılımların devamlı olarak arttığını göstermektedir. Ortalama her 14 saniyede yeni bir kötücül yazılımın ortaya çıktığı belirtilen araştırmalarda, 2015 yılının ikinci çeyreğinde ortaya çıkan 560.671 yeni Android kötücül yazılımın, aynı yılın ilk çeyreğine kıyasla %27'lik bir artış gösterdiği raporlanmıştır [9]. Ayrıca kötücül yazılımlar %98.05 oranında Android işletim sistemlerini hedeflemektedir [10].

Android platformunun saldırıların öncelikli hedefi olması, hızla büyüyen uygulama marketlerinin yönetimini önemli bir konu haline getirmiştir [1]. Uygulama marketleri aracılığı ile kullanıcıların kullanımına sunulan uygulamalar incelendiğin-

de, birçok uygulamanın çalışması için ihtiyaç duyduğu izin sayısından daha fazla izin talebinde bulunduğu görülmüştür. İhtiyaç duyduğundan daha fazla izin talebinde bulunulması, uygulamanın kötücül özellikte olabileceğini düşündürmekte ve uygulamayı şüpheli bir hale getirmektedir. Bu yüzden şüpheli davranışları sergileyen uygulamaların takip edilmesi gerekmektedir [11].

Android yeni sürümlerinde daha güvenilir bir uygulama izin sistemi geliştirmiştir. Android 6.0'dan (Android Marshmallow) önceki sürümlerde kullanılan uygulama izin sisteminde, uygulama indirilirken kullanıcıdan alınan izinler uygulama yüklü kaldığı müddetçe uygulama tarafından kullanılabilmektedir [12]. Android 6.0 ve sonraki sürümlerde ise, uygulama mobil cihaza yüklendikten sonra uygulamanın kullandığı izinler kullanıcı tarafından tek tek kontrol edilebilmektedir [13]. Bunun yanında, cihazın, verilerin ve uygulamaların güvenliğini sağlamak amacıyla sürekli çalışan Google Play Protect kullanıma sunulmuştur [14]. Android 7.0 (Android Nougat) ve sonraki sürümler için geliştirilen Google Play Protect, Google Play Store uygulamalarının mobil cihaza indirilmeden önceki güvenlik kontrolünü gerçekleştirmektedir. Ayrıca başka kaynaklardan mobil cihaza yüklenen uygulamaları kontrol ederek, kötücül uygulamalar hakkında kullanıcıyı uyarmakta ve kötücül uygulamaların cihazdan kaldırılması sağlamaktadır [15].

Her ne kadar Android'in yeni sürümleriyle yeni güvenlik mekanizmaları sunulsa da, mobil cihaz üreticileri ancak yakın zamanda piyasaya sürdükleri ürün modelleri için güncelleme desteği vermektedir. Dolayısıyla Android tabanlı cihaz kullanıcılarının önemli bir kısmı eski sürümleri kullanmaya devam etmektedir. Bu çalışma mobil uygulamalarda, izinleri grup halinde onaylamayı gerektiren Android 6.0'a kadar olan sürümlerdeki uygulama izinlerine odaklanmıştır. Mobil cihaza yüklenen uygulamalar, çeşitli araçlar ile analiz edilerek, uygulama izinlerinin risk seviyeleri, uygulamalarda tespit edilen kötücül yazılımlar, tehlikeli izin kullanımı ve kötücül uygulamaların istedikleri izinleri kullanıp kullanmadıkları araştırılmıştır. Bu sayede kötücül yazılımlar tespit edilerek mobil cihaz kullanıcılarının hassas bilgilerinin korunması hedeflenmektedir. Veri seti, 50 iyicil ve 50 kötücül toplam 100 uygulama ile oluşturulmuştur. Bu çalışmanın ikinci bölümde Android platformunda uygulama izinleri anlatılmıştır. Üçüncü bölümde uygulama izinleri analiz edilerek; dördüncü bölümde sonuç ve değerlendirmelere yer verilmiştir.

II. ANDROID PLATFORMUNDA UYGULAMA İZİNLERİ

Android platformunda izinler, mobil cihazın SMS gönderimi, mikrofon, kamera, konum bilgisi gibi çeşitli kaynaklarını kullanarak, uygulamadan beklenen görevi yapabilmesi için uygulamaların ihtiyaç duyduğu onaylardır [16]. Android 6.0'dan önceki sürümlerde, cihaza indirilecek olan uygulamanın beklenen görevleri yapabilmesi için, uygulama indirilmeden istenilen izin grubuna onay verilmesi gerekmektedir. Uygulamanın istediği izin grubuna onay verildikten sonra, yüklenen uygulama izin grubunda yer alan izinlerden ihtiyaç duyduğunu kullanabilmektedir [12]. Bu durum çeşitli riskleri de beraberinde getirmektedir. Örneğin, kullanıcının cihazına yüklediği bir uygulama, izin grubunun içinde bulunan çeşitli izinleri kullanarak, kullanıcı fark etmeden, kötücül faaliyetler gerçekleştirebilmektedir.

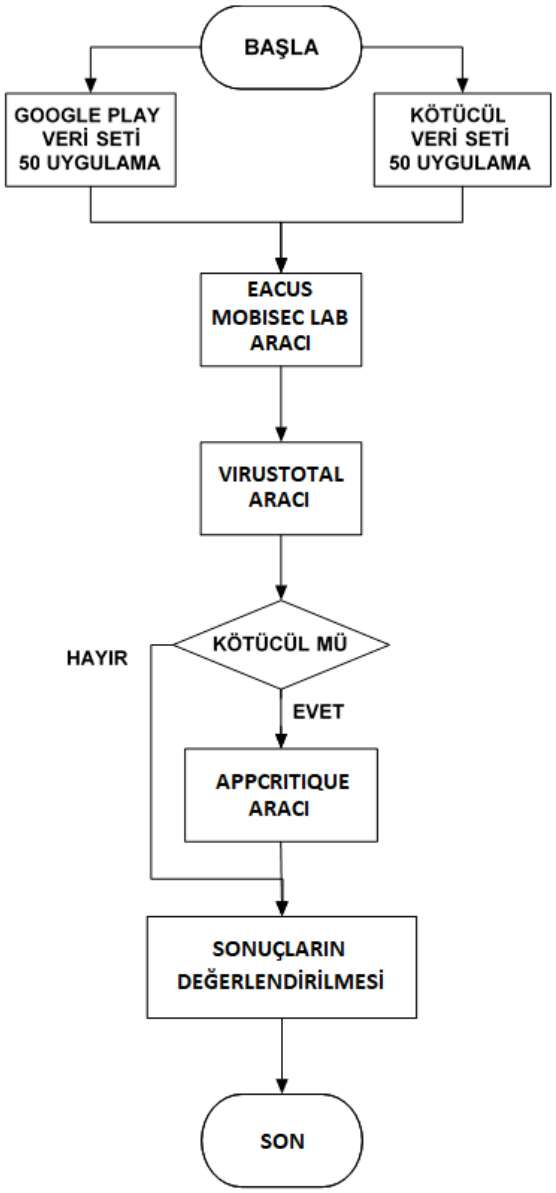
Android platformu izinleri, çeşitli koruma seviyelerine ayrılmıştır. Bunlardan iki tanesi önemlidir; normal ve tehlikeli izinler. Normal izinler, kullanıcı için çok az gizlilik riski oluşturmaktadır. Tehlikeli izinler ise, kullanıcının özel bilgilerine erişebilecek veya değiştirebilecek ya da diğer uygulamaların çalışmasını etkileyebilecek riskli alanları kapsamaktadır. Örneğin; saat dilimini ayarlama izni, normal bir izinken kullanıcı kişilerini okumak, tehlikeli bir izindir [17]. Tablo I'de tehlikeli izinler ve izin grupları ile bu izinlere ait açıklamalar verilmiştir.

TABLO I. TEHLİKELİ İZİNLER VE İZİN GRUPLARI [17]

İzin Grubu	İzin Adı	İzin Açıklaması
Takvim	READ_CALENDAR	Takvimde bulunan etkinlikleri okuma
	WRITE_CALENDAR	Takvimde bulunan etkinlikleri düzenleme
Kamera	CAMERA	Kamera erişimi, fotoğraf çekme ya da video kaydı
Rehber	READ_CONTACTS	Kişilere erişim
	WRITE_CONTACTS	Kişileri düzenleme
	GET_ACCOUNTS	Hesap listesine erişim
Konum bilgisi	ACCESS_FINE_LOCATION	Konum bilgisine GPS ile tam erişim
	ACCESS_COARSE_LOCATION	Konum bilgisine wifi ve hücresel veri ile yaklaşık erişim
Mikrofon	RECORD_AUDIO	Ses kaydı
Telefon	READ_PHONE_STATE	Yapılan arama durumlarını görme
	CALL_PHONE	Arama yapma
	READ_CALL_LOG	Arama listesini görme
	WRITE_CALL_LOG	Arama listesini düzenleme
	ADD_VOICEMAIL	Sesli mesaj ekleme
	USE_SIP	VoIP kullanma
	PROCESS_OUTGOING_CALLS	Giden arama izinlerini düzenleme
Sensörler	BODY_SENSORS	Sağlık verilerine erişim
SMS	SEND_SMS	SMS gönderme
	RECEIVE_SMS	SMS alma
	READ_SMS	SMS okuma
	RECEIVER_WAP_PUSH	WAP Push mesajlarını alma
	RECEIVE_MMS	MMS mesajlarını alma
Depolama	READ_EXTERNAL_STORAGE	Harici depolama birimlerini okuma
	WRITE_EXTERNAL_STORAGE	Harici depolama birimlerini düzenleme

III. UYGULAMALARıN İZİNLERİNİN ANALİZİ

Çalışmanın bu bölümünde, oluşturulan veri seti ile uygulama izinlerinin analizi gerçekleştirilmiştir. Veri seti oluşturulurken 50 iyicil uygulama, Google Play Store [18] içerisindeki ücretsiz uygulamalar arasından seçilmiştir. 50 kötücül uygulama ise, en fazla kötücül uygulama bulunduran veri setlerinden birisi olan Drebin [19] veri setinden elde edilmiştir. Çalışmanın akış diyagramı Şekil 1'de gösterilmiştir.

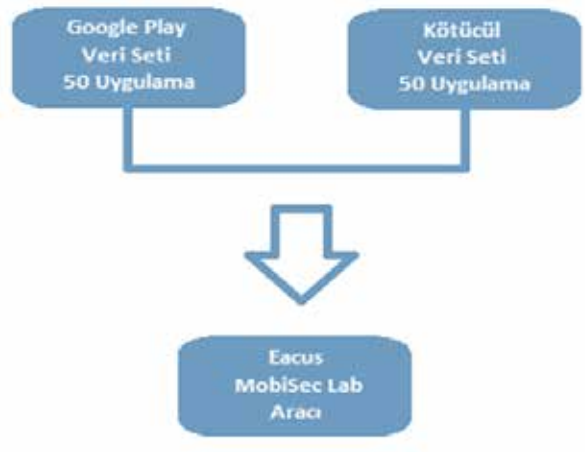


Şekil 1. Akış Diyagramı

Şekil 1'de görüldüğü gibi bu 100 uygulama öncelikle Eacus - MobiSec Lab [20] aracı yardımıyla analiz edilmiştir. Bu araç uygulamaları yüksek, orta ve düşük risk seviyeli izinler bulundurma durumları ve riskli izin tespit edilememe durumu üzerinden değerlendirmektedir. Eacus - MobiSec Lab aracı Android uygulama izinlerini yüksek, orta ve düşük risk seviyeli izinler olarak sınıflandırarak, analiz yapmaktadır. İyicil ve kötücül uygulama izinlerinin risk seviyelerinin karşılaştırılması amacı ile bu araç kullanılmıştır. Ardından VirusTotal [21] aracı ile kötücül yazılım tespit oranları bulunmuştur. VirusTotal çeşitli antivirüs yazılımları kullanarak kötücül yazılım tespitine yardım etmektedir. Bu aracın sonuçlarına göre kötücül olduğu değerlendirilen uygulamalar AppCritique [22] aracı ile detaylı olarak incelenmiştir. AppCritique, uygulamaların istenilen ve kullanılan izinlerinin analiz edilmesini sağlamaktadır. Bu sayede kötücül uygulamaların istedikleri izinler ile kullandıkları izinler arasındaki uyumsuzluk görülmüştür.

A.Uygulamaların Risk Seviyeleri Analizi

Uygulama izinlerinin risk seviyeleri Eacus - MobiSec Lab aracı yardımıyla analiz edilmiştir. Eacus – MobiSec Lab aracı ile 50 kötücül ve 50 Google Play uygulaması kullanılarak gerçekleştirilen analiz Şekil 2'de gösterilmiştir.



Şekil 2. Uygulamaların Risk Seviyesi Analizi

Şekil 2'de gösterilen analizin sonuçları Tablo II'de verilmiştir. 50 Google Play uygulamasının analiz sonuçlarına göre bu uygulamalardan 2 tanesinde yüksek riskli, 7 tanesinde orta riskli, 23 tanesinde düşük riskli izinler bulunduğu tespit edilmiştir. 18 uygulamada ise riskli izin tespit edilememiştir. Yüksek riskli izin bulunduran 2 uygulamanın her 2'sinin de, SMS okuma izni bulunduran bankacılık uygulaması olduğu görülmüştür. 50 kötücül uygulamanın analiz sonuçlarında ise kötücül uygulamalardan 17 tanesinde yüksek riskli, 16 tanesinde orta riskli, 7 tanesinde düşük riskli izinler bulunduğu görülmüş ve kalan 10 uygulamada riskli izin tespit edilememiştir.

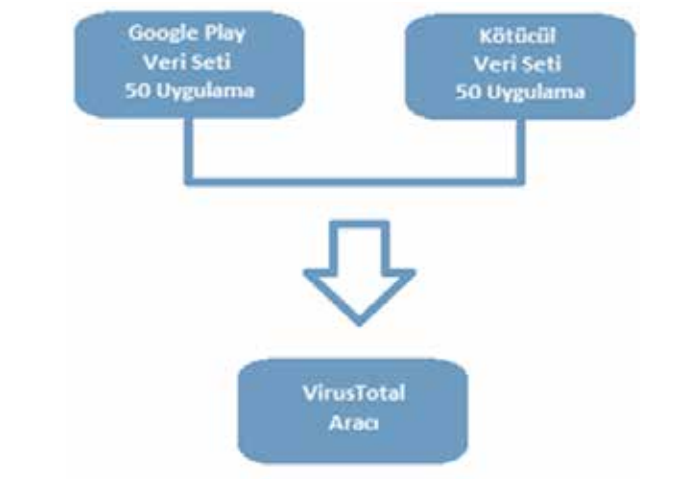
TABLO II. UYGULAMALARıN RİSK SEVİYELERİ

Uygulamalar	Yüksek	Orta	Düşük	Risk Yok	Toplam
Google Play	2	7	23	18	50
Kötücül	17	16	7	10	50
Toplam	19	23	30	28	100

Tablo II'de görüldüğü gibi toplam durumda 100 uygulamanın 19 tanesinde yüksek riskli, 23 tanesinde orta riskli, 30 tanesinde düşük riskli izinler tespit edilmiş ve kalan 28 uygulamada ise riskli izin tespit edilememiştir.

B.Uygulamaların Kötücül Yazılım Tespit Oranı Analizi

Kötücül yazılım tespit oranı (KYTO), bir uygulamada kötücül yazılım tespit eden antivirüs yazılımlarının sayısının, o uygulamayı analiz eden tüm antivirüs yazılımlarının sayısına oranıdır. Veri setinde bulunan uygulamalarda KYTO bulunurken VirusTotal aracından yararlanılmıştır. VirusTotal, çeşitli antivirüs yazılımları ile şüpheli dosyaları, URL'leri analiz etmekte ve çeşitli kötücül yazılımların tespitini sağlamaktadır. VirusTotal yaklaşık olarak 60 farklı antivirüs yazılımından gelen bilgileri birleştirmektedir. Şekil 3'te görüldüğü gibi 50 kötücül ve 50 Google Play uygulaması ile yapılan analizlerde uygulamalar için KYTO elde edilmiştir.



Şekil 3. Uygulamaların Kötücül Yazılım Tespit Oranı (KYTO) Analizi

VirusTotal ile yaklaşık 60 antivirüs yazılımı kullanılarak yapılan analizlerde 50 Google Play uygulamasından 41 tanesinde, KYTO 0'iken (0/59, 0/60, 0/61 gibi); en yüksek KYTO 10/59 olmuştur. 50 kötücül uygulamada en yüksek KYTO 47/60 olurken, en düşük KYTO 32/58'de kalmıştır. KYTO'nun paydasındaki değişimin nedeni, bazı antivirüs yazılımlarının bazı uygulamaları analiz edememesidir.

Bir önceki aşamada Eacus - MobiSec Lab aracı ile yapılan analizlerde kötücül verisetine dâhil olup risk bulunamayan uygulamalarda, VirusTotal ile yapılan analizlerde KYTO'nun yüksek değerlere sahip olduğu görülmüştür. Önceki aşamada risk bulunamayan uygulamalardaki en düşük KYTO 36/61 iken en yüksek KYTO 46/59 olmuştur. Bu durum önceki aşamada gerçekleştirilen analizlerin kötücül yazılımların tespitinde tam olarak yeterli olmadığını göstermektedir.

C.Kötücül Uygulamaların Detaylı Analizi

Eacus - MobiSec Lab aracı, Google Play uygulamalarında ve kötücül uygulamalarda bulunan riskli izinlerin risk seviyelerini göstermiştir. Google Play uygulamalarının bazılarının da, kötücül uygulamaların birçoğunda olduğu gibi yüksek ve orta risk seviyeli izinler bulundurduğu anlaşılmıştır. Ancak kötücül uygulamalar ile Google Play uygulamalarının ayırımı bu araç ile sağlanamamıştır. VirusTotal aracı yardımıyla analiz gerçekleştirildiğinde, KYTO'ya bakılarak, kötücül uygulamalar ve Google Play uygulamaları çok açık bir şekilde ayırt edilmiştir. Kötücül uygulamalarda KYTO'nun çok yüksek olduğu, Google Play uygulamalarında ise KYTO'nun çoğunlukla 0 olduğu görülmüştür. Bu aşamada, Şekil 4'te gösterildiği gibi kötücül uygulamaların izinleri, AppCritique aracı ile detaylı olarak incelenmiştir. AppCritique aracı ile istenilen ve kullanılan izinler araştırılmıştır.

Şekil 4. Kötücül Uygulamaların Detaylı Analizi

Şekil 4'te gösterilen analiz sonuçlarına göre 50 kötücül uygulama tarafından yaklaşık 75 farklı izin, 570 defa istenilmiştir. Kötücül uygulamalarda en çok istenilen 10 izin ile bu izinlere ait frekanslar Tablo III'te gösterilmiştir.

TABLO III. KÖTÜCÜL UYGULAMALARDA EN ÇOK İSTENİLEN 10 İZİN

İstenilen İzinler		
İzin Adı	***Koruma Seviyesi***	***Frekans***
INTERNET	Normal	%94
READ_PHONE_STATE	Tehlikeli	%90
ACCESS_NETWORK_STATE	Normal	%72
WRITE_EXTERNAL_STORAGE	Tehlikeli	%62
SEND_SMS	Tehlikeli	%60
RECEIVE_BOOT_COMPLETED	Normal	%52
ACCESS_WIFI_STATE	Normal	%50
RECEIVE_SMS	Tehlikeli	%42
WAKE_LOCK	Normal	%38
ACCESS_FINE_LOCATION	Tehlikeli	%30

Tablo III incelendiğinde, kötücül uygulamaların en çok istediği izinlerin INTERNET, READ PHONE STATE ve ACCESS NETWORK STATE izinleri olduğu anlaşılmaktadır. 50 kötücül uygulamanın 47 tanesi INTERNET, 45 tanesi READ PHONE STATE, 36 tanesi ACCESS NETWORK STATE izinlerini istemiştir. Kötücül uygulamalar tehlikeli izinlerden ise en çok READ PHONE STATE, WRITE EXTERNAL STORAGE ve SEND SMS izinlerini istemiştir. Kötücül uygulamaların istedikleri izinler içerisinde en çok kullandıkları 10 izin ve bu izinlere ait frekanslar Tablo IV'te gösterilmiştir.

TABLO IV. KÖTÜCÜL UYGULAMALARDA EN ÇOK KULLANILAN 10 İZİN

Kullanılan İzinler		
İzin Adı	***Koruma Seviyesi***	***Frekans***
INTERNET	Normal	%48
SEND_SMS	Tehlikeli	%36
ACCESS_FINE_LOCATION	Tehlikeli	%26
ACCESS_COARSE_LOCATION	Tehlikeli	%22
WAKE_LOCK	Normal	%16
CHANGE_WIFI_STATE	Normal	%8
RESTART_PACKAGES	Normal	%8
WRITE_SMS	Normal	%8
READ_PHONE_STATE	Tehlikeli	%6
VIBRATE	Normal	%6

Tablo IV'e göre INTERNET, SEND SMS ve ACCESS FINE LOCATION en çok kullanılan izinlerdir. Tehlikeli izinlerden en çok kullanılan izinler ise SEND SMS, ACCESS FINE LOCATION, ACCESS COARSE LOCATION izinleridir. Tablo III ve Tablo IV beraber incelendiğinde istenilen izinlerin frekans değerlerinin, kullanılan izinlerin frekans değerlerinden çok fazla olduğu, yani kötücül uygulamaların kullanmadıkları izinleri istedikleri görülmüştür.

IV. SONUÇ

Bu çalışmada Android 6.0'dan önceki sürümler için uygulanabilecek, uygulama izinlerinin analizine dayanan Android kötücül yazılım tespit yöntemi sunulmuştur. İyicil olduğu düşünülen çoğunluğu popüler 50 Google Play uygulaması ve Drebin veri setinden elde edilen 50 kötücül uygulama üç farklı araç ile analiz edilmiştir. İlk olarak Eacus - MobiSec Lab aracı ile gerçekleştirilen analizlerde, Android platformu tarafından belirlenen izinlerin, risk seviyelerine ayrıldığı anlaşılmıştır. Yüksek ve orta risk seviyesine sahip izinlerin kötücül uygulamaların büyük bir kısmında, Google Play uygulamalarının ise bazılarında (bankacılık uygulamaları gibi) bulunduğu tespit edilmiştir. Ardından VirusTotal aracı ile uygulamalara ait KYTO bulunduğunda, kötücül uygulamalarda KYTO'nun çok yüksek değerlerde olduğu görülmüştür. Google Play uygulamalarında KYTO'nun ya sıfır ya da çok düşük değerlerde olduğu belirlenmiştir. Son olarak AppCritique aracı ile kötücül uygulamaların istenilen ve kullanılan izinlerine bakılmış, kötücül uygulamaların istedikleri izinlerin birçoğunu kullanmadıkları anlaşılmıştır. Bu yüzden, mobil cihaza indirilecek bir uygulamanın kullanmayacağı izin için onay istenilmesi durumunda o uygulamaya şüphe ile yaklaşılması gerekmektedir.

Çalışmada veri setindeki Google Play uygulamaların istenilen izinleri, kullanıp kullanmama durumunun araştırılamaması bir eksiklik olmuştur. Android 6.0 ve sonraki sürümlerde kullanıcı kontrolünde olan izin sisteminin kullanılması, kötücül yazılım tespitinde, geleceğe dönük kod analizine dayalı sistemler geliştirmeyi gerektirmektedir.

KAYNAKLAR

[1] W Wang, Y. Li, X. Wang, J. Liu, and X. Zhang, "Detecting android malicious apps and categorizing benign apps with ensemble of classifiers," Future Generation Computer Systems, 2017.

[2] A. Boxall "The number of smartphone users in the world is expected to reach a giant 6.1 billion by 2020," https://www.digitaltrends.com/mobile/smartphone-users-number-6-1-billion-by-2020/, (Erişim Tarihi: 13.06.2017).

[3] Cisco, "Cisco Visual Networking Index: Global mobile data traffic forecast update, 2016–2021 white paper," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, (Erişim Tarihi:13.06.2017).

[4] J. Song, C. Han, K. Wang, J. Zhao, R. Ranjan, and L. Wang, "An integrated static detection and analysis framework for android," Pervasive and Mobile Computing, 2016.

[5] A Feizollah, N. B. Anuar, R. Salleh, G. Suarez-Tangil, and S. Furnell, "AndroDialysis: analysis of Android intent effectiveness in malware detection," Computers & Security, 2017.

[6] S. Wu, P. Wang, X. Li, and Y. Zhang, "Effective detection of Android malware based on the usage of data flow APIs and machine learning," Information and Software Technology, 2016.

[7] J. Walls, and K.K.R. Choo, "A review of free cloud-based anti-malware apps for Android," In Trustcom/BigDataSE/ISPA, IEEE, August 2015.

[8] Gartner, "Gartner says worldwide sales of smartphones grew 7 percent in the fourth quarter of 2016," http://www.gartner.com/newsroom/id/3609817, (Erişim Tarihi:13.06.2017).

[9] Gdata, "G data: mobile malware report," https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_EN.pdf, (Erişim Tarihi:13.06.2017).

[10] Kaspersky, "Kaspersky security bulletin 2013," http://media.kaspersky.com/pdf/KSB_2013_EN.pdf, (Erişim Tarihi:13.06.2017).

[11] R. S. Arslan, İ. A. Doğru, ve N. Barışçı, "Android mobil uygulamalar için izin karşılaştırma tabanlı kötücül yazılım tespiti," Politeknik Dergisi, 2017.

[12] Google Play Yardım, " Android 5.9'a kadar olan sürümlerde uygulama izinlerini inceleme," https://support.google.com/googleplay/answer/6014972?hl=tr&ref_topic=6046245, (Erişim Tarihi:12.07.2017).

[13] Google Play Yardım, "Android 6.0 ve sonraki sürümlerde uygulamanızın izinlerini kontrol etme," https://support.google.com/googleplay/answer/6270602?hl=tr&ref_topic=6046245, (Erişim Tarihi:12.07.2017).

[14] Android, "Introducing Google Play Protect," https://www.android.com/play-protect/?utm_source=social&utm_medium=blog, (Erişim Tarihi:12.07.2017).

[15] Google Play Yardım, "Zararlı uygulamalara karşı korunmaya yardımcı olma," https://support.google.com/googleplay/answer/2812853?hl=tr, (Erişim Tarihi:12.07.2017).

[16] A. T. Kabakuş, İ. A. Doğru, ve A. Çetin, "Android kötücül yazılım tespit ve koruma sistemleri," Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 2015.

[17] Android developers, "Requesting Permissions," https://developer.android.com/guide/topics/permissions/requesting.html,

(Erişim Tarihi:13.06.2017).

[18] Google Play Store, https://play.google.com/store/apps, (Erişim Tarihi:13.07.2017).

[19] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon and K. Rieck, "Drebin: effective and explainable detection of Android malware in your pocket," In NDSS, February 2014.

[20] Eacus-MobiSec Lab aracı, http://www.mobiseclab.org/eacus.jsp, (Erişim Tarihi:30.06.2017).

[21] VirusTotal aracı, https://www.virustotal.com/, (Erişim Tarihi:01.07.2017).

[22] AppCritique aracı, https://appcritique.boozallen.com/, (Erişim Tarihi: 12.07.2017).

SCADA Sistemlerindeki Güvenlik Açıkları ve Tehditleri

Security Vulnerabilities and Threats in SCADA Systems

Burçin YÖNEL
HAVELSAN A.Ş.
Ankara, Türkiye
burcinyonel13@gmail.com

İzzet Gökhan Özbilgin
HAVELSAN A.Ş.
Ankara, Türkiye
gozbilgin@havelsan.com.tr

Özet

Bir SCADA (Denetleyici Kontrol ve Veri Toplama) sistemi, içinde bulunduğu karmaşık altyapıyı dağıtılmış teknolojilerin kullanımı yoluyla izler ve yönetirken, tek başına kritik bir altyapı haline gelir. Bileşenlerinin herhangi birinde bir aksaklık veya bozulma, diğer altyapıların performansı üzerinde ciddi etkiler yaratabilir. Diğer sistemlerle olan bağlantı SCADA sistemini saldırılara karşı daha savunmasız hale getirir ve yeni güvenlik problemleri oluşturur. Bu yüzden, güncellenmiş bir bilgiyi muhafaza etmek ve anormal olayları hafifletmek veya önlemek için öneriler ve / veya çözümler sunmak için çeşitli güvenlik analizi yapmak çok önemlidir. Bunlar, uygun, güvenilir ve kullanılabilir bir kontrol ağının varlığını kolaylaştıracaktır. Makale, SCADA sistemlerinin güvenlik açıklarına genel bir bakış sunmaktadır. SCADA ağı güvenlik açıklarını siber güvenlik açısından analiz ederek en yaygın saldırılar ve bu saldırılara karşı yapılabilecek önlemlerden, standartlardan ve yapılan risk analizlerinden bahsedilmektedir.

Anahtar Kelimeler: SCADA, Siber Güvenlik, Kritik altyapı, Siber tehdit

Abstract

A SCADA (Supervisory Control and Data Acquisition) system becomes a critical infrastructure by itself, using and monitoring other complex infrastructure distributed technologies. A failure or deterioration in any of its components can have a serious effect on the performance of other infrastructures. The SCADA connection with other systems makes the SCADA system more vulnerable to attack and creates new security problems. As a result, it is very important to carry out various security analyzes in order to maintain updated information and to provide suggestions and / or resolutions to mitigate or prevent abnormal events. This will facilitate the availability of a suitable, reliable and usable control network. The article provides an overview of the security vulnerabilities of SCADA systems. By analyzing SCADA network security vulnerabilities in terms of cyber security, the most common attacks and the measures that can be taken against this attack, standards and risk analysis are mentioned.

Keywords: *SCADA, Cyber security, Critical Infrastructure, Cyber threat*

Giriş

Bir ülkede ekonomik ve sosyal hayatın aksamadan işlemesi için ciddi öneme sahip olan fiziksel ve sayısal sistemler yani kritik altyapılar, ülke ekonomisi için kritik faaliyetleri barındıran, her seviyede yüksek maliyetli kamu yatırımına ihtiyaç duyan tesislerdir. Modern toplum yaşamının can damarını oluşturan bu altyapıların korunması ve güvenilirliklerinin sağlanması ulusal güvenlik ve ekonomik sürdürülebilirlik için büyük önem arz etmektedir.

Günümüz ağ sistemleri, operatörlere veya yetkililere sistemleri uzaktan kumanda etme olanağı sağlamaktadır. Endüstriyel komuta ve kontrol sistemlerinin gelişmiş hali olan SCADA sistemleri, ağlara ve internete kolayca bağlanabilmektedir. Bu bağlanma özelliği, sistemlerin kullanımını ve kontrolünü kolaylaştırmış olsa da ciddi boyutta güvenlik risklerini de beraberinde getirmiştir. Eğer sistemler internet vasıtasıyla uzaktan kumanda ediliyorsa SCADA sistemlerine yapılabilecek bir saldırı tüm sistemi etkileyebilecektir. Bu yüzden bu sistemlerin güvenliği çok önem teşkil etmektedir.

Bu makalede ilk olarak SCADA sistemlerinin yapısı, işlevleri, katmanları anlatılmaktadır. Daha sonra bu sistemlerin risk analiz şeklinden bahsedilerek sistemi tehdit eden unsurlar ve güvenlik açıkları ele alınacaktır. Bu doğrultuda oluşan açıklar ve tehditlere çözüm olacak protokoller, standartlar ve tedbirlerin bir araya getirilmesi amaçlanmıştır.

I. SCADA SİSTEMİNİN TEMEL YAPıSı VE BİLEŞENLERİ

Sürekli ve gerçek zamanlı olarak İşlem, Programlanabilir Lojik Kontrolörler (PLC), Döngü Kontrolörleri, Dağıtık Kontrol Sistemleri (DCS), I/O Sistemleri gibi çeşitli cihazlardan veriler toplanır. SCADA, bu verileri tanımlanmış kriterlere göre değerlendiren, gerektiğinde kullanıcıya erken uyarı mesajları üreten, üretimi etkileyen çeşitli faktörlerin grafiksel olarak izlenmesini veya eğri olarak gözetlenmesini sağlayan, ayrıca sahadaki kontrol noktalarının uzaktan denetlenebilmelerine imkân sağlamak amacıyla kullanılan sistemler olarak tanımlanabilir[1].

Elektrik üretim ve dağıtım tesisleri, doğalgaz ve petrol boru hatları, su toplama ve dağıtım tesisleri, otomotiv endüstrisi, bina otomasyonu, hava kirliliği kontrolü gibi kritik alanlarda kullanımı olan SCADA sistemleri genel olarak Şekil 1'de belirtilen ve aşağıda kısaca açıklanan bileşenlerden oluşmaktadır[1]:

1) Yerel sensörler ve aktüatörler ile arayüz sağlayan Uzak Terminal Birimleri (RTU'lar) ve PLC'ler gibi veri alanı aygıtları,

2) SCADA ana ve saha aygıtları (köleler) arasındaki iletişim ağı,

3) Kontrol merkezinde bulunan SCADA ana istasyonu,

4) İnsan Makine Arayüzü (HMI) cihazları. SCADA sistemi, uzak istasyonları okuyan ve bir veri tabanında veri toplayan HMI yazılımını içeren endüstriyel bir PC veya iş istasyonundadır.

Şekil 1: SCADA Sistemlerinin Bileşenleri[2]

Veri toplama ilk önce RTU'lar ve uzaktan algılayıcılar ile kontrol merkezi arasında bulunan PLC'ler tarafından başlatılır. RTU'lara ve PLC'lere bağlı girdiyi okuduktan sonra, işlenmeleri için verileri iş istasyonuna iletirler. SCADA donanımında; ana sunucu ile istemci arasındaki iletişim hatları ve RTU arasındaki iletişim hatları ve saha donanımından oluşur[3].

•***Ana Sunucu – Ana Terminal(MTU):*** Ana terminal, SCADA sisteminin ana kontrolör görevindeki bilgisayarlardır. Bilgisayar tabanlı ağ yapısı üzerinde server-client bilgisayarlar, yazıcı ve diğer bileşenlerden oluşur.

•***Uzak Terminal Birimleri(RTU):*** Sistem değişkenlerini toplayan, depolayan ve bu bilgileri kontrol merkezine, belirli bir iletişim yolu ile gönderen yapıdır.

•***İletişim Hatları:*** MTU ile RTU cihazları arasında bilgi alışverişi yapan ağ yapılarıdır.

•***Saha Donanımı:*** Saha ekipmanları PLC, DCS ve Akıllı elektronik kartlar olarak tanımlanır.

II. SCADA SİSTEM KATMANLARı

SCADA sistemi şu katmanlardan oluşur[4];

• ***İşletme kontrol katmanı:*** Fiziksel kontrollerin yapıldığı katmandır. Mekanik ve elektromekanik aygıtlar uzak terminal birimlerine bağlanarak işletme fonksiyonlarını yerine getirir.

• ***Süreç denetim katmanı:*** İzleme ve veri toplama fonksiyonları ile tesisler ve makineler arası eş zamanlılığı sağlar. Bu katman merkezi kontrol odası ve SCADA yazılımını kapsar.

• ***İşletme yönetim katmanı:*** Bir üst katmanda alınmış stratejilere uygun olarak işletme kararları alarak bölümler arası işbirliği sağlar. İşletme Müdürlüğü görevini üstlenir.

• ***Kaynak yönetim katmanı:*** İşletmenin üretimi için gerekli kaynakların planlandığı, üretim ve hizmet stratejilerinin belirlendiği katmandır.

III. SCADA SİSTEMLERİNİN İŞLEVLERİ

SCADA sistemleri genellikle aşağıdaki özelliklere sahiptirler[4]:

- Çoklu Kullanıcılık
- Grafik ara yüzü
- İşlemlerin taklit edilmesi (benzetim)
- Gerçek zamanlı ve geçmişe yönelik izleme
- Alarm sistemi
- Veri toplama ve kayıt
- Veri analizi
- Rapor hazırlama

SCADA sistemleri kullanarak uygulama yazılımı geliştirmek için iletişim protokolleri ve veri tabanı yapısının tanımlanması gerekmektedir. İletişim protokolleri SCADA'nın işletmede birbirleri ile iletişim kurması gereken birimlerin haberleşmesini sağlamaktadır. SCADA sisteminin gözlem ve denetim fonksiyonlarını üstlenmesi için sürece ait giriş ve çıkış bilgileri bir veri tabanında tanımlanır. Veri tabanında süreç değişkenlerine tekabül eden her bir bilgi etiket, kapı veya nokta olarak tanımlanır. Bu süreç değişkenlerinin bulunması gereken seviyelerle ilgili alarmlar ve bu değişkenlerin işlenmesi gerektiğinde kullanılacak işlem blokları veri tabanı tanımlanması fazında gerçekleştirilir.

IV. SCADA SİSTEM TEHDİTLERİ VE GÜVENLİK AÇıKLARı

SCADA sistemlerinde karşılaşılabilecek güvenlik açıkları ve bunlara ilişkin tehditleri aşağıdaki şekilde sıralanabilir:

İzleme eksikliği: Aktif ağ denetimi olmadan, şüpheli etkinliği tespit etmek, potansiyel tehditleri tespit etmek ve siber saldırılara hızlı tepki vermek mümkün değildir[5].

Geciken güncellemeler: SCADA sistemleri daha ileri seviyeye geldikçe yeni saldırılara karşı daha savunmasız duruma düşerler. Ürün yazılımı ve yazılım güncellemelerinin bakımı uygunsuz olabilir ancak bunlar maksimum koruma için gereklidir[5].

Cihazlar hakkında bilgi eksikliği: Cihazları bir SCADA Sistemine bağlamak, uzaktan izleme ve güncelleme yapılmasına izin verir, ancak tüm cihazların raporlama kapasitesi eşit değildir. Çoğu SCADA sistemi zamana bağlı olarak aşamalı olarak geliştirildiğinden, 5 yaşında ve 20 yaşında olan teknoloji ile eşleştirilmiş olan teknolojiyi görmek nadirdir. Bu da, ağa bağlı cihazlar hakkındaki bilginin eksik olduğunu genellikle gösterir[5].

Trafiğin türü hakkında bilgi eksikliği: Yöneticiler ağlarının

içinden geçen trafik türünün ne olduğunu bilmeliler. Ancak o zaman potansiyel tehditlere nasıl cevap vereceği konusunda bilinçli kararlar verebilirler. İleri veri analizi ile yöneticiler trafik denetiminden toplanan verilerin büyük bir resim görüntüsünü alabilir ve bunları harekete geçirici istihbaratta tercüme edebilirler[5].

Kimlik doğrulama delikleri: Kimlik doğrulama çözümleri, yanlış kişilerin SCADA sistemine erişmesini önlemek için tasarlanmıştır. Bununla birlikte, kötü şifreler, kullanıcı adı paylaşımı ve zayıf kimlik doğrulama gibi yaygın güvensiz uygulamalar nedeniyle bu kolaylıkla yenilebilir[5].

Fiziki güvenliğin eksikliği: İnsanların farkında olmadan bir ofise girip bir bilgisayar monitöründe oturup sisteme erişebildikleri zaman sıklıkla görülür. Bazı şirketler kilitli kapılarla iyi derecede güvenliğe sahip olsa da veya programlara erişimi kısıtlı olsa da, personel, bilgisayar korsanlarının bir şirketin sistemlerine uzaktan erişimine izin veren çalınan dizüstü bilgisayarlar, tabletler ve mobil cihazların yanı sıra, kapıları kilitsiz kılar ve kolayca erişilebilir halde bulunurlar[6].

Erişime açık: LAN ağında birden fazla erişim noktasıdır. Sahadaki hemen hemen her debimetre ve işlemci, COM, USB veya seri portlar için açık protokollere sahiptir ve bu protokol ağa erişim sağlar[6].

Güvenlik: Genellikle firewall tek güvenlik basamağıdır. Birçok şirket, ağ operasyonlarında veya veri merkezlerinde, gelen veri paketlerini taramak için temelde bir çevre savunması olarak işlev gören tek kaynaklı bir firewalla sahiptir. Bununla birlikte, büyük bir veri hacmi girdiğinde, firewall (yalnızca bir filtredir ve geçilemez bir duvar değildir) çok fazla hacim veya çok fazla karmaşıklık veya karmaşıklıkla boğulabilir. Diğer güvenlik sorunu, yerel alan ağı (LAN) üzerinde hiçbir güvenceye sahip olmamasıdır. Bireysel sensörlerle iletişim kurmak için, ofislerdeki gibi, alanda kablosuz bir ağ sıklıkla kullanılır. Ayrıca, bazı ağların herkesin bu LAN'a erişmesine izin veren açık protokolleri vardır. Her ikisi de hiçbir güvenlik, hiçbir virüs tarama ve hiçbir çevre savunma sahip değildir[6].

V. TEHDIT VE SALDıRı ÇEŞITLERI

SCADA sistemlerine yönelik tehditler; yetkilendirme ihlali, izinli-izinsiz erişim ihlalleri, bombalar (mantık veya süre, kontrollerin atlanması, tarama, gayri meşru kullanım, bilgi sızıntısı, veri değişikliği, değiştirme, durdurma, tekrarlama, sabotaj, casusluk, fiziksel Saldırı, tuzak kapısı / arka kapı, trojan atı, tünel açma, virüs, solucanlar) olarak ifade edilebilir.

SCADA sistemlerine olası saldırılar aşağıdaki kategorilere ayrılabilir[3]:

1) Kurumsal veya kontrol ağları üzerinden veri akışını geciktirme veya kesintiye uğratma (hizmet reddi);

Tanı Sunucusu Saldırıları UDP bağlantı noktası üzerinden: Rakipler, aynı hata ayıklama araçlarına erişebilirler. Herhangi bir RTOS geliştiricisi bunu yapabiliyor. Ayrıca, birçok saldırganın kod düzeyinde bilgiye ihtiyaç duymadığını göz önüne alarak, sembol tablolarını okuyabilir, montaj vb. yoluyla adım atabilirler.

Smurf; değiştirilmiş bir Internet Kontrol mesajı akışı göndererek bir adres sızdırma türüdür. Gönderen adresi olan hedef ağa iletişim kuralı (ICMP) paketleri, hedef bilgisayar adreslerinden biri ile aynıdır. SCADA sistemleri bağlamında, bir PLC değiştirilmiş mesaja tepki verirse, aktuatörlere çarpışır veya tehlikeli bir şekilde yanlış komutlar gönderebilir.

ARP: öncelikle IP adreslerini Ethernet Orta Erişim Kontrolü (MAC) adreslerine çevirmek ve LAN üzerindeki diğer bağlı arabirim aygıtını keşfetmek için kullanılır. ARP sızdırma saldırısı, önbelleğe alınmış adres çiftini değiştirmektir. SCADA sistemlerinde sahte MAC adresleri içeren sahte ARP mesajları göndererek, bir düşman şebeke anahtarları gibi ağ cihazlarını şaşırtabilir. Bu çerçeveler yanlışlıkla başka bir düğüme gönderildiğinde, DoS başlatılabilir.

2) PLC'lerde, RTU'larda veya SCADA kontrol cihazlarında programlanmış talimatların değiştirilmesi; Ortak protokollerdeki güvenlik açıklarını içerir. Protokol açıkları, kendilerini potansiyel bir patlatmaya neden olan protokol uygulamasının başarısız olmasına neden olabilecek bölümleme hatalarına, yığınlara, yığınlara veya arabellek taşmalarına vb. dönüştürebilirler. Özellikle Windows'ta TCP / IP protokollerinin uygulanmasını istifade eden çeşitli saldırılar vardır. Çevrimiçi olarak sürekli olarak kısıtlanmış mevcut yamalar olsa da, bu makinelerin güncel tarihsel yamaları bulunmaması muhtemeldir.

3) Sistem işlemlerini kontrol etmek için yanlış bilgi gönderme; İletişim kaçırma ve Man-in-the-middle (MittM) saldırılardır. En tehlikeli saldırılardan biri MittM saldırısıdır ve saldırgana kontrol sistemi üzerinde mutlak kontrol ve uzun süre izin verir. Saldırgan SCADA sistemlerine görünmez bir zararlı yazılım takabilir. Böylece saldırgan sistem ve kumanda yazılımını çalıştırabilir, ağ güvenlik duvarından çıkabilir ve platformuyla bağlantı kurabilir. MittM sistemi tahrip ettiği sırada, kullanıcılar her şeyin normal bir şekilde çalıştığını düşünüyor.

4) Kontrol sistemi yazılımını veya yapılandırma ayarlarını değiştirme; Kapı tokmağının sallanma saldırısıdır (the doorknob-rattling attack). Düşman birkaç bilgisayarda çok az kullanıcı adı ve şifre kombinasyonu gerçekleştirir. Bu, çok az başarısız oturum açma girişimi ile sonuçlanır. Bu saldırı, tüm ana bilgisayarlardan giriş hatalarına ilişkin veriler toplandığı halde herhangi bir uzak varış noktasından kapı tokmağının sızmasını kontrol etmek için bir araya getirilmediği sürece algılanamayabilir.

5) Zararlı yazılımları sisteme tanıtmak: Veri tabanı saldırılarından Yapılandırılmış Sorgu Dili (SQL) Enjeksiyonunu buna

örnektir. Bu saldırı, bir düşman, kullanıcı tarafından sağlanan girdiyi uygun şekilde engellemede başarısız olan bir Web uygulamasına veri girdisini işleyebilmekte ve bir sorguya, bir dizi beklenmedik SQL ifadesi ekleyebildiğinde ortaya çıkar. Üstelik bir 'komut kabuğu' saklanma yordamı etkinleştirilirse, saldırgan bir an önce komuta düzeyine geçebilir. İşlem, komutu yürüten bileşenle aynı izinlerle çalışacaktır. Bu saldırının etkisi, saldırganların veri tabanında tam kontrol sahibi olmalarını veya sistemdeki komutları yürütmelerini sağlayabilir.

Bu saldırıların amaçları; SCADA ana kontrol istasyonuna erişip, bozma, RTU ya da PLC ye erişip bozma, SCADA şifrelerine erişme, SCADA ana istasyonu – RTU arasındaki haberleşmeyi kesme, RTU kontrol programını değiştirme olarak sıralanabilir.

VI. STANDARTLAR VE PROTOKOLLER

SCADA sistemi fiziksel ve mantıksal olarak diğer ağlardan izole edildiği için güvenlik gereksinimleri; verimliliği arttırmak, bağlantı düzeyini arttırmak ve COTS (ticari raflarda) donanım ve yazılımdan yararlanmak için, çoğu büyük sanayi kontrol protokolleri artık SCADA mesajlarını TCP / IP kullanarak taşımak için standartlar içermektedir. Modbus-TCP ve DNP3-over LAN / WAN özellikleri, modern SCADA ağlarında TCP / IP'nin baskın taşıyıcı protokol haline geldiğinin açık bir göstergesidir. TCP / IP, daha önce izole edilmiş SCADA ağları ile kurumsal bilgi teknolojisi ve iletişim altyapıları arasındaki bağlantıları da kolaylaştırıyor. Bu eğilim ciddi güvenlik sorunlarını ortaya çıkarmaktadır. Çoğu SCADA protokolü herhangi bir güvenlik mekanizması olmadan tasarlanmıştır. Bu nedenle, TCP / IP taşıyıcısına yapılan bir saldırı, korunmasız SCADA protokolünü ciddi biçimde ortaya çıkarabilir. Ayrıca, birbirine bağlı bir şirket ağına yapılan saldırılar bir SCADA ağına tünelleşebilir ve endüstriyel süreci tahrip edebilir [7, 8].

ISA-SP99 Üretim ve Kontrol Sistemleri Güvenliği Komitesi Iki teknik rapor üretti [9,10] ve şu anda bir ANSI / ISA standardı geliştirmektedir. Amerikan Petrol Enstitüsü bir boru hattı çıkardı. SCADA güvenlik standardı API-1164 [11] ve Amerikan Gaz Kurumu SCADA'nın kriptografik iletişim koruması için AGA-12 [12, 13] standardını önerdi. Birleşik Krallığın Ulusal Altyapı Güvenlik Koordinasyon Merkezi (NISCC), SCADA sistemleri ve süreç kontrol ağları için güvenlik duvarı dağıtımıyla ilgili iyi bir uygulama kılavuzu yayınladı [14]. NIST, endüstriyel kontrol sistemleri için bir sistem koruma profili [15] ve kontrol sistemlerini güvence altına almak için bir kılavuz olan iki belge üretti [16].

A. ISA-SP99 Teknik Raporları

ISA-SP99 komitesi, kontrol sistemi güvenliği ile ilgili iki teknik rapor hazırladı. İlk rapor [9] imalat ve kontrol sistemleri için güvenlik teknolojilerine odaklanmaktadır. Elektronik güvenlik teknolojileri hakkında kapsamlı bir anket, kullanım kılavuzu ve güvenlik değerlendirmeleri ile tamamlanmaktadır. İkinci rapor [10] güvenlik bileşenlerinin imalat ve kontrol sistemi ortamlarında entegrasyonunu ele almaktadır. İlk raporda tanımlanan unsurlar, güvenlikleri, gereksinimleri, politikaları, prosedürleri ve en iyi uygulamaları içeren iyi tanımlanmış planları kullanarak endüstriyel çevrelere entegre etmek için kullanılır. Raporun temel amacı, kontrol sistemleri için etkili güvenlik uygulama kılavuzlarını sağlamaktır.

B. NIST Sistem Koruma Profili

2004 yılının Ekim ayında, NIST, endüstriyel sistemler için fonksiyonel ve güvenlik gerekliliklerinin resmi ifadelerinin geliştirilmesi için rehberlik sağlayan endüstriyel kontrol sistemleri için sistem koruma protokolünü (SPP) [15] kullanmıştır. NIST dokümanı, Ortak Kriterler tarafından tanımlanan koruma önlemlerini benimser. SpPcorepeci işlevsel gereklilikler (oturum denetimi, rol tabanlı erişim kontrolü, veri kimlik doğrulama, vb.) Ve güvence gereksinimleri (konfigürasyon yönetimi, teslimat ve işletme, hassasiyet değerlendirmesi, güvence bakımı, vb.). NIST SPP ayrıca çeşitli endüstriyel kontrol sistemleri sınıfları için odaklanmış koruma profilleri geliştirme yönergeleri sunmaktadır.

C. API-1164 Güvenlik Standardı

API-1164 SCADA Güvenlik Standardı Eylül 1998'de yayınlandı. Bu standart, sistem bütünlüğü ve güvenliği için yönergeler, operatör denetim listeleri ve bir güvenlik planı şablonu sunmaktadır. API-1164 standardı, operatöre SCADA güvenliğinde endüstri uygulamalarının bir açıklaması ve sağlam güvenlik uygulamalarının geliştirilmesi ve uygulanması için bir çerçeve sunmaktadır. API-1164 yönergeleri ayrıca, erişim kontrolü, iletişim, bilgi dağıtımı ve sınıflandırma, fiziksel güvenlik, veri akış, ağ tasarımı ve personel için bir yönetim sistemi ele alınmaktadır. API-1164 operatör kontrol listesi, SCADA sistemlerinin güvenlik durumunu değerlendirmek için kapsamlı bir önlem listesi. Her önlem gerekli, yerinde veya gerekmeyen olarak sınıflandırılır. Standart ayrıca, API-1164 en iyi uygulamalara uyan ve en düşük modifikasyonlar ile kullanılabilen bir güvenlik planı şablonu içerir.

D. AGA-12 Dokümanları

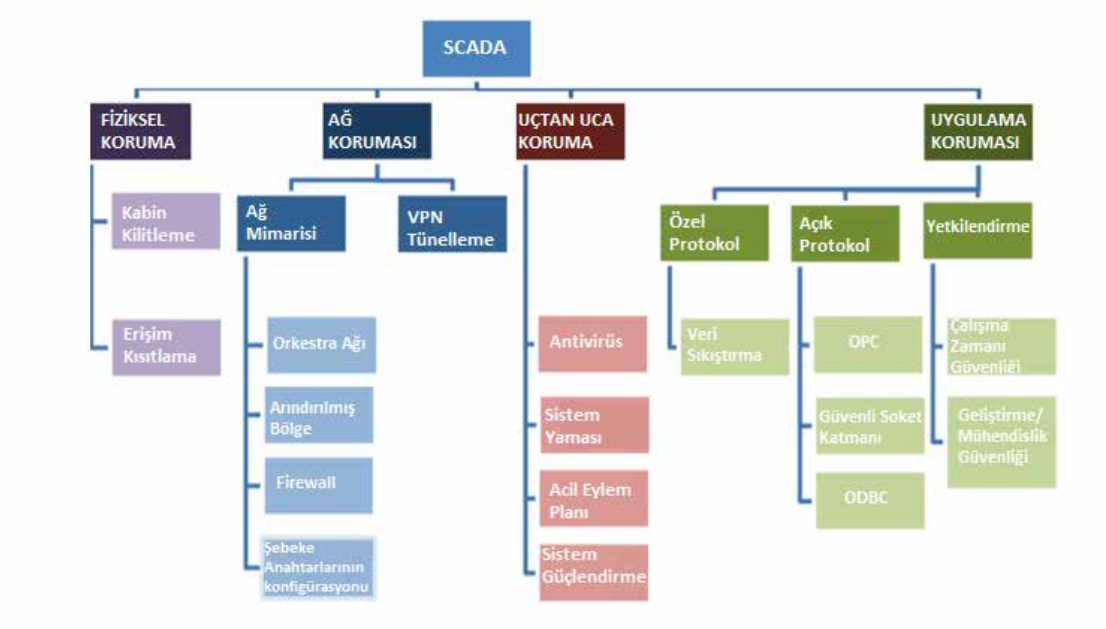
11 Eylül 2001'den üç hafta sonra Amerikan Gaz Kurumu, siber saldırılardan endüstriyel kontrol sistemlerinin güvenliğini sağlamak için protokoller ve mekanizmalar önermek üzere bir çalışma grubu oluşturdu. Çalışma grubu iki belge üretti. İlk doküman, AGA-12 Bölüm 1 [12], politikalara, değerlendirmeye ve denetlemelere yöneliktir. Ayrıca, güvenlik aygıtları için kriptografik sistem gereksinimlerini ve test planlamasını açıklar. AGA-12 Bölüm 1, güvenlik aygıtlarının NIST FIPS 140-2 (Kriptografik Modüller için Güvenlik Gereksinimleri) ile uyumlu olmasını gerektirir. AGA-12 Bölüm 2 [13] 'nin ikinci dokümanı, retro iletişim kurma seri iletişimlerini ve seri iletişim kanallarının kapsüllenmesi / şifrelenmesini tartışıyor. Belgede, simetrik anahtarlar kullanan kimlik doğrulama servislerine sahip bir oturum tabanlı protokol açıklanmaktadır (AES ve SHA1 sırasıyla doğruluğun ve bütünlüğün uygulanması için kullanılmaktadır). Basit tasarım, gecikme ve titreşimi minimum düzeyde etkiler ve tekrarlama saldırılarına karşı koruma sağlamak için sıra numaralarını kullanır. Ayrıca, diğer protokolleri, örn. Modbus ve DNP3'ü kapsüller ve nakledebilir. AGA hali hazırda ağa bağlı sistemlerin korunmasına ve SCADA bileşenlerine güvenlik gömülmesine değinecek olan AGA-12 dokümanlarının 3 ve 4üncü bölümlerini geliştirmektedir.

E. NISCC Güvenlik Duvarı Dağıtım Kılavuzu

SCADA ve Proses Kontrol Ağları için Güvenlik Duvarı Dağıtımı NISCC İyi Uygulama Kılavuzu [14] Şubat 2005'te İngiliz Ulusal Teknoloji Altyapısı Güvenlik Koordinasyon Merkezi için British Columbia Teknoloji Enstitüsü tarafından geliştirilmiştir. Endüstriyel ortamlarda yapılandırma ve konuşlandırma. Özellikle çift ağa bağlı bilgisayarlardan VLAN tabanlı ağ ayrımına kadar sekiz ayırma mimarisini açıklar ve değerlendirir. Her bir mimari yönetilebilirlik, ölçeklenebilirlik ve güvenlik temelinde değerlendirilir. NISCC kılavuzu, duvarlar ve diğer mimari bileşenlerin uygulanması, konfigürasyonu ve yönetimi de tartışılmaktadır. Endüstriyel ağlarda kullanılmak üzere gelecekteki teknolojilerin tartışılması, hizmet kalitesinin önemini ve cihazların endüstriyel protokollerin farkında olması gereğini vurguluyor.

F. NIST SP 800-82 Dokümanı

Eylül 2006'da, NIST, SCADA ve endüstriyel kontrol sistemleri güvenliği için bir kılavuzun ilk halk taslağını yayınladı (NIST SP 800-82 Belgesi [16]). NIST dokümanı, güvenlik unsurlarını kapsamlı bir şekilde ele alır. Özellikle, ortak sistem topolojileri, tehditler ve güvenlik açıklarını tartışır ve riskin azaltılmasında kullanılacak güvenlik önlemlerini önermektedir. Ayrıca, başlangıçta federal bilgi sistemleri bağlamında belirtilen endüstriyel kontrol ortamları için yönetim, operasyonel ve teknik güvenlik kontrollerini yeniden hedeflemektedir. Buna ek olarak, SP 800-82 dokümanı SCADA ve endüstriyel kontrol sistemleri için güvenlik açısından en iyi uygulamaların geliştirilmesine odaklanan diğer inisiyatifleri ve eforları tartışmaktadır.



Şekil 2: SCADA sistemi koruma alanları[17]

VII. TEDBIRLER

Protokoller, standartlar, bazı güvenlik ve fiziki önlemler ile SCADA sistemlerinin güvenliğinin sağlaması amaçlanmıştır. Yukarda anlatılan standartlar dışında alınan diğer önlemler şu şekildedir[1];

Güvenlik Politikaları: Güvenlik planı hazırlanmalıdır. Sistem eğitimli kontrol operatörleri ve mühendisleri tarafından kullanılmalıdır. Güvenlik politikalarının sürekliliği için BT grubu ve kontrol mühendisleri arasında güvenlik çözümlerinin yürütülmesi, uygulanması ve haberleşmenin sağlanması sağlanmalıdır.

Şebeke Mimarisi: Güvenliğin ön planda olduğu mimariler en iyi şekilde tasarlanmalı ve güvenlik duvarları ile ayrılmalıdır.

Sistemin Sağlamlaştırılması: Gereksiz uygulamalar ve hizmetler ile cihazlar süreç kontrol bilgisayarından uzaklaştırılmalı ve gereksiz portlar kapatılmalıdır.

Uzak Bağlantılar: Uzak bağlantılarda mümkün oluğunca kısa süreli şifreler kullanılmalıdır.

SCADA sistemlerinin korunmasını Fiziksel, ağ, uç nokta ve uygulama koruması olarak Şekil 2 de gösterildiği gibi 4 kısımda inceleyebiliriz.

Fiziksel Koruma: İlk savunma katmanı Fiziksel Koruma altındadır. Saldırı, sisteme güvenli olmayan fiziksel erişime sahip kötü niyetli kişilerce yapılabilir. Bunlar, virüsün sisteme USB ile iletilmesi, casusluk yöntemi ile bir anahtar kaydediciyi sisteme yüklemesi olabilir.

Ağ Koruması: Fabrika ve / veya süreç ağını, Sanal Yerel Alan Ağları (VLAN) gibi ayrı alanlara bölerek, bir siber saldırı durumunda güvenlik açığı riskini azaltır. SCADA ortamı, kullanıcıların yalnızca tahsis edilen ayrılmış alanlara erişebilmelerini sağlamalıdır. SCADA ile bu şekilde, düzenlenen ağ mimarisi, yalnızca güvenlik açısından konfigüre edilebilir nitelikte değil aynı zamanda yazılım açıdan zayıf noktaları da azaltıyor. Bu önlemlerin yanı sıra, güvenlik duvarları ve Demilitarized Zones (DMZ) gibi iyi geliştirilmiş Ağ Güvenlik Çözümleri uygulamaları bulunmaktadır. Farklı bir ağ seviyesine girerken, bir güvenlik duvarı her iki tarafa da entegre edilerek erişilebilirliğin sağlanması, istenmeyen erişimin önüne geçer. Güvenlik duvarı uygulayarak; iletişim kurmasına izin verilen portları ayarlama, iletişim kurmasına izin verilen uygulamaları ayarlama, güvenlik duvarı üzerinden işlemlerin olay günlüğü tutulur, farklı alanlar arasındaki veri işlemlerinin kısıtlanması, istenen IP adreslerine izin verilmesi, istenmeyen IP adreslerinin reddedilmesi işlemleri gerçekleştirilir[17].

Uç nokta Koruması: Bir bilgisayar, dış etkilerden korunması gereken hassas bir cihazdır. Tercihen her bilgisayar, anti-virüs yazılımı, sistem sertleştirme prosedürleri ve düzenli sistem yamalama yoluyla güvenlik altına alınmalıdır.

Uygulama Koruması: Uygulamaların güvenli olarak işlevini yerine getirmesi için ise protokoller, açık kontrol sistemleri ve yetkilendirme sistemleri kullanılmaktadır.

VIII. RISK ANALIZI

Risk yönetimi, kritik varlıkları uygun bir şekilde ve maliyet etkin bir şekilde korumak için gerekli kontrolleri belirlemek için kullanılan bir değerlendirme süreci olup, süreçte yer alan beş temel faktör şunlardır[18]:

- Korunacak varlıkların değeri,
- Bu varlıklara yönelik tehditler,
- Bu varlıkların zayıf noktaları,
- Bu tehditlerin uğrayacağı kayıp türleri,
- Bu tehditleri hafifletecek kontroller.

Genel risk değerlendirmesi için, ASIS Uluslararası Yönerge Komisyonu aşağıdaki genel güvenlik risk değerlendirme adımlarını tavsiye etmiştir [18]:

1. Örgüt, kişileri ve risk altındaki varlıklarını anlama,
2. Riskleri ve zayıf noktaları belirleme,
3. Olası risk ve sıklık olaylarının oluşturulması,
4. Etkileri belirleme,
5. Azaltmanın geliştirilmesi,
6. Seçenekler göz önüne alınması,
7. Maliyet ve fayda analizlerinin yapılması.

Kantitatif/Sayısal risk analiz yöntemleri, olasılıksal risk değerlendirmesinin (PRA) geniş kategorisine girer. Genel kabul gören bir PRA tanımı, karmaşık bir mühendislik tekniği ile ilişkili riskleri değerlendirmek için sistematik ve kapsamlı bir metodolojidir. PRA teknik olarak risk tanımlama aşamasını içerse de, HHM gibi yöntemlerin rehberliğini sağlamaz, aksine tasarımcının riskleri belirleyebileceğini varsayar. PRA tüm arıza ve saldırıyı içerir.

(FTA) ağaç analizi, olay ağacı analizi (ETA), başarısızlık modu ve etki analizi (FMEA) veya hata modu etkisi ve kritiklik analizi (FMECA) ve neden / sonuç analizi (CCA) yanı sıra yönlü grafikler kullanan yöntemler ve Mantık diyagramları uzantıları veya bunların kombinasyonları diğer yöntemlerin oluşturur. Daha önce bahsedilen araçların birçoğu bu yöntemleri farklı derecelerde kullanmaktadır[18].

Risk, bir eylemin ve verilen advers etkinin ortaya çıkma olasılığının ortaya çıkabileceği olumsuz bir sonucun şiddeti ile karakterizedir. Olasılıksal risk değerlendirmesinde, sonuçlar nümerik olarak ifade edilir ve oluşma ihtimalleri olasılıklar veya frekanslar olarak ifade edilir. Risk belirleme genellikle 3 soruya cevap olarak kabul edilir[19]:

- Ne yanlış gidebilir?
- Ne kadar ihtimal var?
- Sonuçları nelerdir?

En eski nicel risk değerlendirme yöntemlerinden birisi Yıllık Zarar Verme Beklentisi (ALE) modelini kullanmaktadır. ALE, Tek Kaybı Beklentisini (SLE) Yıllık Oranı ile çarparak hesaplanır[19].

Olayın (ARO), olayın beklenen sıklığı. Drake ve Morse tarafından önerilen sekizinci aşamalı güvenlik risk değerlendirmesi modeli [20] aşağıdaki aşamaları içermektedir:

1) Tehdit tıkanıklığı,
2) Tehdit oluşumu,
3) Algılama tehdidi oluşumu,
4) Tehdit oluşumundan kurtulma,
5) Güvenlik ihlali,
6) İhlal tespiti,
7) Zararı gidermek,
8) Harici kayıpları belirleme.

Harici kayıplar arasında görev başarısızlığı, personel kaybı, kaynak kaybı, gelir kaybı ve zaman kaybı yer alır.

Birleşik Krallık Güvenlik Servisi tarafından geliştirilen Merkezi Bilgisayar ve Telekomünikasyon Kurumu (CCTA) Risk Analizi ve Yönetim Metodu (CRAMM) [21]: Anketlerden toplanan verilere dayanılarak risk değerlendirmek için matris yöntemine dayanmaktadır. Üç aşamadan oluşur:

1) Varlığın tanımlanması,
2) Güvenlik Açığı tanımlama,
3) Karşı önlem yükleme.

Nicel Tehdit-Risk Endeksi Modeli (QTRIM) [22], ulusal bir altyapıya karşı terörist saldırı riskini tahmin etmek için kullanılır. Idaho Ulusal Mühendislik ve Çevre Laboratuarı'nda (INEEL) inşa edilmiş ve test edilmiş ve terörist spesifik kısıtlamaları, hedefleri, değer sistemleri, lojistik ve bir bilanço puan kartı çerçevesindeki fırsatları kullanarak riski hesaplar.

Hata Ağacı Analizi (FTA) [23] yöntemi tümdengelimli, başarısızlığa dayalı bir yaklaşım kullanmaktadır. Yaprak düğüm tetikleyici olayı temsil ederken, kök düğüm istenmeyen bir olayı veya başarısızlığı temsil eder ve en üstteki etkinliğe götürebilecek farklı olaylar düğümlerin dalları olarak modellenir.

Saldırı ağaçları [19], bir sistemin güvenliğini, FTA modelini kullanarak tanımlamak ve arızayı, arıza oranı için saldırı hedefi ve olay olasılığı olarak değiştirmek için resmi bir yol sağlar. Saldırı ağaçlarının son derece kapsamlı saldırı dizilerini temsil etme kabiliyeti, onları oluşturan güvenlik analistlerinin deneyimine oldukça bağlıdır.

IX. İNTERNET SCADA AVANTAJLARı VE DEZAVANTAJLARı

A.Avantajları

İnternet SCADA veya web tabanlı SCADA'nın avantajları[24];

1. Geniş alana bağlantı ve yaygını

İlk önce, SCADA özel radyo, modem veya seri kablo hatları vasıtasıyla veri iletişimi gerçekleştirir. Şu anda SCADA verileri Ethernet veya TCP / IP ile iletilebilir. Yetenekli mobil kontrol sistemi için, SCADA'nın bilgisayar ağları, hassas verilerin İnternet'e girilmeden geniş bir alana bağlantısını sağlar, çünkü bağlantı kurulduktan sonra, aynı zamanda cihaz yanıtlanabilir.

2. Yönlendirilebilir

Veri iletişim mekanizması yardımcı programlarını destekleyen bir SCADA tabanlı kontrol sistemi tasarımında. Sahada kontrol merkezi ile cihaz arasında konuşlandırılabilir. Şu anda güvenlik uygulamalarında öncelikle tekli tedarikçiler tarafından yönlendirilen bir metodoloji kullanılmaktadır. Yönlendirilebilir kontrol sistemi, bireysel protokollere odaklanma eğilimindedir ve yalnızca bazı iletişim protokollerini yardımcı program için artan bir operasyonel yük altında ele alan bir güvenlik çözümleri karışımını içeren sonuç ortamı sağlayacaktır.

3. Paralel Yoklama

SCADA sisteminde, Master İstasyonu, RTU'nun raporlanması gereken bilgileri içeriyorsa, her RTU'ya kısa mesaj göndermek için sırayla RTU'yu tarar. Tarama çevrimi, yaklaşık 7 saniye (maksimum 10 saniye) olmak üzere nispeten kısa bir süre gerektirir. Sistemdeki tüm uzak terminalleri tarayan tarama döngüsü. Master Station bir RTU'ya emir verirse, o zaman tüm RTU sipariş alır, ancak adresi RTU'yu çalıştıran bir komuta uygun bir şekilde alır. Bu sistem, paralel sistem yoklaması olarak adlandırılır.

4. Fazlalık ve Yedek Uyku

SCADA sistemleri diğer avantajları, Master Station ile RTU arasında aktarılan veri miktarını sınırlama olanağıdır. Bu, istisna raporlama olarak bilinen, yalnızca sınır verileri aşan veri değişiklikleri olduğunda gönderilen bazı verilerin (örneğin, frekans değeri 0.05 Hertz'de bir değişiklik olması durumunda değiştirilebileceği kabul edilebilir) bilinen bir yöntemle yapılır. Bu nedenle, eğer değer çok küçükse, frekansı değiştirmediği kabul edilecektir. Bu, gerçek frekans değerinin açıkça okunabilmesi için sistemin histerezis özelliklerini öngörmek içindir.

5. Büyük adresleme aralığı

SCADA üzerindeki merkezi olmayan sistem, belirtilen PLC bellek adreslerinde saklanan verilere kullanıcı arabirimini içeren bir yöntem gerektirir. Veriler çeşitli sensörler, denetçiler ve farklı veri tabanlarından geldiğinde (yerel olabilir veya farklı yerlerde bağlı olabilir), geniş bir adresleme aralığı gerekir. Web tabanlı SCADA'nın faydalarından biri de geniş aralıklarla ilgilenmektir.

6. BT'nin Otomasyon ve İzleme Ağlarına Entegrasyonu

SCADA tesisleri gerçek zamanlı olarak çalışma kontrolünü gerçekleştirmek için gereklidir. Bir SCADA sistemi, bir dizi RTU (Uzak Terminal Birimi), bir Ana İstasyon / RCC (Bölge Kontrol Merkezi) ve RTU ve Ana İstasyon arasındaki verilerin telekomünikasyon ağları arasında IT sistemlerinin entegrasyonu ve şebeke kontrolünün iyi olması için oluşur. Sonuç performansı.

7. Standardizasyon

SCADA iletişimi bir protokolden düzenlenir, eğer eskiden SCADA üreticilerine uygun bir tescilli protokol kullanılırsa, şimdi bazı kurulmuş protokol standartları vardır, bu nedenle iletişimin uyumluluk sorunlarından bir daha endişelenmeye gerek yoktur.

B.Dezavantajları

İnternet SCADA veya web tabanlı SCADA'nın dezavantajları [24];

1. IP Performans Giderleri

IP adresi, TCP / IP'yi kullanarak bilgisayar ağları ve ağ donanımında verilen addır. IP adresi dört basamaklı ondalık sayı grubu olarak yazılabilen 32 bitlik ikili sayılardan oluşur. IP adresleri A sınıfından E sınıfına kadar beş sınıfa ayrılmıştır. Web tabanlı SCADA çok sayıda ana bilgisayara sahiptir. 1.xxx.xxx.xxx IP aralığı. - 126.xxx.xxx.xxx, 16.777.214 (16 milyon) IP adresi var.

2. Güvenlik kaygısı

Şu anda SCADA tabanlı kontrol sistemi, denetim ve disiplin ile yapılmadığında oldukça savunmasızdır. İlk çözüm, gerekli güvenlik seviyesini sağlayabilen VPN (Sanal Özel Ağlar) kullanmaktı, ancak bağlantı zaten geniş alan ağına bağlıysa, risk seviyesi yüksektir. Son zamanlarda, Stuxnet'in haberi, kodla yapılan çok sofistike bir programdır; çok karmaşıktır ve bazı boşluklar işletim sistemini, büyük ölçekli / endüstriyel amaçlı saldırıların hedefiyle aynı anda sömürür.

X. SONUÇ

SCADA sistemleri, kontrol edilmesi gereken kaynakların ve işlevlerin sayısının artması, giderek otomatikleşen kontrol yöntemleri ve bu yöntemleri tam anlamıyla karşılamayan teknolojileri kullandıkları için saldırılara ve tehditlere karşı savunmasızdır. Yeni yazılım yükseltmeleri ve güvenli ekipman mevcut olmasına rağmen, sistemleri güvenlik açıklarından korumak için onları benimser hale getirmek zordur. SCADA sistemlerinin yavaş ilerlemesinin çoğunlukla siber güvenlik konusunda tanınmaması nedeniyle olduğu düşünülmektedir. Bununla birlikte, risk gerçektir. Bu nedenle, olası tehditlere karşı önlemlerin alınması çok kritik öneme sahiptir. Öncelikle, sistemin güvenlik açığı noktalarını ve muhtemel saldırı türlerini analiz etmek ve tanımlamak önemlidir. Bu makalede SCADA sisteminin bileşenleri ve işlevleri anlatılarak çalışma prensibi doğrultusunda nasıl güvenlik açıkları oluşabileceği ve sistemin karışılacağı tehditler bir arada incelenmiştir. Bu açıkların ve tehditlerin hangi tedbir ve protokoller yardımıyla siber ortamda daha güvenli bir şekilde çalışması sağlandığı açıklanarak, bu çalışmalar için nasıl bir risk değerlendirme işlemi yapıldığına değinildi. Son olarak genel olarak SCADA sistemlerinin ve ICS güvenliğini artırmak için genel kabul görmüş çözüm önerileri oluşturuldu.

XI. KAYNAKLAR

[1] Hüseyin Avni Demirci, SCADA Sistemi ile İlgili Teknolojideki Gelişmeler ve Bu Sistemin Samsun Bölge Müdürlüğü Görev Alanı Dâhilindeki Belediyelerde Uygulama Alanları, Bilgi Teknolojileri ve İletişim Kurumu, Mayıs 2013.

[2] Yogesh Sahu, SCADA system vulnerabilities and Threat to critical infrastructure, Tata Power Trombay Generating Station.

[3] Nicoleta IGNAT, Dependabılıty and Vulnerabılıty of SCADA Systems, Annals of The Oradea Unıversıty Fascicle of Management and Technological Engineering ISSUE #1, MAY 2014.

[4] Endüstriyel Otomasyon Teknolojileri, SCADA Sistemlerine Giriş, Millî Eğitim Bakanlığı, Ankara 2014.

[5]http://patriot-tech.com/blog/2015/10/27/common-scada-system-threats-and-vulnerabilities/

[6]http://www.aogr.com/web-exclusives/exclusive-story/cyber-security-strategy-key-to-scada

[7] M. Berg and J. Stamp, A reference model for control and automation systems in electric power, Technical Report SAND2005-1000C, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[8] E. Byres, J. Carter, A. Elramly and D. Hoffman, Worlds in collision: Ethernet on the plant floor, Proceedings of the ISA Emerging Technologies Conference, 2002.

[9] Instrumentation Systems and Automation Society, Security Technologies for Manufacturing and Control Systems (ANSI/ISA-TR99.00.01-2004), Research Triangle Park, North Carolina, 2004.

[10] Instrumentation Systems and Automation Society, Integrating Electronic Security into the Manufacturing and Control Systems Environment (ANSI/ISA-TR99.00.02-2004), Research Triangle Park, North Carolina, 2004.

[11] American Petroleum Institute, API 1164: SCADA Security, Washington, DC, 2004.

[12] American Gas Association, Cryptographic Protection of SCADA Communications; Part 1: Background, Policies and Test Plan, AGA Report No. 12 (Part 1), Draft 5, Washington, DC (www.gtiservices.org/security/ AGA12Draft5r3.pdf), 2005.

[13] American Gas Association, Cryptographic Protection of SCADA Communications; Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, AGA Report No. 12 (Part2),Draft,Washington,DC(www.gtiservices.org/security/aga-12p2-draft-0512.pdf), 2005.

[14] British Columbia Institute of Technology, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Security Co-ordination Centre, London, United Kingdom, 2005.

[15] National Institute of Standards and Technology, System Protection Profile – Industrial Control Systems v1.0, Gaithersburg, Maryland, 2004.

[16] K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security – Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[17] Erik Daalder, SCADA Cyber Security, Information on Securing SCADA systems Version: 1.0, Yokogawa Electric Corporation—Global SCADA Center.

[18] Guillermo A. Francia, III, David Thornton, and Joshua Dawson, Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems.

[19] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, A review of cyber security risk assessment methods for SCADA systems, Computers & Security 56 (2016) 1–27.

[20] Drake, D.L. and Morse, K.L. 1994. The Securityspecific Eight Stage Risk Assessment Methodology. In Proceedings of the 17th National Computer Security Conference (San Diego, CA).

[21] Jones, Andy, and Ashenden, Debi. 2005. Risk Management for Computer Security: Protecting Your Network and Information Assets. ButterworthHeinemann, UK.

[22] Beitel, G.A., Gertman, D. I., and Plum, M.M. 2004. Balanced Scorecard Method for Predicting the Probability of a Terrorist Attack. Risk Analysis IV:581-592, WIT Press, Brebbia, C.A., ed..

[23] Vesely W. Fault Tree Analysis (FTA): Concepts and Applications. Website: http://www.hq.nasa.gov/office/codeq/risk/ docs/ftacourse.pdf. Access date: March 05, 2012.

[24]https://program-plc.blogspot.com.tr/2015/09/the-top-9-advantages-and-disadvantages.html

Tasarımda Veri Koruma: Kişisel Veri Dostu Yazılımlar İçin Hukuki, İdari ve Teknik Bir Yaklaşım

Data Protection by Design: A Legal, Administrative and Technical Approach Towards the Personal Data-Friendly Software

Gizem Gültekin Várkonyi
Siyasal Bilimler ve Hukuk Fakültesi, Szeged Üniversitesi, Szeged, Macaristan
gizemgv@juris.u-szeged.hu

Özet

Kişisel verilerin en etkili biçimde korunması, bazı teknik uygulamaların kişisel veri toplayan, saklayan, işleyen ve transfer eden sistemlerle bütünleştirilmesi sayesinde hukuki gereklilikleri tamamlayıcı şekliyle mümkündür. Kişisel veri içeren sistemlerin, geliştiriciler tarafından güvenlik değerlendirmesine tabi tutulmasının yanı sıra, idari açıdan atılacak adımlar bu süreci daha da kolaylaştırıp bu değerlendirmeler için gerekli verileri sağlayacaktır. Bu makale, tüm bu süreçleri ele alan ve Avrupa Birliği'nin 2018 Mayıs ayında yürürlüğe girecek olan Genel Veri Koruma Tüzüğü'nde yer alan Tasarımda Veri Koruma ve Veri Koruma Etki Değerlendirmesi sunulmaktadır.

Anahtar kelimeler

Veri koruma, gizlilik, veri gizliliği, gizlilik artırıcı teknolojiler, bilgi güvenliği, hukuk

Not

Bu makale, başka bir dergide İngilizce olarak yayımlanabilir.

Abstract

It is possible to protect personal data on an effective way by integrating some of the technical safeguards into the such systems that collect, store, process and transfer personal data. The systems that contain personal data shall be evaluated from the data security point of view and administrative steps shall be taken to maket this evaluation easier as well as create an input for it. This article seeks to given an overview of the two terms: Data Protection by Design and Data Protection Impact Assessment which are the core terms for such evaluations and the terms that are embedded into the European Union General Data Protection Regulation which will enter into force in May 2018.

Keywords

Data protection, privacy, data privacy, privacy enhancing technologies, information security, law

I. GİRİŞ

Daha çok Tasarımda Gizlilik (Privacy by Design) olarak bilinen Tasarımda Veri Koruma anlayışı (Data Protection by Design, TVK), 2018'in Mayıs ayında yürürlüğe girecek Avrupa Birliği Genel Veri Koruma Tüzüğünde (GVKT) yer alan kişisel veri koruma kurallarından biridir [1]. Tüzüğün tüm AB ülkelerinde aynı şekilde uygulanacak olmasının yanı sıra, AB üyesi olmayan ülkeleri de bağlayıcı olması Tüzük için küresel bir geçerlilik hissi vermektedir. TVK'nin yalnızca mevzuatla uyumlu olmak adına değil kişisel verilerin bir insan hakkı olarak korunarak organizasyonlara katma değer sağlayacak bir organizasyon kültürü olarak algılanabilir. Ayrıca, TVK hızlı gelişen teknolojinin getirdiği kişisel veri koruma endişelerini en yeni güvenlik teknikleri ile korumak adına önemli bir adımdır. Bu gibi sebeplerden dolayı, konu yalnızca hukukçular açısından değil, yazılım ve bilgisayar mühendisler ile idareciler için de önemlidir. Bu makale TVK hakkında hem idari hem de teknik açıdan faydalı olabilecek bilgiler vermeye çalışarak konu ile ilgili bütün bir bakış açısı sunmayı hedeflemektedir.

II. TASARIMDA VERİ KORUMA

Kişisel verilerin korunması ile ilgili teknik ve yasal çalışmaların tavan yaptığı 90'lı yıllarda Kanada Bilgi ve Gizlilik Komiseri Ann Cavoukian, TVK prensiplerinin sıralayarak konunun öncüsü olmuş, bu prensipler akademik çevrelerce de kabul edilerek geliştirilmiştir [2,3]. Tüm bu gelişmeler TVK'nin hem hukuksal hem de teknik aşamalarının olduğunu ve bunların bir organizasyon içerisinde geliştirilecek bir ürün için en baştan atılacak adımlarla kabul edilmesi gerektiğini vurgulamaktadır. Bu prensipler hukukla ilişkilidir, çünkü TVK'nin kabul edilmesi gerektiği yasalarla garanti altındadır (AB GDPR). Tekniktir, çünkü kişisel verilerin korunmasına yönelik atılan adımların ilgili sistemde teknik bir karşılığı olmalı, GAT ile güvence altına alınmalıdır. Tüm bunlara bakarak TVK, kişisel verilerin toplanması; kullanımı; transfer edilmesi; kısacası veriye ilişkin tüm işlemlerin haritasının çıkarılması, risk değerlendirmesi yapılması ve teknik araçlar yardımıyla gerekli önlemlerin alınmasını öngörür.

III. NEDEN TVK?

TVK'nin şirketlere ve kurumlara sağladığı katkıların bilinmesi, bu kavramın çok daha hızlı biçimde kabul edilmesini sağlayacaktır.

Öncelikle, kişilerin temel haklarına saygılı bir sistemin üretilebilmesi için "önce kişisel bilgilerin korunması" kültürünün [4] organizasyon içerisinde yaratılması gereklidir. Bu kültür sayesinde organizasyonlar müşterilerinin güvenini kazanacaktır. Özellikle Internet kullanıcıları güvenli biçimde Internet tabanlı ürünleri kullanarak hizmet sağlayıcılara olan güvenlerini göstermekte, Internet ekonomisi bu tabanda büyüyüp gelişmektedir [5,6] çünkü güvenli sistemler daha çok kişi tarafından kullanılmaktadır. Apple şirketinin bu denli pazar payının büyük olmasının sebeplerinden biri de budur çünkü Apple'da "kullanıcıların güveni her şey demektir ve bu yüzden kullanıcıların gizliliğine saygı duyularak şifreleme gibi yöntemlerle sistemler korunur" [7].

Bunu takiben, organizasyonlar veri koruma mevzuatına TVK sayesinde uyum sağlayarak yüksek miktarda para cezaları ile karşılaşmayacaktır. AB mevzuatına göre kişisel verileri mevzuatta belirttiği gibi korumayan organizasyonlar, AB sınırları içerisinde olup olmadığına bakılmaksızın yüksek para cezalarına çarptırılabilecektir. TVK'nin benimsenmesi organizasyonları bu tür ceza ve ekonomik zarardan kurtaracaktır.

Ayrıca, TVK sayesinde sistemlerde kişisel verilerin korunması ile ilgili mevcut ve olası risklerin en baştan yönetimi sağlanarak geleceğe yatırım yapılabilir. Çünkü daha sonra fark edilen riskler veya karşılaşılan zararlar hem organizasyonun itibar kaybına hem de zararın giderilmesi için harcanacak para kaybına sebep olacaktır [8]. Kısacası, TVK'nin benimsenmesi gerçekten de doğru bir adım olacaktır [9,10].

Son olarak, TVK küresel anlamda yaşanan veri koruma asimetrisinin, güç oyunlarının ve politik çekişmelerin azalmasına katkıda bulunabilir; bilginin serbestçe dolaşımını sağlayabilir; demokratik ve güvenli toplumların inşa edilmesini sağlayabilir. Yasa dışı bilgi kullanımın, bilgi sızıntılarının, devletler tarafından gözetlenmelerin karşısına geçmenin bir yolu da kişisel verilerin güvence altına alınmasıdır. Örneğin, AB'nin Facebook gibi Amerikan yazılım firmalarına yaptığı baskılar sonucunda ve küreselleşmenin de etkisiyle, dünyanın her yerindeki Facebook kullanıcısı aynı veri koruma kriterlerinden faydalanmaktadır [10].

Kişisel verilerin korunması 2010 Anayasa referandumu sonrasında ülkemizde de temel bir hak olarak kabul edilmiştir. Konu ile ilgili Avrupa'daki gelişmelerden hukukta ve uygulamada oldukça uzak kalmış ülkemizdeki mevzuat her ne kadar TVK'yi yasal bir zorunluluk olarak göstermese de Bilgi ve İletişim Teknolojileri ile hizmetlerini sunan her kurum ve şirkette bu anlayış sayesinde hızlı ve etkin bir kişisel veri koruma anlayışı edinilebilir.

IV. TVK NASIL UYGULANIR?

TVK, kurumsal değerlendirmeler ve teknik önlemler olmak üzere iki temel konuda incelenebilir ve her ikisi de hukuksal gelişmeler tarafından tetiklenir. Kurumsal değerlendirmeler Veri Koruma Etki Değerlendirmesi (VKED) ile yapılır ve bu değerlendirme sonucunda uygun Gizlilik Artırma Teknolojisi (GAT) ile tamamlanarak kişisel verileri koruyacak teknik önlemler alınır.

A.Veri Koruma Etki Değerlendirmesi

AB GVKT'sinin diğer bir yeniliği olan VKED, yalnızca verilerin işlenmesi insan hakları ve özgürlükleri için yüksek seviyede risk oluşturuyor ise yapılması gerekir. Kişisel veri işleyen her sistemin gerçekte bir miktar risk taşıdığı göz ardı edilmemeli ve Değerlendirme her şekilde ele alınmalıdır. Değerlendirme risk yönetiminin en önemli aşamasıdır ve ancak başarılı bir değerlendirme başarılı bir korumayı beraberinde getirecektir [10].

VKED, organizasyonları çalışanları ve paydaşlarıyla bir araya getirerek planlanan veya çalışmakta olan bir sistem içinde sistematik biçimde hangi riskin nasıl yönetileceğine birlikte karar verilmesini sağlar. VKED ile PDBD arasındaki ilişki iki türlüdür: Birbirlerini beslerler ve tamamlarlar [11,12]. Beslerler, çünkü Değerlendirme sonunda TVK'nin önemli bir adımı olan teknik korumanın nasıl ve hangi tekniklerle yapılacağına karar verilmesi için gerekli veri buradan sağlanır. Tamamlarlar, çünkü gerekli tedbirlerin önceden alınması için Değerlendirme sonucuna ihtiyaç vardır.

Konu ile ilgili her organizasyonun, Veri Koruma Kurulunun veya kurumun "nasıl" sorusuna yanıt vermek için farklı yaklaşım ve rehberi vardır. Bunun temel sebebi ise her organizasyonunu kendine göre bir iş akışı, işlemi, ürünü ve hizmeti kısacası her organizasyonun birbirinden farklı olmasıdır. Bu sebeple öncelikle hiçbir VKED'nin birbirinin aynısı olması beklenmemelidir. Ancak bir başlangıç noktası olması açısından aşağıdaki adımların takip edilmesi önerilir:

- Ürünün kişisel veri bakımından tanımlanması
    - Veri türlerinin tanımlanması
    - Verilerin nasıl ve neden toplandığının, nasıl kullanıldığının, işlendiğinin, transfer edildiğinin, ve saklandığının tanımlanması
    - İşlemlerin görselleştirilmesi (diyagramlar, tablolar, çizimler vs. ile)
- Risk tanımı ve değerlendirmesinin yapılması
    - Risk türlerinin tanımı (sunucu güvenliği gibi teknik riskler, anonimleştirme gibi kodlama riskleri veya politika eksikliği gibi idari riskler)
    - Ürün kişisel veriler açısından yüksek derecede risk yaratacak işlemler yapıyor mu?
    - Yüksek risk yaratan durumlar ile ilgili Kişisel Verileri Koruma Kurumuna danışılmalıdır [1]

• Planlanan veya sistemin zaten çalışıyor olması durumunda eldeki mevcut önlemlerin değerlendirilmesi
    - Önlemler hukuki gerekliliklerle uyumlu mu?
    - Teknik önlemler risk yönetimi için uygun ve yeterli mi?
• Gerekliliklerin listelenmesi
    - Organizasyon hedefleri
    - Yasal gereklilikler
• Kontrol listesinin oluşturulması
    - Teknik toplantılar (çalıştaylar, know-how toplantıları, beyin fırtınası toplantıları, personel toplantısı, uzmanlar toplantısı vb.)
    - Değerlendirmenin tamamlanması ve karar alma aşamasına geçmek için yapılacak idari toplantılar
    - Listenin hayata geçirilmesi (bu aşama birçok idari ve teknik aşama gerektirecektir)
• Değerlendirmenin şu amaçlarla dokümante edilmesi:
    - Kişisel Verileri Koruma Kurulu başta olmak üzere ilgili tüzel kişilere ve müşteri/kullanıcılara hesap verebilmek
    - değerlendirmeyi benzer ürünler için tekrar kullanabilmek
    - işlemlerin standartlaştırılması
    - milli ve küresel veri koruma kültürüne katkı yapabilmek amacıyla tecrübe paylaşımı
• Gözetim ve değerlendirme
    - Teknik uzman, kullanıcı, hukuk uzmanları gibi ürünle ilgili kişilerin geribildirimlerinin alınması
    - Gözden geçirme, denetim ve hesap verilebilirlik mekanizmalarının değerlendirilmesi

Verilen kontrol listesi standart olmayıp listenin organizasyon ihtiyaçlarına göre şekillendirilmesi uygun olacaktır. Örneğin profili Büyük Veri analizi yapmak olan organizasyonların VKED'si de daha geniş kapsamlı ve masraflı, kontrol listesi daha geniş olacaktır [13] Bu aşamada değerlendirmenin daha ekonomik, hızlı ve otomatik olarak yapılabilmesi adına konuyla ilgili yazılımların kullanılması uygun olabilir. Aynı zamanda herhangi bir otoriteye bağlı olmadan ürün, organizasyon ve mevzuat arasında köprü görevi kuracak bir veri analistinin görevlendirilmesi organizasyon için olumlu bir adım olacaktır [10].

Risk analizinin yapılmasından sonra sistem içerisinde kişisel verilerinin korunması için gerekli GAT'ın seçilmesi aşamasına geçilir.

B.Sistemler İçerisinde Veri Güvenliği: Gizlilik Artırıcı Teknolojiler

Gizlilik Artırıcı Teknolojilerin (Privacy Enhancing Technologies, GAT) kişisel verilerin korunması yaklaşımıyla yapılmış en kapsamlı diyebileceğimiz tanımını AB literatüründe bulmak mümkündür. Buna göre GAT:

"Herhangi bir bilgi sistemini işlev kaybına uğratmadan, içinde barındırdığı kişisel verileri yok etme veya en aza indirgeme yoluyla, verilerin istenmeyen biçimde veya amacı dışında işlenmesini önleyen ve böylece veri gizliliğini koruyan bilgi iletişim teknolojileri tedbirleridir" [14]

GATs AB veri koruma literatüründe yeni bir kavram değildir ancak GVKT kapsamına alınarak genişletilmiş ve açıklanmıştır. Buna göre, GATler organizasyonlara VKED sonucu ortaya çıkan kişisel veri risklerinin teknik araçlar yardımıyla azaltılmasını veya ortadan kaldırılmasını sağlayan araçlardır. Bu araçlar genelde veriyi anonimleştirme, kriptolama, e-posta gizliliği araçları, PSUD, yetkilendirme, çerez engelleyici, Platform for Privacy Preferences (P3P) gibi çok çeşitlidir. Verilen örneklerin ve geçerli güvenlik araçlarının GVKT'nin yürürlüğe girmesiyle hızlı bir şekilde artıp çeşitleneceği öngörülmektedir.

GAT araçları organizasyonlar için faydalı olabilecek verileri yok eden bir düşman değildir; aksine, örneğin, sistemlerde verinin ait olduğu bütünü ve orijinal veri grubunu etkilemeden korumak mümkündür [15]. Böylelikle kişisel veriler herhangi bir yasal kurala karşı gelmeden de fonksiyonel biçimde sistem içerisinde kullanılabilir.

ENISA raporuna göre GAT'lerin sistem tasarımının kavramsallaştırılması aşamasında belirlenip uygulanması organizasyonlar için avantajlıdır. Bahsi geçen rapor mevcuttaki GAT araçlarını toplayan, araçların kullanım alan ve durumlarını özetleyen, örnekler veren ve risklerini tartışan önemli bir rapordur. Tüm GAT araçlarının bir çalışmada toplanması araçların çeşitliliği ve özellikleri açısından oldukça zor olduğundan [16,17], aşağıda bu rapordan yararlanarak bir tablo sunmak mümkündür [18]. Tablo organizasyonlar için uygun bir kişisel veri koruma tekniği seçimi aşamasında başlangıç noktası teşkil etmesi açısından önemlidir.

TABLO I. ENISA RAPORUNA GÖRE KİŞİSEL GİZLİLİĞİ ARTIRI

Teknik Türü	Metot ve/veya Örnek
Anonimleştirme ve takma isim verme	• Tekli Vekil Sunucuları veya Sanal Özel Ağlar (SÖA), Only routing (Sadece dolaşma, TOR ve Jondonym) d, Karışık ağlar (mixmaster ve minminion,Verificatum), Yayın şemaları, Steganografi (TrueCrypt) ve blocking resistance (Tor, TrueCrypt)
Yetkilendirme	• İstemci-sunucu • Uçtan uca (önerilendir) • Federe kimlik yönetimi ve Tek Oturum Açma (Single Sign On) • Just Fast Keying (JFKi/r) ve Taşıma Katmanı Güvenliği (TKG) protokolleri, • Shibboleth, Infocards, Liberty Alliance Projesi
Özelik Bazlı Yetkilendirme (Attribute Based Credential)	• U-Prove (Microfost) , • Baldimtsi-Lysyanskaya, • Idemix (IBM)
Güvenli Özel İletişim (Secure Private Communications)	• Temel kriptolama o İstemci-sunucu o Uçtan uca o Dönüşümlü anahtar (Key rotation), yönlendirilmiş gizlilik, coercion resistance • TKG (Certificate Pinning ile desteklenerek), Secure Shell, IPSec (SÖA ile desteklenerek) • Akıllı telefonlar için: PrettyGood Privacy, S/MIME standardı, Off-The-record mesajlaşma, TextSecure mobil sohbet, Crypto Phone ve Red Phone • DH veya ECDH ve OTR ile geliştirilmiş TKG
Veritabanı gizliliği (Database privacy)	• Yanıtlayıcı gizliliği • Veri sahibinin gizliliği • Kullanıcı gizliliği
Deneklerin gizliliği (bilimsel ve istatistiki amaçlar için)	• Statistical Disclosure Control (SDC) veya Statistical Disclosure Limitation (SDL) o Çizelgesel veri koruma o Sorgusal veri koruma o Mikroveri koruma: Veri maskeleme ve veri sentezi

Teknik Türü	Metot ve/veya Örnek
	o Priori privacy modelleri o Priori ve posteriori anonimleştirme • Olası bir saldırıya karşılık: (n, k)-dominance kuralu, pq-kuralı, p% kuralı) • Sorgu pertürbasyonu, Sorgu sınırlama • Pertürbatif maskeleme
Veri sahibinin gizliliği	• Gizlilik sağlayan veri madenciliği ve malumat saklama
Depolama gizliliği (Storage privacy)	• İşletim sistemi kontrolü • Yerel kriptolu bellek türleri: Tam bellek kriptolama; Dosya sistem düzeyi kriptolama (örn.Format Preserving) • Steganografik depolama: Güvenli uzak bellek • FileVault, TrueCrypt, BitLocker, LUKS (Linux Unified Key Setup). • Steganografi: TrueCrypt • Güvenli uzaktan erişim: Tahoe-LAFS (bulut için) • Güvenli kriptolanmış veri arama: Simetrik Aranabilir Kriptolama, Açık Anahtarlı Kriptolama
Gizlilik Sağlayan Bilişim (Privacy Preserving Computation)	• Homomorfik Teknikler: Tam Homomorfik Kriptolama ve Kısmen Homomorfik Kriptolama • Güvenli Bilişim: Gizlilik sağlayan veri madenciliği (PPDM) ve özel bilgi erişimi (PIR) içeren MPC uygulamaları • Gizli paylaşım ve habersiz transfer: E-oylama sistemler (SCYTL, Prêt à Voter)
Şeffaflık Artırıcı Teknolojiler	• Örnekler: Google gibi şirket gösterge tablolar yayınlamak,Firefox'un Lightbeam'i, Taint Droid, Mobilitics (akıllı telefonlar için), Data Track (Prime Project örneğinden), ToS; DR ve TOSBack; P3P ve Privacy Bird, Contextual Integrity, S4P, SIMPL, RFID logosu örneğindeki gibi logolar kullanmak
Müdahaleyi iyileştirme	• The Data Track

Bu tablo yalnızca şu anda mevcut teknik, metot ve örnekleri toplamaktadır. PET'in önemi ve gerekliliği kavrandıkça daha yeni teknik ve metotlar geliştirilecek, böylelikle tablonun daha da genişleyeceğini düşünmekteyiz. Bu gibi tablolar özellikle geliştiricilerin sistemlerde kişisel veri korumanın güçlendirilmesi için gerekli adımı atmak adına nereden başlayacaklarını, mevcut teknikleri, riskleri ve örnekleri görebilmeleri açısından önemlidir.

V. SONUÇ

Kişisel verilerin korunması ancak bir dizi idari ve teknik adımların atılması ile mümkündür. Tasarımda Veri Koruma kavramı hem idareleri hem de geliştirici gibi teknik çalışanları başta olmak üzere birçok paydaşı bir araya getirerek kişisel veri içeren sistemlerin değerlendirilmesini öngörür. Değerlendirmeler bir sistem içerisindeki verinin Veri Koruma Etki Değerlendirmesi kapsamında yapılır. Bunun sonucunda sistemlerdeki veri güvenliğini tehdit eden riskleri azaltmak ve güvenliği sağlamak için Gizlilik Artırıcı Teknolojilerden yararlanılır. Ülkemizde kişisel verilerin korunması adına atılan hukuki adımların Tasarımda Veri Koruma kavramının benimsenerek takip edilmesi birçok açıdan oldukça faydalıdır. Bu kavramın daha iyi açıklanması ve anlaşılması için gelecekte yapılacak çalışmalara ihtiyaç vardır.

KAYNAKLAR

[1]European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) Official Journal L 119, pp. 1–88.

[2]A. Cavoukian, "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices," 2011

[3]I. Rubinstein, "Regulating Privacy by Design," Berkeley Technol. Law J.,vol.26,p.1409,20. Çevirim içi erişilebilir: :http://dx.doi.org/doi:10.15779/Z38368N

[4]E. Everson, "Privacy by Design: Taking Ctrl of Big Data," Cleveland State Law Review, vol. 65. pp. 27–44, 2016.

[5]A. Rachovitsa, "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue," Int. J. Law Inf. Technol., vol. 24, no. 4, pp. 374–399, Dec. [Online]. Available: http://dx.doi.org/10.1093/ijlit/eaw012

[6]P. Schaar, "Privacy by Design," Identity Inf. Soc., vol. 3, no. 2, pp. 267–274, 2010

[7]Apple Inc. "Apple's commitment to your privacy." Available: https://www.apple.com/privacy/

[8]Information Commissioner's Office (ICO), "Conducting privacy impact assessments code of practice," 2014. Elektronik kaynak

[9] N. Hodge, "The EU: Privacy by Default Analysis," In-House Perspective, vol. 8. pp. 19–22, 2012.

[10]K. A. Bamberger ave D. K. Mulligan, "PIA Requirements and Privacy Decision-Making in US Government Agencies," in Privacy Impact Assessment, D. Wright ve P. De Hert editörler Dordrecht: Springer Netherlands,2012,pp.225-250. Çevirim içi erişilebilir: http://dx.doi.org/10.1007/978-94-007-2543-0_10

[11]I. S. Rubinstein ve N. Good, "Privacy by Design: A Counterfactual

Analysis of Google and Facebook Privacy Incidents" Berkeley Technology Law Journal, vol. 28. pp. 1333–1414, 2013. Çevirim içi erişilebilir: http://dx.doi.org/doi:10.15779/Z38G11N.

[12]S. Sarah ve M. C. Oetzel, "Privacy-by-Design Through Systematic Privacy Impact Assessment – A Design Science Approach," ECIS - Conference Proceedings, 2012

[13]M.Chibba ve A.Cavoukian,"Privacy, consumer trust and big data: Privacy by design and the 3 C's," 2015 ITU Kaleidoscope: Trust in the Information society (K-2015). International Telecommunication Union, p.1, 2015.

[14]Europen Union, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) COM/2007/0228 final. 2007.

[15]J. Hajny, L. Malina, ve P. Dzurenda, "Practical privacy-enhancing technologies," in 2015, 38th International Conference on Telecommunications and Signal Processing (TSP), 2015, pp. 60–64. Çevirim içi erişiebilir: https://doi.org/10.1109/tsp.2015.7296224.

[16]J. Heurix, P. Zimmermann, T. Neubauer, ve S. Fenz, "A taxonomy for privacy enhancing technologies," Computer&Security., vol. 53, pp. 1–17,2015 [Online]Available:http://dx.doi.org/10.1016/j.cose.2015.05.002.

[17]Y.Kang, H.Lee, K.Chun, and J.Song, "Classification of Privacy Enhancing Technologies on Life-cycle of Informatio," in The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), 2007, pp. 66–70.

[18]European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design – from policy to engineering," 2014. Çevirim içi erişilebilir: http://dx.doi.org/10.1007/978-3-642-37282-7 5.

Kurumsal Bilgi Güvenliği Üzerinde Yeni Kayıtlı İnternet Sitelerinin Etkisinin Analiz Edilmesi

Analysing Internet Websites for Enterprise Security

Samet Ganal
Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Isparta, TÜRKİYE
samet.ganal@kuveytturk.com.tr

Mehmet A. Yalçınkaya
Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Isparta, TÜRKİYE
mehmetyalcinkaya@sdu.edu.tr

Ecir U. Küçüksille
Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Isparta, TÜRKİYE
ecirkucuksille@sdu.edu.tr

Özet

İnternet üzerinde yayına başlaması üzerinden 14 gün geçmemiş ve Proxy uygulamaları tarafından henüz kategorize edilmemiş olan web siteleri, yeni kayıtlı web siteleri olarak adlandırılmaktadır. Kurumsal bilgi güvenliğini sağlamak için, yeni kayıtlı internet sitelerine yönelik ne tür bir politika uygulanması gerektiği, çözülmesi gereken bir problemdir. Bu çalışmada bir kurum bünyesinde yer alan 6000 kurum çalışanına ait bir yıllık internet aktivitesi incelenmiştir. Kurum çalışanlarının yeni kayıtlı internet sitelerine erişim oranları ve erişim nedenleri araştırılmıştır. Gerçekleştirilen çalışmada ayrıca, yeni kayıtlı internet siteleri ile ilgili bir test senaryosu oluşturulmuştur. Oluşturulan test senaryosunda, ilk 6 aylık sürede kullanıcıların yeni kayıtlı internet sitelerine erişimi açılmış, sonraki 6 aylık süre içinde ise engellenmiştir. Gerçekleştirilen test sonrasında kullanıcıların serbest erişim ve engelleme işlemlerine yönelik tepkileri analiz edilmiştir.

Anahtar Kelimeler

Yeni kayıtlı internet siteleri, kurumsal bilgi güvenliği, Proxy, zararlı yazılım.

Abstract

Websites that have not yet been categorized by proxy applications and that have not passed 14 days since its launch on the Internet are called newly registered web sites. To ensure corporate information security, what kind of policy should be applied to newly registered internet sites is a problem must be solved. In this study, one year internet activity belonging to 6000 institution employees in an institution was examined. Institution employees' access rates to new registered websites and reasons for access were investigated. In our study also, a test scenario related to newly registered internet sites has been established. In the test scenario that was created, users were allowed access to newly registered internet sites during the first 6 months, and they were blocked within the next 6 months.

Index Terms

Newly registered web sites, enterprise information security, proxy, malware.

I. GİRİŞ

Günümüz teknoloji dünyasında kurumlar çalışanlarını zararlı yazılımlar ve oltalama saldırılardan korumayı amaçlamakta, bu ideallere ulaşmak için çeşitli internet sınırlandırmaları yapmaktadırlar. Yapılan internet sınırlandırmalarının en büyük sebebi kurumsal bilgi güvenliğini sağlamaktır. Bunun yanında kurum içi çalışma veriminin artırılması ve kurum imajına uygun şekilde duruş sergilenmesi amacıyla da sınırlandırmalar yapılabilmektedir.

Gelişen ve çoğalan internet kategorileri arasında yenice ortaya çıkan "Yeni Kayıtlı İnternet Siteleri" kategorisi; kurum güvenliğini yakından ilgilendirmektedir. Bunun yanı sıra kullanıcılar tarafından kurum internet politikalarının aşılması amacıyla da kullanılabilmektedir.

İnternet üzerinde yayına başlamasının üzerinden 14 gün geçmeyen ve bu süreçte proxy uygulaması tarafından herhangi bir kategorize işlemine tabi tutulmayan internet siteleri, yeni kayıtlı internet siteleri olarak tanımlanmaktadır. Bu tür internet sitelerine erişim proxy uygulaması üzerinden engellenebilmekte ya da izin verilebilmektedir. Birçok firmada bu kategori varsayılanda izinli olarak gelmektedir.

Yeni kayıtlı internet sitelerinin engellenmediği durumlarda kullanıcılar proxy uygulaması tarafından henüz kategorize edilmemiş tüm yeni kayıtlı internet sitelerine erişebilme hakkına sahiptir. Bu durumda kullanıcı, içerisinde spam yaymak ya da oltalama saldırısı gerçekleştirmek amaçlı zararlı yazılımlar barındıran sitelere, yeni kayıt olduğu ve kategorize işlemine tabi tutulmadığı için erişebilmekte, kendisini ve içerisinde bulunduğu ağdaki tüm cihazları riske atabilmektedir [1].

Yeni kayıtlı internet siteleri kategorisinin bir diğer artısı ise kullanıcıların kurum internet politikalarını aşmasını çok daha zorlaştırmasıdır. Kullanıcılar kurum internetini kullandığı sürece mesai saatleri içinde veya dışında belirli internet politikalarına tabidir ve uymak zorundadır. Kimi zaman kullanıcılar bahis, yetişkin, dizi-film izleme siteleri gibi kurum ağından izin verilmeyen internet sitelerine erişmeyi denemektedir. Bu tür siteler arasında düzgün şekilde kategorize edilmiş olanlar hali hazırda proxy uygulaması tarafından engellenmektedir. Ama

domain adı yeni alınan siteler proxy uygulaması tarafından kategorize edilene kadar erişime açık kalacaktır.

- dizimag.co
- dizimag.me
- dizimag.com
- dizimag.site
- dizimag1.co
- dizimag1.com
- dizimag2.co
- dizimag2.tr.gg
- dizimag4.com
- dizimagizle.com
- dizimagx.com
- dizimagyeni.com

Şekil 1. Kurum çalışanlarının erişmeye çalıştığı yeni kayıtlı site örnekleri

Şekil 1'de kurum kullanıcılarının 4 aylık bir periyotta erişmeye çalıştığı "dizimag" isimli bir dizi izleme sitesinin farklı domainlerden yaptığı yayınlar gösterilmiştir. Kullanıcılar asıl domain olan "dizimag.com"a erişmeye çalışmış ama bu internet sitesi "Streaming Media" kategorisinde olduğundan dolayı proxy uygulaması tarafından engellenmişlerdir. Yeni kayıtlı internet siteleri kategorisinin izinli olması durumunda kullanıcı erişmeye çalıştığı alan adını veya uzantısını değiştirip ilgili siteye erişim sağlayabilmekte, kurumun internet politikalarını atlatabilmektedir. İncelenen örneğin yanı sıra, içerisinde zararlı yazılım barındıran yeni kayıtlı internet sitelerinin alan adlarının rastgele oluşturulduğu ve anlamsız sözcükler içerdiği de görülmüştür [2].

Öte yandan kurum içerisinden yeni açılan internet sitelerine yönelik olarak yapılacak engelleme, kurum personelinin erişmesi gereken zararsız sitelere erişmesini de engelleyebilmektedir. Sonuç olarak, bu kategorinin erişime kapatılması halinde, türüne bakılmaksızın yeni kayıtlı tüm internet sitelerine yapılan istekler engellenecektir. Bu durumda kullanıcılar zararsız ve işleri gereği erişmeleri gereken internet sitesine erişemeyebilmekte, söz konusu kategori tabanlı engellemenin kurbanı olabilmektedir. Bu tür erişimi gerekli olan fakat ulaşılamayan internet siteleri üzerindeki engelin kaldırılması için bilgi teknoloji departmanına fazlaca talep gelebilmektedir. Belirli bir talep sayısının aşılması durumunda ise kullanıcılar kategoriye bakmadan farklı siteler için de erişim isteyebilmektedir. Bu durumda bilgi teknolojilerine gelen talep sayısı katlanarak artmaktadır. Talep sayısı arttıkça, söz konusu taleplerin çözülme süresi uzamakta, kullanıcının bilgi teknolojileri departmanına güveni azalmaktadır.

Bu çalışmada 6000 kurum çalışanının bir yıllık internet aktivitesi incelenmiş olup, kullanıcıların yeni kayıtlı siteler ile etkileşimleri analiz edilmiştir. Kullanıcıların bu tür sitelere erişim sıklıkları, nedenleri ve bu sitelerin engellenmesi durumuna oluşan tepkileri ölçülmeye çalışılmıştır.

Gerçekleştirilen bu çalışma kapsamında kurum kullanıcılarının yeni kayıtlı internet sitelerine erişim istekleri ilk 6 ay boyunca açık bırakılmış, sonraki 6 aylık sürede ise engellenmiştir. Yapılan araştırmalar sonrasında yeni kayıtlı internet siteleri üzerinden toplamda 84419 adet vaka elde edilmiştir. Edinilen bu veri pek çok yönüyle incelenip, kurumların yeni kayıtlı internet sitelerine yönelik olarak ne tür politikalar izlemeleri gerektiği araştırılmıştır.

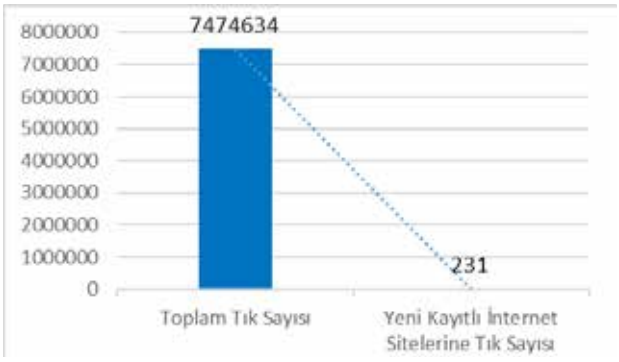
Literatürde yer alan çalışmalar incelendiğinde kurumsal bilgi güvenliğini sağlama üzerine çeşitli çalışmaların gerçekleştirildiği görülmektedir. Özenç tarafından gerçekleştirilen çalışmada; bilgi ve iletişim teknolojilerindeki bilgi güvenliğinin ekonomik boyutu, bilgi güvenliği konusuna Avrupa Birliği' nin hukuki yaklaşımı, Avrupa Birliği' nde güvenlik kültürüne ilişkin politikaların geliştirilmesi gibi konular incelenmiştir [3]. Şahinaslan ve arkadaşları tarafından gerçekleştirilen çalışmada ise; kurumlarda bilgi güvenliği farkındalığının önemine değinilmiş, kurum personellerinin bilgi güvenliği farkındalığını arttırmak amacıyla çeşitli yöntemler önerilmiştir [4]. Vural ve Sağıroğlu tarafından gerçekleştirilen çalışmada ise, kurumsal bilgi güvenliğini sağlamada mevcut bilgi güvenliği standartları ve yeni oluşturulmakta olan bilgi güvenliği standartları detaylı olarak incelenmiştir. Çalışmada ayrıca kurumsal bilgi güvenliğine yönelik güncel tehditlere ve bulgulara da yer verilmiştir [5]. Literatürde yer alan çalışmalar incelendiğinde kurumsal bilgi güvenliği üzerinde yeni kayıtlı internet sitelerinin etkisinin incelendiği bir çalışma bulunmamaktadır. Bu yönüyle bu çalışma, kurumsal bilgi güvenliği açısından özgün bir değer taşımaktadır.

Gerçekleştirilen bu çalışmanın II. bölümünde kurum personelinin yeni kayıtlı internet siteleri ile karşılaşma durumları incelenmiştir. III. bölümde kurum personelinin yeni kayıtlı internet sitelerine erişme amaçları incelenmiş, IV. bölümde ise çalışma kapsamında incelenen veri üzerinde yapılan testler ve elde edilen sonuçlar paylaşılmıştır. V. bölümde ise gerçekleştirilen çalışma, sonuçların sunulması ile tamamlanmıştır.

II. KURUM PERSONELİNİN YENİ KAYITLI İNTERNET SİTELERİ İLE KARŞILAŞMA DURUMLARI

Bu bölümde kullanıcıların, yeni kayıtlı internet siteleri ve tüm internet sitelerine yaptıkları erişim sayıları ve detayları incelenmiştir. Elde edilen bulgular kullanılarak, kullanıcıların yeni kayıtlı internet siteleri ile hangi durumlarda karşılaştıkları yorumlanmıştır.

Şekil 2' de şirket personelinin bir aylık süre içinde erişim isteğinde bulunduğu toplam internet sitesi sayısı ve yeni kayıtlı internet sitesi sayısı gösterilmektedir.



Şekil 2. Kurum personelinin bir ay sürecinde erişim isteğinde bulunduğu toplam internet sitesi sayısı ve yeni kayıtlı internet sitesi sayısı

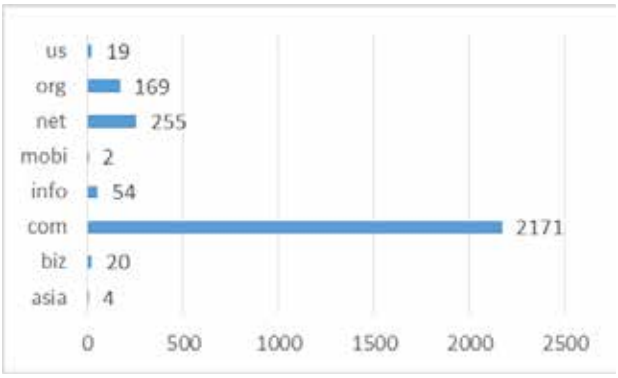
Gösterilen verilere göre kurum personeli ortalama bir günde neredeyse 7.5 milyon internet sitesine erişim isteği yapmaktadır. Yeni kayıtlı internet sitelerine yapılan 231 erişim isteği ise tüm erişim isteklerine oranla çok az bir değere karşılık gel-

mektedir. Bu iki erişim isteği sayısını birbirine oranladığımızda yeni kayıtlı internet sitelerine yönelik erişim isteğinin tüm erişim isteklerine oranı %0.003 olarak karşımıza çıkmaktadır.

Şekil 3'te, bir yıllık süre içinde, en az bir defa yeni kayıtlı internet sitelerine erişim isteğinde bulunan ve yeni kayıtlı internet sitelerine hiç erişim isteğinde bulunmayan kullanıcıların oranı gösterilmiştir. Bu süreçte 6000 kullanıcının %56'sı yeni kayıtlı internet sitelerine en az bir defa erişmeye çalışmıştır. Buna göre; uzun vadede kullanıcılar isteyerek ya da istemeyerek bir şekilde yeni kayıtlı internet siteleri ile karşılaşmaktadır.

Şekil 3. Bir yıl içinde en az bir defa yeni kayıtlı internet sitelerine erişim isteğinde bulunan ve hiç erişim isteğinde bulunmayan kullanıcıların oranı

Şekil 4'te ise, kullanıcıların erişim isteğinde bulunduğu internet sitelerinin uzantılarının oranına yer verilmiştir. Buna göre; kullanıcılar büyük oranda "com" uzantısına ait yeni kayıtlı internet sitelerine erişmeye çalışmış, bunu "net" ve "org" uzantıları takip etmiştir. Devlet sitelerinin "gov" uzantısını, eğitim sitelerinin ise "edu" uzantısını kullanmasından dolayı bu internet siteleri direkt olarak kendi kategori bilgisini almaktadır. Kategori bilgisi girilen siteler yeni kayıtlı internet sitelerine dâhil edilmediği için kullanıcılar herhangi bir devlet veya eğitim sitesinden engellenme yaşamamıştır.

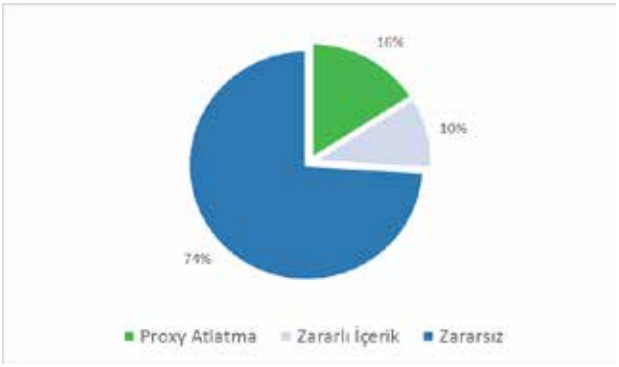


Şekil 4. Kurum personelinin erişim isteğinde bulunduğu internet sitelerinin uzantılarının oranı

III. KURUM PERSONELİNİN YENİ KAYıTLI İNTERNET SİTELERİNİ ZİYARET ETME AMAÇLARI

Kullanıcılar işleri gereği bir internet sitesini ziyaret etmek isteyebilir, mailde kendilerine gönderilen bir linke tıklayabilir ya da engellendikleri siteye alternatif olarak başka bir site arayabilmektedirler. Tüm bu durumlar kullanıcıları yeni kayıtlı internet sitelerine yönlendiren etmenlerdir.

Gerçekleştirilen çalışma kapsamında kullanıcıların yeni kayıtlı internet sitelerine yapmış olduğu erişim isteklerinin kategori üzerinden analizi Şekil 5'de gösterilmiştir.

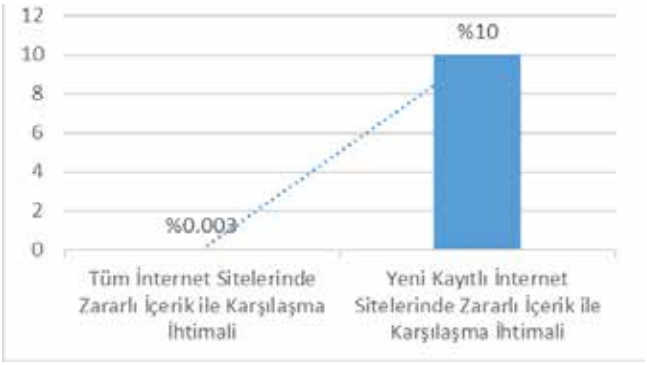


Şekil 5. Kurum personelinin yeni kayıtlı internet sitelerine isteklerin kategorilere göre oranı

Şekil 5' te görüldüğü üzere kullanıcıların erişmeye çalıştığı yeni kayıtlı internet sitelerinin %74'ü zararsız içeriğe sahiptir. Öte yandan erişilmeye çalışılan yeni kayıtlı internet sitelerinin %10'u, içerisinde zararlı yazılım barındırmaktadır. Erişilmeye çalışılan yeni kayıtlı internet sitelerinin %16'sı ise bahis, kaçak yayın ya da yetişkin içeriğine sahiptir ve internet politikası yasaklarını atlatmak için kullanılmaktadır.

Şekil 6. Kurum personelinin yeni kayıtlı internet sitelerine gerçekleştirdiği erişim istek sayıları

Şekil 6 incelenecek olursa; kullanıcılar bir yılda 84419 kez yeni kayıtlı internet sitelerine erişim isteğinde bulunmuşlardır. Yapılan erişim isteklerinin %10'u içerisinde zararlı yazılım barındıran bir yeni kayıtlı internet sitelerine yapılmıştır. Bu oran; 8442 erişim isteğine karşılık gelmektedir. Bu verinin 1 yıllık bir süreçte elde edildiği düşünülürse ortalama bir günde 23 defa içerisinde zararlı yazılım barındıran internet sitesine erişim isteğinde bulunulmuştur.



Şekil 7. Kurum personelinin erişim sağladığı tüm internet sitelerindeki zararlı yazılım oranı ile yeni kayıtlı internet sitelerindeki zararlı yazılım oranı

Şekil 7' de, kullanıcıların tüm internet sitelerinde zararlı yazılım ile karşılama oranı ve yeni kayıtlı internet sitelerinde zararlı yazılım ile karşılaşma oranı gösterilmiştir. Şekle göre kullanıcıların ziyaret ettiği tüm internet siteleri içerisinden yalnızca %0.003' lük kısmı zararlı yazılım barındırmaktadır. Yeni kayıtlı internet sitelerinde ise bu oran %10'a çıkmakta, neredeyse 3000 kat artmaktadır.

Şekil 8. Kurum personelinin kurum internet politikalarını atlatma istekleri

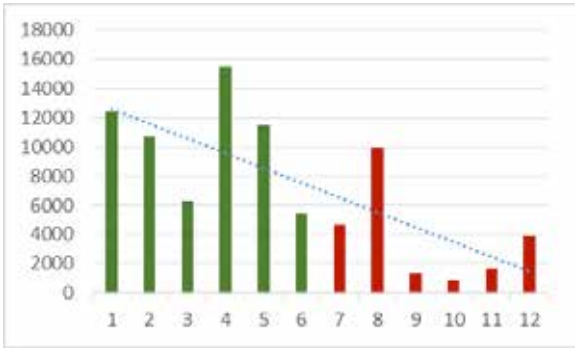
Şekil 8'de gösterildiği üzere bir yılda yeni kayıtlı internet sitelerine yapılan 84419 erişim isteğinin %16'sı kurum internet politikalarını atlatmaya yöneliktir. Bu oran bir yıl içinde bu alanda 13507 erişim isteği yapıldığı anlamına gelmektedir. Bu da ortalama bir günde 37 defa kurum internet yasaklarını atlatmaya yönelik erişim isteği yapılmaktadır.

Şekil 9. Kurum personelinin yeni kayıtlı zararsız internet sitelerine yönelik erişim isteği

Şekil 9' da gösterildiği üzere bir yılda yapılan 84419 yeni kayıtlı internet sitesi erişim isteğinin %74'ü erişime açık olması gereken zararsız sitelere yapmıştır ve bu oran 62470 erişim isteğine karşılık gelmektedir. Eldeki verinin bir yılda elde edildiği düşünülürse, yeni kayıtlı internet siteleri kategorisinden bir günde ortalama 171 erişimi isteğine izin verilmesi gerekilirken, söz konusu istekler engellenmektedir.

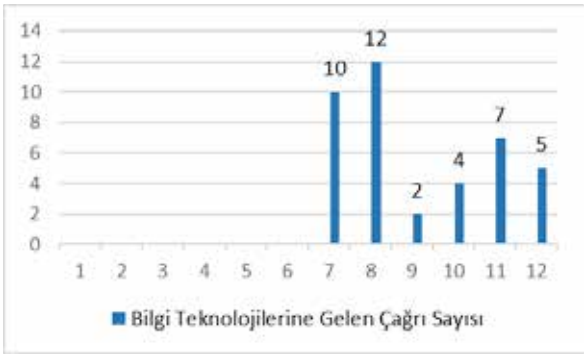
IV. YENİ KAYITLI İNTERNET SİTELERİ ÜZERİNDE DÖNEMSEL ERİŞİM TESTLERİNİN GERÇEKLEŞTİRİLMESİ

Gerçekleştirilen çalışma kapsamında yapılan test işleminde kurum ağından yeni kayıtlı internet sitelerine erişim için 2 farklı senaryo oluşturulmuş ve her iki durum sonunda elde edilen veriler analiz edilmiştir. Oluşturulan senaryoya göre 6 aylığına kurum ağından, yeni kayıtlı internet sitelerine erişim durumu açık bırakılmıştır. İkinci senaryoda ise, sonraki 6 aylık sürede kurum ağından yeni kayıtlı internet sitelerine erişim engellenmiştir. Toplam bir yıllık süreçte kullanıcıların bu internet kategorisine adaptasyonları ve tepkileri ölçülmeye çalışılmıştır.



Şekil 10. Kurum personelinin yeni kayıtlı internet siteleriyle olan etkileşimlerinin ay bazında gösterimi

Şekil 10' da kullanıcıların bir yıllık yeni kayıtlı internet siteleriyle olan etkileşimleri gösterilmiştir. Buna göre ilgili kategorinin kullanıcıların erişimine açık olduğu aylarda yüksek sayıda etkileşim aldığı ve kullanıcılar tarafından yüksek oranda kullanıldığı görülmüştür. İlgili kategorinin erişime kapatıldığı sonraki aylarda ise etkileşim istekleri büyük oranda azaldığı görülmektedir.



Şekil 11. Kurum personelinin erişimin engellendiği yeni kayıtlı internet sitelerinin erişimlerine açılması için oluşturdukları çağrı talepleri

İkinci 6 aylık sürede yapılan engelleme ile kullanıcıların yeni kayıtlı internet sitelerine erişimlerinin kapatılmasıyla, günde ortalama 125 adet kullanıcının erişim isteği engellenmiştir.

Bu denli çok engelleme yapılmasına karşın kullanıcılar tarafından erişim isteği amacıyla açılan çağrı sayısı beklenenin çok altında kalmıştır. Kullanıcıların engellendikleri yeni kayıtlı internet sitelerinin erişimlerine açılması için oluşturdukları çağrı talepleri Şekil 10' da gösterilmiştir.

V. SONUÇ VE DEĞERLENDİRME

Elde edilen veriler ışığında yeni kayıtlı internet siteleri kategorisinin erişime kapatılması ve erişime açık tutulması durumuna incelenmiştir.

Yeni kayıtlı internet sitelerine erişimin açık bırakılması durumlarında;

- Bir günde ortalama bir kullanıcı, içerisinde zararlı içerik bulunan yeni kayıtlı internet sitesine erişecektir. Kullanıcının eriştiği zararlı içeriğe göre olay sonrası müdahale ekibinin hızlı reaksiyon vermesi gerekecektir.
- Bir günde yeni kayıtlı internet sitelerine yönelik ortalama 37 erişim isteği kurum internet politikalarını atlatmak için yapılacaktır. Normalde erişilmemesi gereken bu sitelerin görüntülenmesi kurum kimliğine yakışmayacak durumlar ortaya çıkarabilmektedir.
- Kullanıcılar normalde erişmesi gereken yeni kayıtlı internet sitelerine erişimde sorun yaşamayacaktır. Bu durum kullanıcıların sürekli kısıtlı bir internet politikasında olduğu izlenimini azaltacaktır.

Yeni kayıtlı internet sitelerine erişimin engellenmesi durumlarında;

- Bir günde ortalama 177 erişim isteğine izin verilmesi gerektiği halde, yeni kayıtlı internet sitelerine yönelik olduğu için engellenecektir. Gereksiz yere engellenen kullanıcıların iş aktiviteleri aksayacak, bilgi teknolojilerine bu konuyla ilgili talep açacaklardır. Bilgi teknolojileri departmanı, gelen yeni kayıtlı internet sitesi erişimlerini incelemek için ekstra bir efor sarf etmek zorunda kalacaktır.
- Kullanıcıların kurum internet politikalarını atlatması ciddi derecede zorlaşacaktır.
- %10'luk zararlı içeriğine sahip yeni kayıtlı internet sitelerinden hiçbir kullanıcı enfekte olmayacak, bu kategoriden dolayı olay sonrası müdahaleye gerek kalmayacaktır.

Devlet, eğitim gibi kendine ait site uzantısı olan internet sitelerinin doğrudan kategorize edilmesi ve yeni kayıtlı internet sitelerine dâhil olmaması bu kategoriye erişimi kapatmak isteyen kurumlar için büyük artı sağlamaktadır. Sonuç olarak kategori erişime kapatılsa da kullanıcılar devlet ve eğitim sitelerine problemsiz erişmeye devam edecektir.

Kullanıcılar tarafından yapılan erişim isteklerinin yalnızca %0.003'ünün yeni kayıtlı internet sitelerine yönelik olmasına rağmen bir yıllık süreçte kullanıcıların %56'sı yeni kayıtlı internet siteleri ile etkileşime girmiştir. Kullanıcılar tarafından yapılan erişim istekleri incelendiğinde;

- %74'ünün zararsız sitelere erişmek istediği,
- %10' unun içeriğinde zararlı olduklarını bilmedikleri sitelere erişmek istediği,
- %16' sının ise kurum internet yasaklarını atlatmak için erişmek istediği tespit edilmiştir.

Buna göre kullanıcılar sadece %16'lık bir oranda bu kategoriyi zafiyet olarak kullanmak istemiştir. Geri kalan tüm istekler masum internet siteleri ya da içeriğinde zararlı olduğu bilinmeyen internet sitelerinden oluşmaktadır.

Yapılan tüm bu testlerin sonucunda kullanıcıların yeni kayıtlı internet sitelerine erişimini açık bırakmanın ne denli tehlikeli boyutlara ulaşabileceği, kapatmanın ise kısıtlama ve sonrasında mağduriyet oluşturabileceği gösterilmiştir. Kurumlar bu noktada yeni kayıtlı internet siteleri kategorisinin artılarını ve eksilerini kendi kurumsal politikalarına göre değerlendirmeli ve gerekli düzenlemeleri gerçekleştirmelidir.

KAYNAKLAR

[1]M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a Dynamic Reputation System for DNS". In USENIX Security Symposium, Washington, USA, pp. 273-290, August 2010.

[2]Y. He, Z. Zhong, S. Krasser, and Y. Tang, "Mining DNS For Malicious Domain Registrations". In 6th Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Chicago, USA, pp. 1-6, October 2010.

[3]K. Özenç, "Bilgi Ve İletişim Teknolojilerinde Kişisel Ve Kurumsal Bilgi Güvenliğinin Sağlanması." Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey), Ankara, Türkiye, Ss. 183-190, 13-14 Aralık 2007.

[4]E. Şahinaslan, A. Kantürk, Ö. Şahinaslan, ve E. Borandağ, "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi Ve Oluşturma Yöntemleri". XI. Akademik Bilişim Konferansı, Şanlıurfa, Türkiye, Ss. 605- 610, Şubat 2009.

[5]Y. Vural, Ş. Sağıroğlu, "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt 23, Sayı 2, Ss. 507-522, 2008.

Güvenlik Duvarı Etkinlik Ölçümü
(Firewall Efficiency Measurement)

M. Fikret Ottekin
ICterra Bilgi ve İletişim Teknolojileri San. ve Tic. A.Ş.
Ankara, Türkiye
fikret.ottekin@icterra.com

Abstract

Filtering rules enforced by firewall systems are designated by system administrators. In that context, due to the maintenance agreements between the user and the firewall manufacturer, filtering rules automatically downloaded by the firewall from the manufacturer's database are employed as well. Hence, the overall performance of the firewalls become correlated with the malicious domain detection competence and preferences of the manufacturer company. In this article, a methodology to measure the efficiency of firewalls, utilizing blacklists published by cyber security companies independent from the firewall manufacturer is proposed. Method should be applied with an Intrusion Detection System listening to the target network from multiple points. Successful application of the proposed method would lead to the use of firewall systems with enhanced confidence.

Index Terms

Firewall, filtering rules, measurement, Intrusion Detection System.

Özet

Güvenlik Duvarı sistemleri tarafından uygulanan erişim kontrol kuralları sistem yöneticileri tarafından belirlenir. Bu kapsamda güvenlik duvarı üreticisi firmalarla yapılan bakım anlaşmaları sayesinde firmaların veritabanlarından otomatik olarak indirilen kurallar da kullanılmaktadır. Dolayısı ile güvenlik duvarının performansı, kısmen de olsa üretici firmanın zararlı IP alanları ile ilgili tercihleri ve bu adresleri belirleme konusundaki yetkinliği ile orantılı hale gelmektedir. Bu çalışmada, üretici firmadan bağımsız siber güvenlik firmaları tarafından yayınlanan kara listeleri kullanarak güvenlik duvarının etkinliğini ölçen bir metodoloji tanımlanmaktadır. Güvenliği sağlanacak ağı çok noktadan dinleyen bir Saldırı Tespit Sistemi tarafından çalıştırılması öngörülen metodolojinin başarı ile uygulanması, güvenlik duvarı sistemlerinin çok daha yüksek bir güvenle kullanılmasını sağlayacaktır.

Anahtar Kelimeler

Güvenlik Duvarı, kural listesi, ölçüm, Saldırı Tespit Sistemi.

I. GİRİŞ

Güvenlik duvarları halen en çok kullanılan sınır güvenliği sistemleri arasında yer almaktadır [1]. Kurumsal ağlar ile Internet arasında konuşlandırılarak ağ erişim kontrolünü sağlayan güvenlik duvarlarının kural listelerinin yapılandırılması ile ilgili olarak iki yaklaşım olasıdır:

•Gevşek yaklaşım: "Yasaklanan trafiği tanımla ve engelle, kalan trafiği geçir",

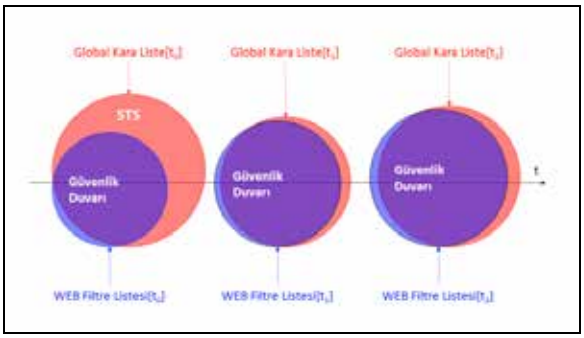
•Sıkı yaklaşım: "İzin verilen trafiği tanımla ve geçir, kalan trafiği yasakla" [2].

Fiili uygulamada güvenlik duvarlarında genellikle bu iki yaklaşımın karmasından oluşan bir durumla karşılaşılmaktadır. Internet ile DMZ arasındaki trafiğin izlenmesi ve engellenmesi sıkı yaklaşımla yapılandırılırken, kullanıcı bilgisayarlarının bulunduğu kurumsal ağ ile Internet arasındaki trafik gevşek yaklaşımla yapılandırılmaktadır. Bu durum, kullanıcı bilgisayarlarına WEB'in engellenen alanlar haricinde her yerine bağlantı kurma olanağını vermekte, kullanıcıları pek çok farklı saldırı türüne açık hale getirmektedir. Dolayısı ile güvenlik duvarı tarafından engellenmesi gereken zararlı IP alanlarının devamlı olarak güncellenmesi gerekmektedir. Ancak pek çok kurum ve kuruluş bu işi hakkıyla yapacak insan kaynağına ve prosedüre sahip değildir. Internet ile kurumsal ağlar arasında akan trafiğin yönetilmesi kapsamında genellikle güvenlik duvarı ile birlikte alınan ve güvenlik duvarı platformunda çalışan "WEB filtreleme" modülü ve bakım hizmetinden faydalanılmaktadır. Güvenlik duvarı üreticisi firma tarafından belirlenen ve sistem yöneticisinin tercihi ile etkinleştirilen "Terör", "Kumar", "Ekstremizm", "Zararlı madde satışı", "Proxy" vb. kategorilerdeki kurallar aracılığı ile kurum içinden Internet'e yapılmaya çalışılan erişimler engellenmektedir. Güvenlik duvarları periyodik olarak geliştirici firma veritabanına bağlanarak engellenecek kategorilere ait en güncel WEB filtreleme listelerini alıp kullanarak bu işlevi gerçekleştirmektedir. Böylece en önemli sınır güvenliği sistemlerinden biri olan güvenlik duvarlarının yönetilmesi konusunda yetki önemli ölçüde üretici firmaya geçmektedir.

Yukarıda sayılan kategorilerde siber uzayda faaliyet gösteren pek çok grup veya örgüt mevcut olduğundan bunların izlenmesi ve tespiti kurumsal siber güvenliğin kapsamını gerçekten aşan bir iştir. Ancak güvenlik duvarının izlenmesi, performansın ölçülmesi ve iyileştirme yollarının araştırılması kurumsal olanaklarla yapılabilir.

Güvenlik duvarlarının hızla yer ve yöntem değiştiren saldırganlara karşı ne kadar etkin koruma sağladığı belirsizdir. Esasen siber uzayda faaliyet gösteren saldırganların etkinliği de WEB filtreleme listesi de zaman içinde değişmektedir (Şekil-1). Herhangi bir t0 anında saldırganları karşılama ve engelleme

konusunda etkili olan filtreleme listesini üreten firmanın, iki hafta, iki ay veya iki yıl sonra da aynı başarıyı göstereceğinin garantisi yoktur. Dolayısı ile güvenlik duvarı etkinliğinin, filtreleme listesi bakımı hizmetini sağlayan firmadan bağımsız kuruluşlar tarafından üretilen saldırgan bilgileri kullanılarak izlenmesi son derece faydalı olacaktır.



Şekil. 1. Güvenlik Duvarı WEB filtre listesinin ve STS kara listesinin zaman içinde değişimi.

Güvenlik duvarı performansından genellikle iletim hızı, desteklenen paralel oturum sayısı gibi ağa ilişkin parametreler anlaşılmaktadır [3], [4]. Güvenlik duvarı kural listesi uzunluğunu optimize ederek performansı yükseltmeyi hedefleyen çalışmalar da yapılmıştır [5]. Bu makaledeki çalışma ise güvenlik duvarı WEB filtreleme listesinin kapsayıcılığını ve etkinliğini izleyerek performansı ölçmeyi hedeflemektedir.

İzleyen bölümlerde çok portlu bir saldırı tespit sistemi ve üretici firmadan bağımsız siber güvenlik firmaları tarafından üretilen kara listeler kullanılarak (bu çalışmanın geri kalanında "Bağımsız kaynaklardan alınan IP kara listeleri" olarak adlandırılacaktır) ve güvenlik duvarından geçen ağ trafiği izlenerek güvenlik duvarı etkinliğinin ölçülmesi ve sınır güvenliğinin iyileştirilmesi için kullanılabilecek bir metod önerilmektedir. Metod dört bölümde açıklanacaktır:

1.Bağımsız kaynaklardan IP kara listelerinin toplanması ve işlenmesi

2.Çok portlu saldırı tespit sisteminin kurum ağında konuşlandırılması

3.Etkinlik ölçümü

a.Güvenlik Duvarını aşarak "bilinen saldırganlar" ile kurum bilgisayarları arasında akan trafiğin izlenmesi

b.Güvenlik Duvarının istenmeyen trafiği engelleme etkinliğinin belirlenmesi

4.Güvenlik Duvarında ve kurum bilgisayarlarında yapılması gereken iyileştirmeler

II. BAĞIMSIZ KAYNAKLARDAN ALINAN IP KARA LİSTELERİ

Saldırı Tespit Sistemi (STS), güvenlik duvarı etkinliğini ölçmek için çalıştırılırken bağımsız kaynaklardan alınan IP kara listelerinden faydalanacaktır. USOM zararlı bağlantılar listesine [6] benzer şekilde, pek çok yabancı kaynak sık sık güncellenen IP kara listeleri yayınlamaktadır [7], [8]. STS düzenli aralıklarla bu kaynaklara bağlanacak ve kaynaklar tarafından yayınlanan listeleri kullanarak kendi IP kara listesini oluşturacaktır.

Farklı kaynaklardan alınan listeler değerlendirilirken çeşitli yöntemlerden biri tercih edilebilir. Örneğin, kara listeler hiç bir işleme tabii tutulmadan birleştirilebileceği gibi sadece kara listelerin tamamında veya birkaç tanesinde yer alan IP adreslerinden oluşan bir kara liste de üretilebilir.

Giriş bölümünde "Bilinen Saldırganlar" olarak atıf yapılan, üçüncü tarafların IP adreslerinden oluşan ve birleştirme işleminin ardından elde edilen IP adresleri seti, bu makalenin geri kalanında "Kara Liste" olarak adlandırılacaktır.

Kara Listenin asli özelliği saldırganlar tarafından kullanılma olasılığı yüksek olan bilgisayarların adreslerini içermesidir. Bu listeye bağımsız kaynaklardan alınan adreslere ilave adresler de eklenebilir. Örneğin, farklı ağlarda konuşlu STS'ler tarafından tespit edilen imza tabanlı saldırıların yapıldığı bilgisayarların adresleri de Kara Listeye eklenebilir.

Kara Liste, kurumsal ağ ile dış dünya arasında akan trafiğin değerlendirilmesi kapsamında referans olarak kullanılacaktır. Dolayısı ile Kara Liste'nin olabildiğince çok sayıda ve birbirinden bağımsız kaynaktan toplanan bilgilerden oluşturulması etkinlik ölçümü açısından önem arz etmektedir.

III. SALDIRI TESPİT SİSTEMİNİN KURUM AĞINDA KONUŞLANDIRILMASI

Sınır güvenliği sistemlerinin kurumsal ağlarda konuşlandırılması ile ilgili olarak bilinen pek çok topoloji mevcuttur [9]. Kurumsal ağın birden çok noktadan, çok sayıda gerçek veya sanal sensör ile izlenmesi de halen bilinen bir uygulamadır [10].

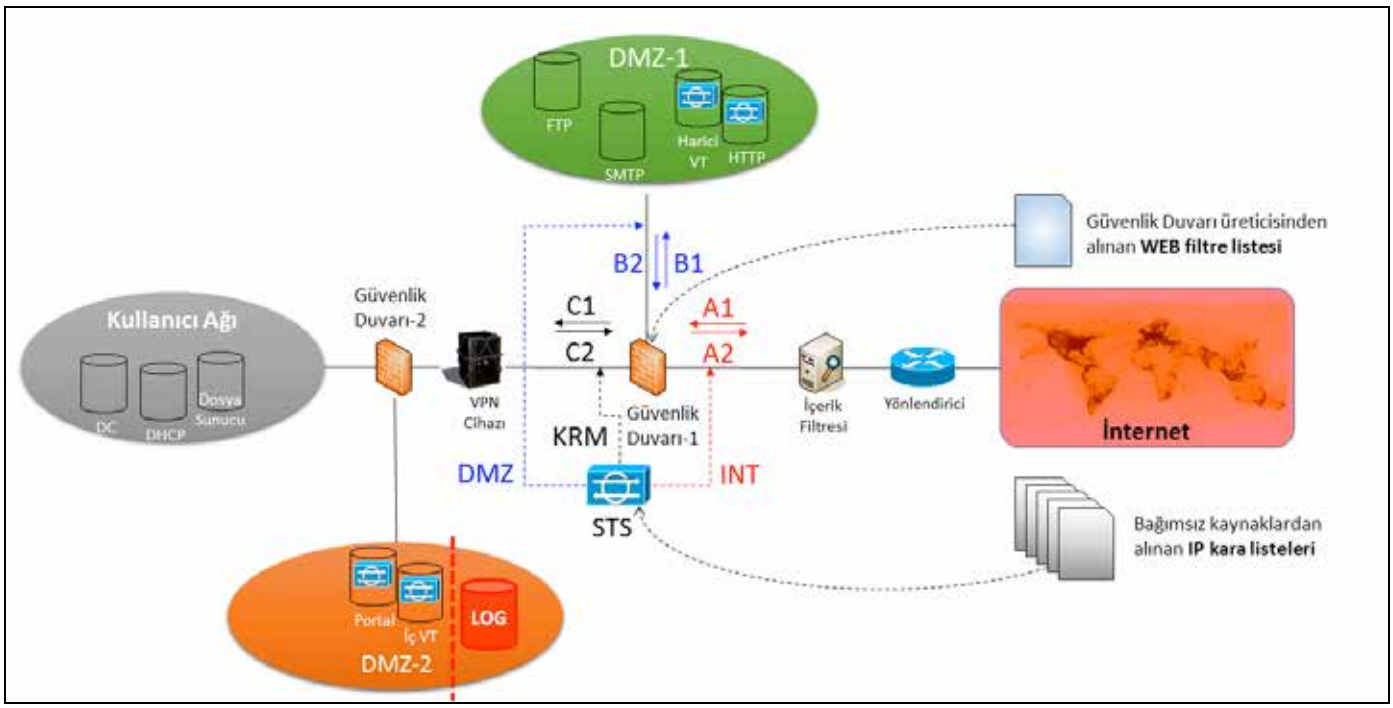
Bu çalışmada, STS'nin kurumsal ağda konuşlandırılması konusunda Şekil-2'de gösterilen temel ağ topolojisi üstünde çalışılacaktır. Bu makalenin geri kalanında kullanılan "Güvenlik Duvarı" ifadesi ile kastedilen ve etkinliği ölçülen, Şekil-2'deki "Güvenlik Duvarı-1"dir.

STS'nin Şekil-2'de gösterilen topolojide üç port ile izleme yapması önerilmektedir.

•İlk portun Internet hattı ile Güvenlik Duvarı arasındaki trafiği,

•İkinci portun Güvenlik Duvarı ile DMZ-1 arasındaki trafiği,

•Üçüncü portun ise Güvenlik Duvarı ile Kullanıcı Ağı ve DMZ-2 arasındaki trafiği izleyecek şekilde konuşlandırılması gerekmektedir.



Şekil. 2. Kurumsal Ağ Topolojisi ve Çok Portlu Saldırı Tespit Sistemi

Bu portlar sırası ile INT, DMZ ve KRM portları olarak adlandırılacaktır. Kurumun İnternet erişimine açık birden fazla DMZ kullanması halinde aynı metodoloji kullanılarak dört veya daha fazla noktadan da izleme yapılabilir.

Üç portun her birinden okunan trafiğin "kuruma gelen trafik" ve "kurumdan çıkan trafik" şeklinde ikiye ayrılarak incelenmesi, dolayısı ile altı farklı paket dizisi üstünde çalışılması gerekecektir.

Bu bağlamda STS portlarından okunan trafiğin Kaynak IP adresleri ve Hedef IP adreslerinde bulunan bilgi Tablo-1'de özetlenmiştir.

TABLO I. STS TARAFINDAN İZLENEN PAKET DİZİLERİ VE IP ADRESLERİ

Port	Paket Dizisi	Kaynak IP Adresi	Hedef IP Adresi
INT	A1. Internet'ten gelen trafik	Saldırgana ait olabilecek kurum dışı bilgisayar adresi	Güvenlik Duvarı dış IP adresi *(NAT'lanmış* kullanıcı bilgisayarı adresi veya DMZ-1 sunucu adresi)
DMZ	B1. DMZ-1'e gelen trafik		DMZ-1'de bulunan sunucu adresi
KRM	C1. Kurumsal ağa gelen trafik		Kullanıcı bilgisayarı adresi
INT	A2. Internet'e giden trafik	Güvenlik Duvarı dış IP adresi (NAT'lanmış kullanıcı bilgisayarı adresi veya DMZ-1 sunucu adresi)	Saldırgana ait olabilecek kurum dışı bilgisayar adresi
DMZ	B2. DMZ-1'den giden trafik	DMZ-1'de bulunan sunucu adresi	
KRM	C2. Kurumsal ağdan giden trafik	Kullanıcı bilgisayarı adresi	

Şekil-2 ve Tablo-1 göz önünde bulundurularak aşağıdaki çıkarımlar yapılabilir:

1.Kuruma gelen trafikte (A1, B1 ve C1 dizileri) Kaynak IP adresleri, kurumdan çıkan trafikte ise (A2, B2, ve C2 dizileri) Hedef IP adresleri kurum bilgisayarlarının dış dünyada iletişim halinde olduğu bilgisayarların adreslerini vermektedir. Bu adresler Kara Liste ile karşılaştırılacaktır.

2.Hemen her kurum tarafından kullanılan NAT ("Network Address Translation") mekanizması, sadece A1 ve A2 dizilerindeki paketler incelenerek Internet ile bağlantı halinde olan kurumsal kullanıcı bilgisayarlarının belirlenmesini güçleştirmektedir [11].

3.A1, B2 ve C2 dizilerinde Kara Liste'de bulunan IP adreslerinin tespit edilmesi, kurumsal bilgisayarların Kara Liste'de bulunan bilgisayarlarla iletişim halinde olduğunu veya iletişime geçmeye çalıştığını gösterir. Bu trafik Güvenlik Duvarı tarafından engellenecek bile olsa, kurumsal bilgisayarlara kötücül yazılımların büyük olasılıkla yerleştiği anlamına gelmektedir.

4.A2, B1 ve C1 dizilerinde Kara Liste'de bulunan IP adreslerinin tespit edilmesi, hem kurumsal bilgisayarların Kara Liste'de bulunan bilgisayarlarla iletişim halinde olduğunu, hem de Güvenlik Duvarı'nın bu trafiği engellemediğini gösterdiğinden kurumsal güvenlik açığının mevcut olduğu ve tehdit ajanları tarafından kötüye kullanıldığı anlamına gelmektedir. Kurum açısından en büyük riski arz eden durum budur.

IV. ETKİNLİK ÖLÇÜMÜ

Güvenlik Duvarı etkinliği, belli zaman aralıklarında akan trafiğin izlenmesi ve trafiği oluşturan paketlerin incelenmesi sonucunda, zaman aralıklarının sonunda hesaplanacaktır.

Etkinlik ölçümünün yapıldığı zaman aralıklarında *STS, A1, B1*

ve *C1* paket dizilerinde yer alan her paketin kaynak *IP* adresini, *A2, B2* ve *C2* paket dizilerinde yer alan her paketin ise hedef *IP* adresini "Kara Liste"de arayacaktır.

A1n, B1n ve *C1n* parametreleri, sırası ile *A1, B1* ve *C1* dizilerindeki paketlerden, Kaynak *IP* adresi kara listede bulunduğu *STS* tarafından belirlenen paketlerin sayısını belirtir.

A2n, B2n ve *C2n* parametreleri ise, sırası ile *A2, B2* ve *C2* dizilerindeki paketlerden, Hedef *IP* adresi kara listede bulunduğu *STS* tarafından belirlenen paketlerin sayısını belirtir.

Bu durumda, gözlemin yapıldığı zaman aralığında Güvenlik Duvarına ait

GeTrEn ("Gelen Trafik Paket Engelleme Etkinliği") =(A1n – (B1n + C1n)) / A1n, (1)

GiTrEn ("Giden Trafik Paket Engelleme Etkinliği") = ((B2n + C2n) – A2n) / (B2n + C2n), (2)

ToTrEn ("Toplam Trafik Paket Engelleme Etkinliği") = ((A1n + B2n + C2n) – (A2n + B1n + C1n)) / (A1n + B2n + C2n) (3)

olacaktır.

Gelen trafik kapsamında A1n'in, giden trafik kapsamında *(B2n + C2n)*'in, toplam trafik kapsamında ise *(A1n + B2n + C2n)*'in gözlemin yapıldığı zaman aralığında "sıfır" olarak ölçülmesi mümkündür. Bu durumda Güvenlik Duvarının engellemesi gereken trafik tespit edilemediğinden, etkinlik ölçümünün yapılması da söz konusu olmayacaktır (Yukarıdaki formüllerde "sıfır ile bölme hatası" ortaya çıkacaktır).

Etkinlik ölçümü yapılırken paket sayısı yerine toplam veri uzunluğu da kullanılabilir. Bu durumda,

A1k, B1k ve *C1k* parametreleri, *STS* tarafından Kaynak *IP* adresi kara listede bulunduğu belirlenen paketlerin uygulama katmanı yüklerinin toplam uzunluğunu, yani kurum bilgisayarlarına iletilen toplam kötücül veri/dosya/komut uzunluğunu belirtir.

A2k, B2k ve *C2k* parametreleri ise *STS* tarafından Hedef *IP* adresi kara listede bulunduğu belirlenen paketlerin uygulama katmanı yüklerinin toplam uzunluğunu, yani kurum bilgisayarlarından gönderilmek üzere olan toplam veri/dosya/mesaj uzunluğunu (spam e-posta ve eki, sızdırılan veri, Botnet *C/C* merkezine gönderilen yanıtlar vb.) belirtir.

Bu durumda, gözlemin yapıldığı zaman aralığında Güvenlik Duvarına ait

GeTrEk = ("Gelen Trafik Veri Engelleme Etkinliği") = (A1k – (B1k + C1k)) / A1k (4)

GiTrEk = ("Giden Trafik Veri Engelleme Etkinliği") = (A1k – (B2k + C2k)) / A1k (5)

ToTrEk ("Toplam Trafik Veri Engelleme Etkinliği") = ((A1k + B2k + C2k) – (A2k + B1k + C1k)) / (A1k + B2k + C2k) (6)

GeTrEn, GiTrEn, ToTrEn, GeTrEk, GiTrEk, ToTrEk ϵ *[0,1]*

olacaktır.

Etkinlik parametreleri oran gösterdiğinden 0 ile 1 arasında gerçek sayılardır. Etkinliğin "sıfır" olarak ölçülmesi Güvenlik Duvarı'nın Kara Liste'den gelen trafiği engelleme konusunda tamamen etkisiz, "bir" olarak ölçülmesi ise tamamen etkili olduğunu gösterecektir.

Engelleme etkinliklerinin daha da çeşitlendirilmesi mümkündür. Örneğin, kara listede adresi yer alan (bilinen saldırganların kullandığı) bilgisayarlarla gerçekleşen iletişim yerine bilinen saldırı imzalarını içeren paketlerin ne kadarının engellendiği ölçülebilir.

Etkinlik ölçümünün doğru şekilde yapılması için dikkat edilmesi gereken en önemli husus, sensörler arası zaman senkronizasyonudur. Yukarıda tanımlanan A*, B* ve C* parametrelerinin aynı zaman aralığında hesaplanması, sonuçların doğruluğu açısından önem arz etmektedir. Zaman senkronizasyonunun tam olarak sağlanması halinde bile Güvenlik Duvarının işlem süresi dolayısı ile bazı paketlerin kaybolmuş gibi gözükmesi ve Güvenlik Duvarı tarafından engellenmediği halde engellenmiş gibi gözükmesi olasıdır. Bu durumda etkinlik ölçümü, bazı zaman aralıklarında gerçek etkinlikten daha yüksek, takip eden zaman aralığında ise gerçek etkinlikten daha düşük hesaplanabilir. Zaman aralığının uzatılması halinde problem büyük ölçüde azalacaktır.

Güvenlik Duvarı etkinliğinin zaman içindeki seyri izlenerek, henüz Güvenlik Duvarı kural listesine girilmemiş saldırgan adreslerinden kurum ağına yapılan erişim denemelerinin yoğunluğundaki değişim gözlenebilir.

V. İYİLEŞTİRME ÇALIŞMALARI

Bir önceki bölümde de belirtildiği gibi, A2, B1 ve C1 dizilerinde Kara Liste'de bulunan IP adreslerine raslanması, kurumsal güvenlik açığının mevcut olduğu, daha doğrusu Güvenlik Duvarında kural listesi ve WEB filtreleme listesinden oluşan bütünün güncel olmadığı anlamına gelmektedir.

Hem bu dizilerde, hem de "Kara Liste"de yer alan adresler, kurum bilgisayarları ile aralarında gerçekleşen trafikteki paket sayısı ve/veya toplam veri hacmi büyüklüğüne göre sıralanabilir. Gerçekleşen sıralama göz önünde bulundurularak belirlenen adreslerin Güvenlik Duvarı kural listesine eklenmesi ve engellenmesi yerinde olacaktır.

İkinci olarak, kara listedeki bilgisayarlarla iletişime geçen kurum bilgisayarlarının belirlenmesi ve bu bilgisayarlarla saldırganlar arasında gerçekleşen iletişimden kaynaklanan sorunların (AV taraması, formatlama vb. işlemlerle) düzeltilmesi gerekecektir.

Kara listedeki bilgisayarlarla iletişime geçen kurum bilgisayarları şunlardır:

1.B1 ve C1 paket dizilerinde, Kaynak IP Adresi Kara Liste'de bulunan paketlerin, Hedef IP adresini kullanan kurum bilgisa-

yarları (sunucular ve kullanıcı bilgisayarları).

2.A2 paket dizisinde, Hedef IP Adresi Kara Liste'de bulunan paketlerin, Kaynak IP adresini kullanan kurum bilgisayarları. Güvenlik duvarında muhtemelen çalıştırılmakta olan NAT mekanizması dolayısı ile hangi kurum bilgisayarı olduğu doğrudan anlaşılamayacaktır. Kullanıcı bilgisayarını tam olarak tespit etmek için NAT kayıtları veya gözlemin yapıldığı zaman aralığında kaydedilen B2 ve C2 paket dizileri ile korelasyon sağlanması gerekecektir.

Yukarıda tanımlanan metodoloji kullanılarak yapılan izleme sonucunda Tablo-2'de gösterilene benzer bir sonuç oluşabilir:

TABLO II. GÜVENLİK DUVARI ETKİNLİĞİ İZLEME BULGULARI

Sıra no.	İç (Kurumsal IP) Adresi	Dış (Kara Liste) IP Adresi	Güvenlik Duvarı Kural Listesinde ve/veya WEB filtreleme listesinde	Engellenen Paket Sayısı	Geçen Paket Sayısı
1	148.15.62.11	81.88.178.14	VAR	32345	0
2	148.15.62.13	81.88.178.14	VAR	31876	0
3	172.25.65.76	199.23.65.11	VAR	1455	0
4	172.25.65.93	204.15.77.23	YOK	0	2208
5	172.25.65.95	213.44.18.2	YOK	0	11452
-	Güvenlik Duvarından geçen Kara Liste paket sayısı *(A2n + B1n + C1n)*			-	13660
-	Güvenlik Duvarına gelen Kara Liste paket sayısı *(A1n + B2n + C2n)*			79336	
-	Engellenen Kara Liste paket sayısı *((A1n + B2n + C2n) - (A2n + B1n + C1n)) / (A1n + B2n + C2n)*			65676	-
-	**ToTrEn ("*Toplam Trafik Paket Engelleme Etkinliği*")**			**0,82782 (%82,8)**	

Yukarıdaki tablodaki parametrelerden ToTrEn ana gösterge olmakla birlikte, bu parametrenin Güvenlik Duvarına gelen Kara Liste paket sayısı (A1n + B2n + C2n) ile birlikte değerlendirilmesi gerektiği unutulmamalıdır. ToTrEn, toplam paket sayısının çok düşük olduğu durumlarda, yüksek olduğu durumlardaki kadar anlamlı olmayacaktır.

Kaynak kısıtı vb. nedenlerle STS ile üç portlu izlemenin mümkün olmadığı, ancak iki portlu izlemenin yapılabileceği durumlarda, bu makaledeki topolojide etkinlik ölçümü yapılamayacaktır (Güvenlik Duvarının iki portlu olarak kulanıldığı durumda etkinlik ölçümü yapılabilir). Güvenlik Duvarı etkinlik ölçümü yapılamasa da, STS B* ve C* paket dizilerinin izlenebileceği DMZ ve KRM portlarına bağlanabilir. Bu durumda, Kara Liste ile konuşmaya çalışan kurum bilgisayarlarının hangileri olduğu, herhangi bir korelasyon çalışması yapılmadan bu paket dizilerinden belirlenebilecek ve bu bilgisayarlarla ilgili düzeltici önlemler devreye sokulabilecektir.

VI. SONUÇ

Güvenlik Duvarı sisteminin zaman zaman kurum ağına yapılan kötü niyetli erişimleri engelleme konusunda düşük performans göstermesi mümkündür. Bu çalışmada tarif edilen etkinlik ölçüm metodolojisi aracılığı ile çok portlu bir STS kullanılarak kurumsal Güvenlik Duvarı'nın Kara Liste trafiğini engelleme etkinliği ölçülmektedir. Ölçüm metodolojisinin merkezinde, Güvenlik Duvarı üreticisinden bağımsız kuruluşlar tarafından üretilen verilerden oluşturulan Kara Liste yer almaktadır.

Güvenlik Duvarı etkinliği, Güvenlik Duvarı'na tüm portlardan giren ve çıkan trafiğin Kara Liste göz önünde bulundurularak ve bu makalede tarif edilen metodoloji kullanılarak değerlendirilmesi sonucunda ölçülmektedir. Kara Listede bulunan adreslerle iletişime izin vermesi Güvenlik Duvarı etkinliğinin düşük, izin vermemesi ise etkinliğin yüksek olduğunu göstermektedir. Bu parametrenin sistem yöneticileri tarafından izlenmesi, Güvenlik Duvarı etkinliğinde gerçekleşen düşüş ve yükselişlerin algılanmasını sağlayarak kuruma bu sorunla ilgili düzeltici/önleyici faaliyetlerin gerçekleştirilmesi gerektiğini anımsatabilir.

Dolayısı ile çok portlu bir STS'nin bu metodolojiyi çalıştıracak uygulama yazılımı ile donatılması, yapılandırılması ve kurum ağında konuşlandırılması, WEB filtreleme hizmeti veren firmanın performansı ve Güvenlik Duvarının etkinliği ile ilgili fikir vererek, sistemin çok daha bilinçli bir şekilde kullanılmasını sağlayacaktır.

TEŞEKKÜR

Yazar, bildirinin hazırlanmasını destekleyen ICterra Bilgi ve İletişim Teknolojileri A.Ş.'ye teşekkürlerini sunar.

Yazar, bildiriye konu olan "Güvenlik Duvarı Etkinlik Ölçümü" metodu ile çözümlenmeye çalışılan ihtiyacın belirlenmesine ve Global Kara Listelerle ilgili çalışmaların başlamasına vesile olan "Yeni Nesil Akıllı Tehdit Algılama ve Engelleme Siber Güvenlik Sistemi (ATES)" projesini destekleyen TÜBİTAK Sanayi Ar-Ge Projeleri Destekleme Programı'na teşekkürlerini sunar.

KAYNAKLAR

[1] T. Grudziecki, P. Jacewicz ve J. Łukasz, «Proactive Detection of Security Incidents,» ENISA, Heraklion, 2012.

[2] R. Contreras, «Best practices for firewall rules configuration,» 20 06 2016. [Çevrimiçi]. https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/. [Erişildi: 23 6 2017].

[3] D. Newman, «RFC 2647 Benchmarking Terminology for Firewall Performance,» 8 1999. [Çevrimiçi]. Available: https://tools.ietf.org/html/rfc2647. [Erişildi: 23 6 2017].

[4] B. Hickman, D. Newman, S. Tadjudin ve T. Martin, «RFC 3511 Benchmarking Methodology for Firewall Performance,» 4 2003. [Çevrimiçi]. Available: https://tools.ietf.org/html/rfc3511. [Erişildi: 23 6 2017].

[5] E. W. Fulp ve S. J. Tarsa, «Methods, Systems and Computer Program Products for Network Firewall Policy Optimization». Patent: EP 1 864 226 B1, 15 5 2013.

[6] «Zararlı Bağlantılar,» USOM, TR-CERT, [Çevrimiçi]. https://www.usom.gov.tr/zararli-baglantilar/1.html. [Erişildi: 2017 6 15].

[7] «abuse.ch SSL IPBL for Suricata / Snort,» [Çevrimiçi]. https://sslbl.abuse.ch/blacklist/sslipblacklist.rules. [Erişildi: 19 6 2017].

[8] «DShield.org Recommended Block List,» [Çevrimiçi]. Available: https://www.dshield.org/block.txt. [Erişildi: 17 6 2017].

[9] K. Stouffer, V. Pillitteri ve S. Lightman, «5.5 Network Segregation,» Guide to ICS Security, Gaithersburg, National Institute of Standards and Technology, 2015, sf. 55-61.

[10] «Decide where to deploy Sensors and in what operating mode,» McAfee Network Security Platform 8.3, IPS Administration Guide Revision H, Intel Security, 2017, sf. 48-49.

[11] «Firewalls and Network Address Translation (NAT),» [Çevrimiçi]. Available: https://notes.shichao.io/tcpv1/ch7/. [Erişildi: 23 6 2017].

Ağda Anomali Tespiti
Anomaly Detection in a Network

Ebubekir BÜBER
Bilgisayar Mühendisliği Bölümü
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
ebubekirbbr@gmail.com

Ozgur Koray SAHINGOZ
Bilgisayar Mühendisliği Bölümü
Hava Harp Okulu
İstanbul, Türkiye
sahingoz@hho.edu.tr

Özet

Bilgisayar teknolojisinin ve sistemlerin çok hızlı bir şekilde gelişmesi global internete bağlı bilgisayarları çok değişik türde saldırılara açık bırakmaktadır. Bilinen türde saldırılara karşı önlem almak kolayken bilinmeyen tür saldırılara karşıda ağ trafiğindeki anormalliklerin belirlenerek önlem alınması gerekmektedir. Bu bildiride ikinci türden olan anomali tabanlı saldırı tespiti üzerinde durulmuş olup bir anomali tabanlı saldırı tespit sisteminin geliştirilmesinde ihtiyaç duyulabilecek temel kavramlar açıklanarak örneklenmiştir.

Anahtar Kelimeler

Anomali Tespiti, Saldırı Tespit Sistemleri, İmza tabanlı Saldırılar, Değerlendirme Kriterleri

I. GİRİŞ

Bilgi teknolojilerinin gelişmesi ile birlikte bilgisayar güvenliği, insanların günlük yaşantısında oldukça önemli yer tutmaya başlamıştır. Bilgisayar sistemlerinin artan bir şekilde kullanılmasıyla, bu sistemlere yönelik yapılan saldırılar da her geçen gün artmaktadır. 2017 yılında yayımlanan Symantecs Internet güvenlik Tehdidi Raporuna göre 2016 yılında saldırıların %53 lük Spam mail oranına, 1/2596'lık bir oltalama saldırı oranı, 1/131'lik bir kötü amaçlı yazılım oranına ulaştığını ifade edilmektedir [1].

Gelişen teknoloji ile dünyada internet kullanımı oldukça yaygınlaşmaya başlamıştır. 2016'da dünya nüfusunun %46'sı (3,4 milyar kullanıcı) internete erişim gerçekleştirmektedir [2]. Günümüzde bir kişinin, birden fazla internete bağlı cihaza sahip olduğu düşünülürse internete bağlı cihaz sayısının, internet kullanıcı sayısından çok daha fazla olduğu anlaşılacaktır. Aynı zamanda gelişen bulut teknolojisi sayesinde birçok insan, kişisel bilgilerini sanal ortamlarda saklamaya başlamıştır. Bu nedenle, internet kullanımının yaygınlaşmasına paralel olarak internete yüklenen bilgilerin güvenliği de büyük önem kazanmıştır. Siber güvenlik kavramı olarak tabir edilen bu konu, günümüzde çokça araştırma yapılan bir alan olarak karşımıza çıkmaktadır.

İlerleyen bilgisayar ağı teknolojileri ile birlikte; spam tehditleri, saldırganlar ve zararlı organizasyonların sayısında büyük bir artış yaşanmaktadır. Saldırı Tespit Sistemleri) ve Güvenlik Duvarı teknolojileri ile bu tehditlerin bazıları önlenebilmektedir. Güvenlik Duvarı, bir sisteme internet üzerinden bağlanan kişilerin, sisteme girişini kısıtlayan/yasaklayan ve genellikle bir Internet Gateway Servisi (ana internet bağlantısını sağlayan servis) olarak çalışan bir bilgisayar ve üzerindeki yazılıma verilen genel addır.

Saldırı Tespit Sistemleri (STS), bir veri paketinin bir saldırı paketi olup olmadığını, anlayıp bu işlemin sonucuna göre bazı tedbirler alabilen sistemlere verilen addır. STSler çalışma mantığına göre ikiye ayrılır; İmza Tabanlı Saldırı Tespit Sistemleri (İT-STS) ve Anomali Tabanlı Saldırı Tespit Sistemleri (AT-STS).

İT-STS'leri bilinen zafiyetlere yönelik imzalar kullanarak çalışmaktadır. İmzalar, saldırı tiplerine dair detaylı bilgiler içermektedir. Bu tip sistemler bilinen saldırı tiplerini tanımada oldukça başarılıdır. Ancak bilinmeyen saldırıları ve olası anomalileri tespit etmekte yetersiz kalmaktadırlar. Bu nedenle yeni tespit edilen bir atak türünün tanınabilmesi için o atağa ait imzanın oluşturulup sisteme tanıtılması gerekmektedir. Gerçekleştirilen saldırıların önemli bir çoğunluğunun bilinmeyen saldırlar olduğu günümüzde, bu tip STS'lerin; kurulum, bakım ve idameleri çok masraflı olmaktadır [3].

AT-STS'leri ise, bilinmeyen saldırıları ya da Sıfırıncı Gün olarak bilinen saldırıları tespit edebilme yeteneğine sahip STS'lerdir. Ancak bu tip STS'ler, çok sayıda Yanlış Alarm (False Alarm) verebilmektedir. Son yıllarda, Anomali-Tabanlı STS'ler için Yanlış Alarm oranını düşürerek aynı zamanda başarıyı artırma üzerine çalışmalar yapılmaktadır.

İmza Tabanlı yaklaşımlar veya kural tabanlı yaklaşımlar gerek saldırganlar tarafından gerekse sistem yöneticileri tarafından bilinmektedir. Bu gibi yaklaşımlar daha önceden bilinen saldırı türlerini engellese de önceden karşılaşılmayan saldırılar bilgisayar ağlarına çok ciddi hasar verebilmektedir. Bu nedenle bu bildiride bilinen türdeki saldırıların tespit edilmesinden ziyada daha önceden bilinmeyen tipten saldırıların anomali tespiti yöntemleri ile yakalanması yolundaki yaklaşımlar ve yapılması gerekenler açıklanarak konu üzerindeki araştırmacılara bir kaynak teşkil edilmesi amaçlanmıştır.

Bildirinin kalan kısmı şu şekilde organize edilmiştir. İkinci bölümde konu hakkındaki gerekli terminolojik tanımlamalar yapılmış ve izah edilmiştir. Sonraki bölümde anomali tespit aşamaları, kullanılan veri setleri ile birlikte detaylandırılmıştır. Dördüncü bölümde bu alanda kullanılan yaklaşımlar sınıflandırılmış ve örneklendirilmiş olup, devam eden bölümde kullanılan sistemin geçerlilik ölçütleri tanımlanmış olup son bölümde sonuç ve öneriler yapılmıştır.

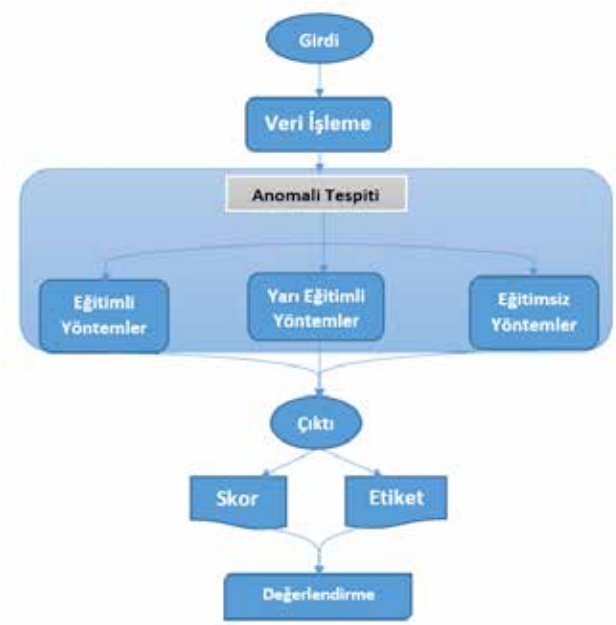
II. ANOMALİ TESPİTİ TERMİNOLOJİSİ

Kullanıcıların bir ağ üzerindeki günlük işlemleri genellikle benzer ve sabit şekildedir. Bunun haricindeki davranışlar anormal olarak görülmekte ve saldırılarda bu sınıf içerisinde yer almaktadır. Başarılı bir anomali tespit sistemi bu tür davranışları olma anında yakalayarak tespit etmeyi amaçlamaktadır. Bunun ihtiyaç duyulan kullanıcı profili ağ yönetimi üzerinden temin edilerek sürekli güncel tutulmalıdır. Anomali tespit işlemi, temelde bazı varsayımlardan yola çıkar. Bunlar;

•Bir kullanıcı profili, anlık değişimlerde çok büyük farklılıklar göstermez.

•Bir saldırgan aktivite ağ trafiğinde anormal değişikliklere neden olur.

Bir Anomali Tespit sisteminin işlem adımları Şekil 1'de verilmiştir. Sistemin çalışması aşamasında, 1) Öncelikle giriş bilgisi alınır, 2) Veri bir ön işleme tabi tutularak tespit için uygun bir formata dönüştürülür, 3) Tespit işlemi için uygun algoritmalar çalıştırılarak sonuç elde edilir, 4) Elde edilen sonuçlar için bir skor değeri hesaplanır ve sonuçlar etiketlenir, 5) Son olarak başarı değerlendirmesi yapılır.



Şekil 1. Anomali Tespiti İşlem Adımları

A.Anomali Çeşitleri

Anomali verileri, normal ağ trafiği gibi tanımlı bir modele uygun bir davranış sergilemez. Bu nedenle, literatürde anomaliler 3 gruba ayrılmıştır [4].

1)Nokta Anomali

Belli bazı veri örnekleri, veri setinin geri kalanına göre anormal davranış sergiler. Buna nokta anomali denir. Örneğin; düzenli olarak haftada 20 lira benzin harcaması olan birisinin bir haftada 200 liralık benzin harcaması olduysa, bu durum nokta anomali olarak değerlendirilir.

2)İçerik Anomali

İçerik anomalinin nokta anomaliden farkı, verinin içerdiği bazı bilgilerin sonuca etki etmesidir. Örneğin; normalde haftalık kredi kartı harcaması 200 lira olan birisinin, yılbaşı haftasında çok daha fazla harcama yapması anormal davranış olarak değerlendirilmez. Bu durumda yılbaşı haftası 1000 lira harcaması o durumu anomali yapmaz. Ancak kullanıcıya göre sıradan bir günde aynı miktarda harcama yapılması o durumu anomali yapabilir.

3)Toplu Anomali

Bu tarz anomali, veri setindeki bazı örnekler için değil, bir grup veri örneğinin anormal davranış göstermesini ifade eder. Örneğin, bir insanın Elektro Kardiyogram (EKG) verisi, normal zamandakinden farklı değerler üretiyorsa, bu durum toplu anomali olarak değerlendirilir.

B.Saldırı Tipleri

Ağ güvenliği sistemlerinde dijital verinin korunması güvenilirlik (confidentiality), bütünlük (integrity), ulaşılabilirlik (availibility) ölçütlerine bağlıdır. Ağa yapılan saldırılar, bu ölçütlerden bir ya da birkaçına etki eder. Saldırıların, bu şekilde farklı karakteristik özelliklere sahip olmaları nedeniyle, ağa yapılan saldırılar 4 ana grup altında toplanmıştır.

•Erişim Engelleme (Denial of Service - DoS): Bir sistemin kaynaklarının aşırı derecede tüketilmesi ile bu sistemin gerçek kullanıcılara hizmet veremez duruma getirilmesine yönelik saldırılardır.

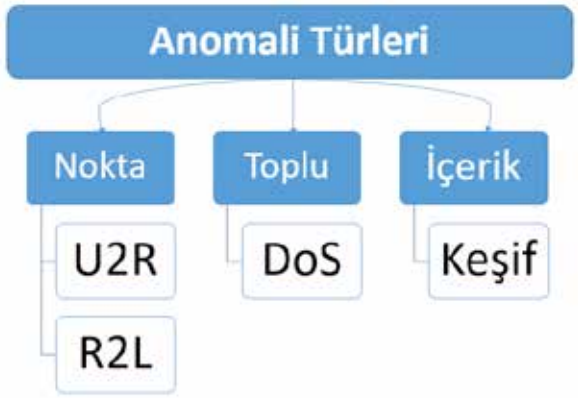
•Keşif Saldırıları (Probe Attacks): Keşif saldırıları, hedef sistem hakkında bazı bilgilerin elde edilmesine yönelik saldırılardır. Bu saldırı sonucunda saldırgan, hedef ağ hakkında elde ettiği bilgilere göre belirli bir hedefe yönelik saldırı planı hazırlayabilir.

•User to Root (U2R): Saldırganın, hedef sistem üzerinde illegal bir şekilde, tam yetkili erişim elde etmesine yönelik saldırılardır. Sosyal mühendislik yöntemi gibi yöntemlerle normal bir kullanıcının hesap bilgilerini ele geçiren saldırgan, tam yetkili erişim elde edebilmek için sistem içerisindeki güvenlik açıklarından faydalanır.

•Remote to Local (R2L): Saldırgan, ağ üzerinden hedefe gönderdiği paketler ile hedef makine üzerinde normal kullanıcı gibi erişim sağlar. Bu tip saldırılar genellikle sosyal mühendislik yöntemi kullanırlar.

Belirtilen dört saldırı çeşidi, karakteristik özellikleri gereği farklı tip anomali davranışları sergiler. Örneğin; DoS saldırılarında,

bir web sunucuya çok fazla sayıda bağlantı kurulur. Bu da ağ trafiğinde toplu bir değişikliğe neden olur. Bu nedenle DoS saldırılarının karakteristik özelliği Toplu Anomaliye uygundur. Keşif Saldırılarında yapılan aktiviteler, normal kullanıcıların gerçekleştirdiği aktivitelere benzer ancak bu aktivitelerin içeriğinde ağ yapıları hakkında bilgi elde edinebilmek amacı vardır. Bu nedenle Keşif Saldırıları, içerik anomali şeklinde davranış gösterirler. U2R ve R2L saldırıları ise diğer saldırılara kıyasla daha karmaşık ve anlaşılması zordur. Bu tip saldırılar da nokta anomali olarak değerlendirilir. Saldırı tiplerinin gösterdiği anomali davranışları Şekil 2 'de verilmiştir.



Şekil 2. Anomali Türleri

AT-STS'nin ağ trafiği verilerini değerlendirmesi sonucu 4 farklı durum oluşabilir. Her durumun bulunma olasılığı sıfırdan farklıdır. Bu durumlar şöyledir;

•False Negative (FN): Anomali davranış sergilemeyen saldırılar bu gruba girer.

•False Positive (FP): Aktivitenin saldırgan olmamasına rağmen anomali olarak rapor edildiği durumdur. Bu durumda, normal kullanıcının yaptığı aktiviteler hatalı olarak rapor edilmiş anlamına gelmektedir.

•True Negative (TN): Saldırgan olmayan aktivitelerin saldırgan olarak tanınmaması durumudur.

•True Positive (TP): Saldırgan aktivitelerin saldırgan olarak değerlendirildiği durumdur.

Başarılı bir STS de, TP ve TN durumuna ait aktivitelerin sayısının fazla, FN ve FP durumuna ait aktivitelerin sayısının az olması beklenir. AT-STS için yapılan çalışmalarda, TP ve TN değerlerinin fazla olmasının yanı sıra FP değeri de yüksek olarak çıkmaktadır. Bu nedenle son yıllarda, TP ve TN oranının artırılmasının yanı sıra FP oranının da azaltmasına yönelik çalışmalar da gerçekleştirilmiştir.

III. ANOMALİ TESPİT AŞAMALARI

Anomali tespit işlemi yapılabilmesi için öncelikle, veri setinin işlem yapılabilecek bir format haline getirilmesi gerekmektedir. Bunun için gerekiyorsa bazı dönüşüm işlemleri yapılmalıdır. İşlenebilir formattaki veri seti, belirlenen anomali tespiti yaklaşımlarının uygulanması ile test edilir. Elde edilen sonuçlar değerlendirilerek, başarı oranı hesaplanır.

A.Veri Seti

AT-STS'lerin test edilmesi için toplanan veri setindeki örneklerin, normal ve anormal olarak etiketlenmesi çok masraflı bir işlemdir. Ağ güvenliği uzmanları, eğitim setinin oluşturulabilmesi için, çok fazla emek gerektiren bu işlemi genellikle elle yaparlar. Anormal aktivite sergileyen örneklerin incelenmesi, normal aktivite sergilen ağ trafiği paketlerin incelenmesinden çok daha zordur ve bu nedenle fazla vakit almaktadır.

Araştırmacılar, geliştirdikleri Anomali Tespiti yaklaşımlarını test etmek ve değerlendirmek için gerçek-zamanlı olmayan çeşitli veri setleri kullanmaktadırlar. Ancak gerçek zamanlı bir ağ trafiğinde bilinmeyen birçok çevresel etmen bulunduğu için bu tip bir veri setinde Anomali Tespit sisteminin değerlendirilmesi çok zordur. Anomali Tespit sistemlerinin başarısının doğru bir şekilde değerlendirilebilmesi için bazı veri setleri oluşturulmuştur. Bu veri setleri, araştırmacıların kullanımına da açılmıştır.

Anomali Tespit sistemlerinin test edilmesi için kullanılan veri setlerinden en yaygın kullanılanlarından bir tanesi Lincoln Lab Dataset'tir (KDD99).

Lincoln Lab Dataset, Darpa iş birliği ile ilk defa 1998 yılında oluşturulmuştur. Bu veri seti, Makine Öğrenmesi tekniklerinin kullanılabilmesi için eğitim ve test verileri içermektedir. Yedi haftalık internet trafiği verisi içeren bu veri seti işlenmemiş hali yaklaşık dört gigabayt boyutundadır. Bu veri setinin, algoritmalar tarafından daha kullanışlı bir formatta saklanabilmesi adına bir ön işleme tabi tutulmuştur. Bu işlem sonrası veri beş milyon bağlantı kaydından oluşan bir şekil almıştır. Yeni bir form kazanmış bu veri seti KDD99 veri seti olarak bilinir. KDD99 veri seti dört farklı saldırı türüne ait veriler içermektedir. Bu saldırı türleri şunlardır; DoS, U2R, R2L ve Keşif Saldırıları.

Oluşturulan veri seti içerisinde, saldırı ve saldırı olmayan verilerden oluşan yedi haftalık internet trafiği verisi bulunmaktadır. Aynı şekilde test seti de saldırı ve saldırı olmayan verileri içerisinde barındırmaktadır. Bunların yanı sıra eğitim setine dahil edilmeyen bazı saldırılar test verisi içerisinde yer almaktadır.

KDD99 veri seti zaman içerisinde güncellenmiş ve son olarak gureKddcup (2008) isminde yayınlanmıştır.

STS'lerin test edilebilmesi için literatürde kullanılan diğer veri setlerinden bazıları şunlardır;

•Lawrence Berkeley National Laboratory Dataset (LBNL)

(2004-2005)

•Endpoint Dataset (2008)

•Network Trace (2003)

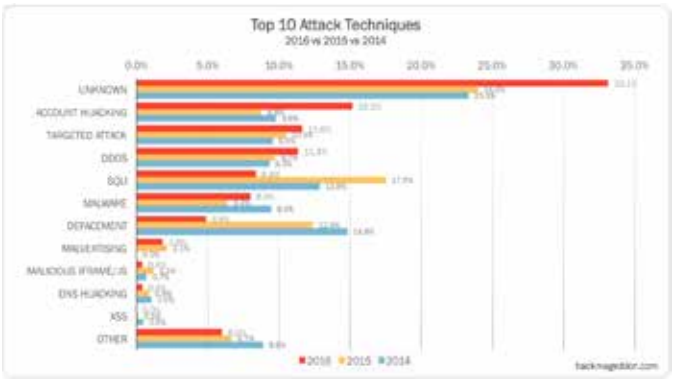
•Predict Dataset (2014)

•ADFA Intrusion Detection Dataset (2014)

•Kyoto Dataset (2014)

•ICS Attack Dataset (2014)

Saldırganlar, her geçen gün farklı yöntemlerle saldırılarını gerçekleştirmektedirler. 2014-2016 yılları arası saldırı istatistiklerine bakıldığı zaman, yapılan saldırıların büyük çoğunluğunun bilinmeyen saldırılar olduğu görülmektedir. Hackmageddon sitesinin açıkladığı 2014-2016 yılları arasına ilişkin siber saldırı istatistiklerine ait veriler [5] Şekil 3'te verilmiştir. Bu istatistik verilerine göre, 2014-2016 yılları arasında yapılan saldırıların yaklaşık dörtte birisi daha önce karşılaşılmamış bilinmeyen saldırılardır. Bu oran 2016 yılında daha artmıştır. Bu oran çok ciddi bir sayı teşkil etmektedir.



Şekil 3. 2014-2016 Yıllarında En Çok Gerçekleştirilen 10 Saldırı Türü [5]

Anomali Tespiti için kullanılan veri setleri, her geçen gün güncelliğini yitirmektedir. Dolayısıyla bu veri setleri kullanılarak gerçekleştirilen bir sistemin, yeni ortaya çıkan saldırılara dayanıklı olup olmadıkları test edilememektedir. Bu nedenle Anomali tespiti yapılacak sistemde kullanılacak veri setinin güncel olması gerekmektedir.

Araştırmacıların, güncel veri setlerine erişimleri kısıtlı olması nedeniyle bu konu üzerinde yapılan çalışmalar genellikle güncelliğini yitirmiş veri setleri ile test edilebilmektedir. Bu nedenle, akademik çalışmalarda yer alan başarı değerlerinin, güncel saldırıların gerçekleştiği sistemlerde ne kadar olacağı hakkında kesin bir bilgi verilememektedir.

B.Veri İşleme

Anomali Tespit sistemlerinin çalışabilmesi için kullanılan veriler genellikle çok fazla miktarda ham verilerden oluşmaktadır. Bu verilerin işlenebilmesi için, standart bir formata ihtiyaç vardır. Ayrıca ham veri içerisinde yer alan, ancak Anomali Tespitine herhangi bir faydası olmayan, alakasız bazı bilgiler filtrelenerek, kullanılacak veri setinin daha küçük boyutlara indirgenmesi gerekmektedir. Bu amaçlara yönelik olarak veri setine; Özellik Seçimi, Veri Tipi Dönüştürme, Normalizasyon ve Ayrıklaştırma adımları uygulanır. Bu adımların yanı sıra örnekler arası benzerliğin/uzaklığın hesaplanacağı Mesafe Hesaplama Algoritmasının seçimi de önemli bir adımdır.

1)Özellik Seçimi (Feature Extraction)

AT-STS'ler için özellik seçimi çok önemli bir adımdır. Gerçek zamanlı ağ trafiğini inceleyip sınıflandırmak, AT-STS'ler için çok maliyetli bir işlemdir. Bu nedenle ham veri setindeki tüm özelliklerin kullanılması yerine bazıları seçilip kullanılarak iş yükü azaltılabilmektedir. Ağ trafiğinde bulunan ayırt edici özellikler dört kategori altında değerlendirilmektedir [6].

•*Temel Özellikler (TÖ):* Payload kısmı hariç, paket başlığında yer alan bilgiler temel özellikler olarak değerlendirilir. Protocol tipi, service, flag, source bytes, destination bytes özellikleri bu kategoriye girer.

•*İçerik Tabanlı Özellikler (İTÖ):* TCP paketlerinin orijinal yükü, alan bilgisini değerlendirmek için kullanılır. Hatalı giriş denemesi gibi özellikler bu kategoriye girer.

•*Zaman Tabanlı Özellikler (ZTÖ):* Belirli zaman aralıkları içerisinde gerçekleşen durumları ifade eden özelliklerdir. Örneğin, aynı uç birim tarafından 2 saniyelik zaman dilimleri içerisinde kurulan bağlantı sayısı buna örnektir.

•*Bağlantı Tabanlı Özellikler (BTÖ):* Belirli zaman aralıkları yerine, belirli bağlantı sayıları arasındaki bilgileri ifade eden özelliklerdir.

Kullanılan özellik kategorileri bazı saldırıların tespit edilmesinde önemli rol oynamaktadır. İTÖ'ler, KDD99 veri setindeki R2L ve U2R tipi saldırıların tespit edilmesi için ön plana çıkmaktadır [7]. ZTÖ ve BTÖ'ler ise DoS ve Keşif tipi saldırıların tespit edilmesinde önemli rol oynamaktadır [8].

2)Veri Tipi Dönüştürme

Ham veri ve özellik verilerinin her ikisinde de sayısal tipte değerler olabileceği gibi kategorik tipte değerler de olabilir (tcp, icmp, telnet gibi). Bu nedenle kümeleme tabanlı anomali tespit tekniklerinde yakınlık bilgisinin hesaplanabilmesi için, veri setinde bir dönüşüm uygulanması gerekebilir.

3)Normalizasyon

Veri setinde yer alan özellik değerleri anomali tespiti için eşit derecede ağırlığa sahip olmayabilir ya da bu özellikler farklı değer aralıkları kullanabilirler. Böyle bir durumda, anomali tespit mekanizması kurulmadan önce normalizasyon işlemi yapmak faydalı olabilmektedir.

4)Ayrıklaştırma

Anomali Tespit veri seti, her bağlantı boyunca sürekli ve dinamik bir şekilde değişen bazı değerler içerir. Örneğin; paket sayısı, byte sayısı vb. Veri madenciliği tekniklerinin uygulana-

bilmesi için bu tarz özellik değerlerinin ayrık parçalara bölünmesi şeklinde bir dönüşüm uygulanması gerekmektedir.

5)Mesafe Hesaplama Algoritması

Mesafe tabanlı ya da yoğunluk tabanlı değerlendirme yaklaşımları, birlikte ya da ayrı ayrı olarak AT-STS'lerin değerlendirmesinde sıkça kullanılır. Mesafe tabanlı yaklaşımlarda, yakınlık hesabı (proximity measure), bilgi çıkarımında çok önemli rol oynamaktadır. Matematiksel anlamda mesafe, iki nesnenin birbirlerinden nicel olarak ne kadar uzakta olduklarını belirtir. Ancak mesafe tabanlı değerlendirme yaklaşımları genellikle O( ) karmaşıklığına sahiptir. Bu nedenle büyük çaptaki sistemlerde yavaş sonuç üretilmesine neden olabilir. Bazı uygun veri tipleri ve algoritmik optimizasyonlarla karmaşıklık O(nlogn) seviyelerine indirilebilir.

C.Anomali Tespiti Çıktıları

Bir anomali tespit sisteminin, anomali bir durum tespit etmesi halinde, bu durum uygun bir şekilde rapor edilir. Anomali tespit sistemi çıktısı, genellikle iki farklı şekilde raporlanmaktadır.

1)Skor

Bir test verisi, anomali olmasına neden olacak içerik bilgisinin değerlendirilmesiyle bir puan alır. Bu tarz tekniklerde örnekler, anomali olma ihtimallerine göre sıralanır. Bir eşik değeri belirlenerek, bu değerin üstünde kalan örnekler anomali olarak sınıflandırılır. Belirlenen eşik değeri dinamik olarak güncellenerek sistem, anomali tespiti için değişen şartlara daha uyumlu hale getirilebilmektedir.

2)Etiket

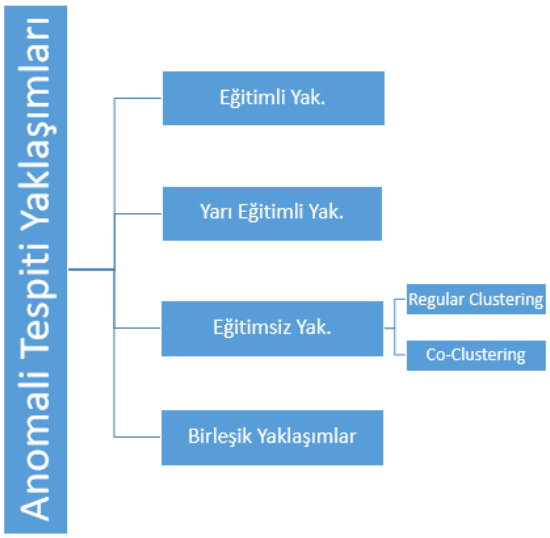
Kullanılan eğitim setinde bulunan örnekler bir model oluşturulduktan sonra sınıflandırmak istenin veri örneği bu modele verilir. Oluşturulan model, veri örneğinin "Normal" ya da "Anormal" olmak üzere sınıf bilgisini geri döndürür [9].

IV. ANOMALİ TESPİTİ YAKLAŞIMLARI

Anomali Tespitine yönelik literatürde yer alan çalışmalar, bu çalışmada dört ana başlık altında değerlendirilmiştir. Bunlar başlıklar;

- Eğitimli Yaklaşımlar (Supervised Approaches)
- Eğitimsiz Yaklaşımlar (Unsupervised Approaches)
- Yarı-Eğitimli Yaklaşımlar (Semi-Supervised Approaches)
- Hibrid Yaklaşımlardır.

Anomali Tespiti için kullanılan yaklaşımlara dair genel şema, Şekil 4'te verilmiştir.



Şekil 4. Anomali Tespit Yaklaşımları

A.Eğitimli Yaklaşımlar (Supervised Approaches)

Eğitimli Anomali Tespit Yaklaşımlarında (EY), aktivitelere ilişkin etiketli eğitim setinin kullanılmasıyla bir tahmin makenizması oluşturulmaya çalışılır. Etiketsiz olarak gelen veri (test verisi), eğitim setindeki etiketli örneklerle karşılarştırılarak, bu verinin hangi sınıfa ait olduğu tespit edilir.

Eğitimli Yaklaşımlarda üstesinden gelinmesi zor iki problem vardır. Bunlardan ilki, eğitim setindeki anomali örneği, normal veri örneğin çok az sayıda yer almaktadır. Bu durum. dengesiz sınıf dağımlımlarının ortaya çıkmasına neden olmuştur. Bu problem, veri madenciliği ve makine öğrenme teknikleri literaturunde yer almaktadır [10]. Bu problemlerden ikincisi ise, eğitim setindeki anomali ve normal verilerin etiketlenmesidir. Yapay anomali örneklerinin etiketli bir şekilde üretilip, eğitim setine eklendiği bazı yaklaşımlar da literatürde mevcuttur.

EY sınıflandırma tabanlı ve soft computing tabanlı olmak üzere iki alt başlığa ayrılmaktadır.

1)Sınıflandırma Tabanlı Yaklaşımlar

Sınıflandırma işlemi, yeni bir gözlem verisinin, eğitim setinde öğrenilen bilgilere göre hangi sınıfa dâhil olduğunu belirleme problemidir. Sınıflandırma teknikleri, ağ trafiğinin birçok sınıfa ayrılabilmesi için bir model oluşturmaya dayanır. Literatürde, anomali tespiti için ağ trafiği üzerinde çalışan birçok sınıflandırma tabanlı algoritma kullanılmaktadır. Bu algoritmalardan bazıları; Destek Vektör Makineleri (Support Vector Machine) [11, 12], Bayesian Network [13], Yapay Sinir Ağları (Artificial Neural Network) [15], Karar Ağaçları (Decision Tree) [14], k-En Yakın Koşu Yöntemi (k-Nearest Neighbor) [16].

2)Yapay Zeka Tabanlı Yaklaşımlar (Soft Computing)

Anomali tespiti için genellikle tam ve kesin bir sonuç elde edilemediği için Yapay Zekâ Tabanlı Yaklaşımlar (YZTY), ağda anomali tespiti için kullanılabilmektedir. YZTY; Genetik Algoritma Tabanlı, Bulanık Mantık Tabanlı, Kaba Küme Tabanlı, Yapay Bağışıklık Sistemi Tabanlı yaklaşımlardan oluşmaktadır.

a)Genetik Algoritma Tabanlı Yaklaşımlar

Genetik algoritmalar, doğada gözlemlenen evrimsel sürece benzer bir şekilde çalışan arama ve eniyileme yöntemlerine verilen isimdir. Bu tarz yaklaşımda algoritmalar, karmaşık çok boyutlu arama uzayında en iyinin hayatta kalması ilkesine göre bütünsel en iyi çözümü arar. Problem için olası pek çok çözümü temsil eden küme, genetik algoritma terminolojisinde nüfus adını alır. Nüfuslar vektör, kromozom veya birey adı verilen sayı dizilerinden oluşur. Birey içindeki her bir elemana gen adı verilir. Nüfustaki bireyler evrimsel süreç içinde genetik algoritma işlemcileri tarafından belirlenirler.

Genetik algoritmalar STS'lerde, trafik verilerine basit kurallar uygulamak için kullanılabilir. Bu kurallar, anormal trafik verilerinden normal verileri ayırmak için kullanılır. Veri kümesi, tcpdump [17] ya da Snort [18] gibi trafik dinleyiciler (sniffers) kullanılarak toplanır. Genetik algoritmalar öncelikle küçük boyutlu rasgele üretilmiş kurallar kümesi ile başlar, daha sonra bu kural kümesi genişletilir.

Saldırı tespiti işleminde bu tarz yaklaşımların kullanılabilmesi için öncelikle ağ verisinin kromozom benzeri bir veri yapısına dönüştürülmesi gerekir. Khan'ın gerçekleştirdiği çalışmada [19], saldırı tespiti işlemi için genetik algoritma kullanılarak geliştirilen kurallar kullanılmıştır.

b)Bulanık Mantık Tabanlı Yaklaşımlar (Fuzzy Logic)

Bulanık mantık tabanlı yöntemler, STS'lerde kullanılan bir diğer yaklaşımlardır. Bulanık mantık tabanlı olarak geliştirilen FIRE (Fuzzy Intrusion Recognition Engine), ağ verilerinin işlenmesiyle birlikte saldırıları tespit etmek için bulanık mantık kullanan örneklerden birisidir [20]. Ağ paketleri üzerinde çalışan FIRE'de; TCP, UDP ve ICMP için otonom ajanlar kullanılmıştır. Aynı zamanda kural tabanlı bir sistem olan bu çalışmada, güvenlik yöneticisi ve edinilen tecrübe sayesinde belirlenen bulanık kurallar oluşturulmuştur. Oluşturulan kurallar saldırıların tespit edilebilmesi kullanılmaktadır.

c)Kaba Küme Tabanlı Yaklaşımlar (Rough Set)

Eğitim setinin çok küçük olduğu durumlarda daha iyi eğitim yapılabilmesi için Kaba Küme Tabanlı Yaklaşımlar (KKTY) kullanılır. Varsayılan ayarlama olarak alt sınır ve üst sınır tahmini olmak üzere iki farklı tahmini veri seti elde edilir. Bu veri setlerin her birine Kaba Küme (Rough Set) denir. Bazı varyasyonlarda bu setler, bulanık veri setleri (fuzzy set) de olabilir. Kaba Kümeler kullanılarak eğitim işlemi küçük veri setleri ile gerçekleştirilebilir. Bu yöntem, anomali tespiti için normal davranışa sahip ağ trafiği modelleme işleme için kullanılabilir. Adetunmbi [16], anomali tespit işlemi için Kaba Kümeler ve k-NN sınıflandırma algoritmasını kullanmış ve yüksek saldırı tespit oranı ve düşük Yanlış Alarm oranı elde etmiştir. Başka bir çalışmada ise Chen [21], iki aşamadan oluşan saldırı tespit sistemi için ilk aşamada kaba kümeler ile özellik azaltma işlemi uygulamış ardından ikinci aşamada ise destek vektör makineleri ile son sınıflandırmayı yapmıştır. Bu çalışmada %89 civarında başarı oranı elde edilmiştir.

d)Yapay Bağışıklık Sistemi Tabanlı Yaklaşımlar (Artificial Immune System)

Literatürde insan bağışıklık sistemine dayalı birçok STS yaklaşımı bulunmaktadır. Bu çalışmalar, doğal bağışıklık sisteminden esinlenerek geliştirilmiştir. Yapay Bağışıklık Sistemi Tabanlı Yaklaşımlarda (YBSTY), anomali tespiti işlemi için biçimsel çatı (formal framework) önerilmiştir.

Doğal bağışıklık sisteminde olduğu düşünülen üç temel özellik bu tarz sistemlerin geliştirilmesinde temel alınmıştır [22]. Bu özellikler; farklılık (diversity), dağıtık doğallık (distributed nature) ve hata toleransı (error tolerance)'dır. YBSTY'da özellik seçimi aşamasında Karınca Kolonisi Optimizasyon yöntemini kullanan çalışmalar da bulunmaktadır. Bu çalışmalarda, her özellik değeri graf içerisinde bir düğüm olarak ifade edilir. Düğümler birbirlerine kenarlar ile bağlıdır. Karıncalar, grafta gezinmeye başlarlar ve durdurma kriteri sağlanana kadar gezinmeye devam ederler. Bir süre sonra optimum özellik grubu elde edilmiş olur.

B.Yarı Eğitimli Yaklaşımlar (Semi-Supervised Approaches)

Yarı Eğitimli Yaklaşımlar (YEY) saldırı tespiti için kullanılan bir diğer yaklaşım sınıfıdır. Literatürde bu tip yaklaşımlar kullanılarak geliştirilen çalışmalar mevcuttur [23-25]. YEY'de, Eğitimli Yaklaşımlarda olduğu gibi etiketli eğitim seti kullanılır. Ancak Yarı Eğitimli yaklaşımlarda kullanılan eğitim seti içerisinde sadece saldırı verisi olmayan normal veri örnekleri bulunur. Anomali durumları gösteren veri örnekleri bu eğitim seti içerisinde yer almaz. Bu yaklaşım ile normal olarak nitelenen veriler net bir şekilde öğrenilir ve bu normal örneklere uygun bir model oluşturulur. Test verisi olarak işlenen veriler, bu modele uygunsa normal olarak, modele uygun değilse anomali olarak değerlendirilir.

C.Eğitimsiz Yaklaşımlar (Unsupervised Approaches)

Eğitimsiz Yaklaşımlar (EsY), etiketlenmiş eğitim setine ihtiyaç duymazlar. Bu nedenle büyük ölçekli sistemlere uygulanması kolaydır. EsY'ler, normal veri örneklerinin sayısının, anormal veri örnekleri sayısından çok daha fazla olması varsayımından yola çıkar. Bu varsayımın doğru olmadığı durumlarda, sistemde çok sayıda Yanlış Alarm üretmektedir. EsY'ler genellikle, kümeleme tabanlı (clustering based) sistemlerdir. Kümeleme tekniği ise, verinin içeriğine bakmadan birbirlerine benzer objeleri bir araya getirme mantığına dayanır. Bu işlem için verilerin etiketlenmiş olması gerekmez. Az sayıda gruplamaya tabi tutulmuş veri setlerinde, bazı önemli detaylar kaybedilebilir, ancak basitlik sağlanmış olur. Anomali tespit sistemlerinde, verinin normal ya da anormal olarak kümelenmesi işlemi, veri setinin analizi için çok önemli rol oynamaktadır. Kümeleme tabanlı sistemler çalışma mantığına göre ikiye ayrılırlar. Bunlar; Regular Clustering ve Co-Clustering'dir.

1)Regular Clustering Yaklaşımları

Bu yaklaşımlarda, veri örnekleri gruplandırılır. Test verisinde yer alan bir örnek eleman sayısı fazla olan (normal aktivite grubu) veri kümelerine yakın ve eleman sayısı az (anormal aktivite grubu) olan veri kümelerine uzak ise "normal" olarak etiketlenir. Benzer şekilde test verisi elaman sayısı az olan (anormal aktivite grubu) veri kümelerine yakın ve eleman sayısı çok olan (normal aktivite grubu) veri kümelerine uzaksa "anomali" olarak etiketlenir. Bunlara ek olarak test verisi, normal veri küme merkezlerine belli bir eşik değerinden (threshold) fazla uzaksa yine "anomali" olarak değerlendirilir. Literatürde bu yöntem kullanılarak geliştirilmiş birçok çalışma mevcuttur [26, 27]. Literatürde anomali tespiti için birçok farklı Regular Clustering tekniği kullanılarak geliştirilmiş çalışma mevcuttur. Bunlardan bazıları şunlardır; Partitioning Based Çalışmalar [28], Hiyerarşik Tabanlı Çalışmalar [25, 38, 39], Yoğunluk Tabanlı Çalışmalar [29] ve Grid Tabanlı Çalışmalar.

2)Co-Clustering Yaklaşımları

Bu yaklaşımlarda veri örneklerine ait özelliklerin bulunduğu veri seti, örnekler ve özelliklerin her ikisi ayrı ayrı sınıflandırılır. Bu yaklaşımlarda özellikler alt özellik gruplarına ayrılır, bununla birlikte örnekler de alt örnek gruplarına ayrılır. Diğer kümeleme algoritmalarından farklı olarak bu yaklaşımlarda, Co-Clustering, bir kümeleme kriteri belirler ve zamanla bunu optimize eder. Belirli bir kritere göre eşzamanlı olarak belirlenen örnek ve özellik alt kümeleri belirlenerek kümeleme işlemi yapılır. Diğer bir deyişle orijinal veride yer alan bilgilerin optimize edilmiş hali kullanılarak karmaşıklık azaltılır ve bu sayede bellek alanından ve işlemci gücünden tasarruf edilir. Bunlara ek olarak mevcut özellik değerleri kullanılarak yeni özellik değerleri hesaplanabilir. Bu tarz yöntemler kullanılarak geliştirilen çalışmalara da literatürde rastlanmaktadır [30, 31].

D.Hibrid Yaklaşımlar

Anomali Tespiti işlemi için kullanılan sınıflandırma tabanlı eğitimli yaklaşımlar ile, Bilinen Saldırıları tanımada yüksek başarı elde edilebilmesine rağmen bilinmeyen saldırıları tespit etmek zor olmaktadır. Benzer şekilde eğitimsiz yaklaşımlarda ise Bilinmeyen Saldırılar tanınabilmekte ancak, bilinen saldırıların tanınma başarısı eğitimli sistemler kadar yüksek olamamaktadır. Bu nedenle son yıllarda yapılan çalışmalarda, saldırı tespiti için sadece bir temel algoritmanın gerçeklenmesinin yerine birden fazla algoritmanın birlikte çalıştığı Hibrid Yaklaşımlar (HY) geliştirilmiştir. HY'lerle ağırlıklı olarak eğitimli ve eğitimsiz algoritmaların birlikte çalıştığı sistemler tasarlanmıştır. Ancak birden fazla eğitimsiz algoritmanın ya da birden fazla eğitimli algoritmanın birlikte çalıştığı sistemlere de literatürde rastlanabilmektedir.

Eğitimli ve eğitimsiz algoritmaların birlikte kullanıldığı sistemlerde temel amaç, eğitimli sistemlerin bilinen saldırıları yüksek başarı oranı ile tanıyabilme kabiliyetleri ile eğitimsiz sistemlerin bilinmeyen saldırıları tespit edebilme kabiliyetlerini birleştirmektir. Bu tarz yaklaşımlar ile bilinen ve bilinmeyen saldırıları bir arada ve yüksek başarı ile tanıyan aynı zamanda düşük false alarm oranı olan sistemlerin geliştirilmesi hedeflenmiştir.

Muda [32], iki aşamalı olarak tasarladığı saldırı tespit sisteminde, başlangıç olarak eğitimsiz bir algoritma olan K-Means algoritması ile öncelikle veri setini üç gruba ayırmıştır. Bu gruplar, keşif saldırıları (G1), U2R-R2L saldırıları (G2), erişim engelleme saldırıları (G3)'dır. K-Means algoritması veriyi bu üç gruba ayırmada iyi sonuçlar vermektedir. Daha sonra eğitimli bir algoritma olan Naive Bayes Algoritması ile veri seti dört saldırı sınıfı ve bir normal sınıf toplam beş adet sınıfa ayrılmaktadır.

Gaddam [33], anomali tespiti için k-Means ve Karar Ağacı (Decision Tree-ID3) algoritmalarını kullanmıştır. Sistem, öncelikle veri setini k adet gruba ayırmaktadır. Ardından oluşturulan Karar Ağacı ile anomaliler tespit edilir. Ağlardaki anomali durumların tespitinde yüksek başarı oranı ve düşük Yanlış Alarm oranı elde edilmiştir.

Khan [34], Desktek Vektor Makinelerinin (DVM) çok uzun süren eğitim aşaması kısaltabilmek için bir hiyerarşik kümeleme algoritması kullanmıştır. Kümeleme işlemi ile DVM eğitimi birbirine paralel olarak çalışmaktadır. Bu işlem hiyerarşik bir ağaç ortaya çıkana kadar devam etmektedir. Bu yöntemle, başarı oranından herhangi bir kayıp yaşamadan DVM'lerin eğitim süresi kısaltılmıştır.

V. GEÇERLİLİK ÖLÇÜTLERİ

AT-STS'lerin başarı performansı, önemli ölçüde; kendisine ait yapılandırma ayarlarına, monitör edilen ağa ve bu sistemlerin ağ içerisindeki konumu gibi kriterlerle doğrudan ilişkilidir [35]. Bunların yanı sıra AT-STS'lerin geçerli ve başarılı sayılabilmeleri için bazı ölçütler belirlenmiştir [35]. Bu ölçütlerden bazıları şunlardır;

•***Saldırı Yapıldığının Anlaşılması:*** AT-STS'lerin performansını belirleyen ana ölçüt, saldırının tanınmasıdır. Özel olarak bazı firmalar ve araştırmacılar saldırı niteliği taşıyan zararlı ağ trafiğine ilişkin tüm durumları dikkate alır. Ancak, günlük yaşantıda, zararlı trafik ciddi bir tehdit oluşturma aşamasına gelene kadar sadece kayıt altına alınır. Zararlı trafik, sadece kullanıcı güvenliğine ciddi bir tehdit oluşturmaya başladığında yetkililere bilgilendirme yapılır.

•***Bilinen Zafiyetler ve Saldırılar:*** Bütün AT-STS'ler bilinen zafiyetlere yapılan saldırıları tanıma kapasitesine sahip olmalıdır. Başka bir deyişle, yeni bir saldırı tespit edildiğinde tüm sistemler, bu saldırıyı tespit edebilecek şekilde güncellenmelidir.

•***Bilinmeyen Saldırıları Tespit:*** Bilinmeyen saldırıları tespit etme, aslında AT-STS'ler için en önemli fonksiyondur. Başarılı bir AT-STS'nin, bilinmeyen saldırıları tespit edebilme yeteneğine sahip olması gerekir. Her an yeni güvenlik zafiyetlerinin keşfedildiği günümüzde, sadece bilinen saldırıları tanımak yeterli olmamaktadır.

•***Kararlılık, Güvenilirlik ve Güvenlik:*** Bir AT-STS, çalışmasını her şart altında yürütebilmelidir. Bu tarz sistemlerin çalıştığı uygulamalar ve işletim sistemleri, aylar ve yıllar boyunca hiçbir hata vermeden çalışabilir olmalıdır. Ayrıca sistemin güvenliği de çok önemlidir. Saldırgan, sistem üzerinde bir AT-STS tespit ederse DoS ya da DDoS saldırı ile sistemi servis dışı bırakamamalıdır. AT-STS bu tarz saldırılara karşı dayanıklı olmalıdır.

•***Hedef ve Kaynağın Belirlenmesi:*** Bir saldırı tespit edildiğinde, saldırının kaynağı ve hedefi tam olarak belirlenebilmelidir. Bunların yanı sıra, gerekirse, saldırgan IP'sine dair whois sorgusu veya DNS Lookup bilgisi de elde edilebilmelidir.

•***Saldırı Sonucu:*** Başka bir önemli bilgi ise, saldırının sonucunu başarıya ulaşıp ulaşmadığı bilgisidir. Genellikle, saldırı girişiminde bulunulduğunda alarm verilir. AT-STS'ler bunun da ilerisinde, birbirleri ile ilişkili aktiviteleri analiz ederek saldırının başarılı bir sonuca ulaşıp ulaşmadığını tespit etmekle sorumludur.

•***Toplanan Verilerin Yasallığı:*** Özellikle, yapılan bir saldırıya karşılık bir karşı saldırı ile cevap verilmesi gereken durumlarda, toplanan verinin yasallığı çok önemli bir konudur. Çok fazla sistem, asıl ağ trafiği paketlerini kayıt altına almaz, bunun yerine bu ağ trafiğini işleyerek kendi belirlediği bir formatta kaydeder. Güvenilir sistemler, basit bir alarm durumunda dahi ağ trafiği paketleri kayıt altına alıp saklamalıdır.

•***Saldırı İmza Veri Tabanının Güncellenmesi:*** AT-STS'ler, tespit ettiği yeni bir saldırının imzasını oluşturabilmeli ve saldırı imzalarını dinamik olarak güncelleyebilmelidir.

A.Değerlendirme Kriterleri

Saldırı tespit işleminin değerlendirilmesi için yaygın olarak kullanılan dört adet ölçüt vardır. Bunlardan ilki True Pozitif oranı ve False Pozitif oranı, ikincisi ise True Negative ve False Negative oranlarıdır. Bunların yanı sıra STS'lerin başarı değerlendirmesinde Staniford [36] tarafından da kullanılan diğer ölçütler ise Geçerlilik ve Verimliliktir. Geçerlilik ve Verimlilik ölçütleri ise şu şekilde tanımlanmaktadır.

Geçerlilik = (TP) / (TP+FN)

Verimlilik = (TP) / (TP+FP)

Anomali Tespiti işlemi, belirli bir miktar zaman ve bellek tüketir. Tespit süresi, kullanılan yöntemin karmaşıklığına bağlıdır. Tespit süresi kabul edilebilir bir değerin üzerinde ise sistemin, anomali tespiti yapamadığı kabul edilir. Ancak bu çalışma boyunca incelenen anomali tespit sistemleri, uygun bir gecikme süresi miktarına (1 saniyeden daha az) sahiplerdir.

Analiz edilen çalışmalarda; TP oranı, FP oranı, Geçerlilik ve Verimlilik değerlerinin, AT-STS'leri değerlendirmede daha sıklıkla kullanıldığı belirtilmiştir [37].

VI. SONUÇ

Gelişen internet ve ağ teknolojileri ile ağlara yapılan saldırılar da gün geçtikçe artmaktadır. Bu saldırılan tespit edilmesi ve uygun önlemlerin alınması günümüzde çok büyük önem arz etmektedir. Anomali tabanlı saldırı tespit sistemleri, yapılan bu saldırıları tanınmasında ve gerekli önlemlerin alınmasında büyük rol oynamaktadır. Bu çalışmada öncelikle saldırı tespit sistemlerinin genel terminolojisi açıklanmıştır. Ardından, anomali türleri ve saldırı türleri açıklanmış ve bu türlerin karakteristik özelliklerine dair bilgiler verilmiş olup bu alanda çalışacaklara bir kaynak yayın geliştirilmesi amaçlanmıştır.

Anomali tespiti için kurulan sistemin başarısının test edilmesi için veri setlerine ihtiyaç duyulmaktadır. Akademik çalışmalarda kullanılabilmesi için oluşturulmuş veri setleri bu çalışmada açıklanmış ve akademik çalışmaların birçoğunda kullanılan veri seti KDD99 hakkında açıklayıcı bilgiler verilmiştir. Anomali tespiti için veri seti oluşturulması çok çaba gerektiren bir işlem olduğundan, gelişen saldırı sistemlerine karşı güncelliğini koruyan veri setlerine olan ihtiyacın üzerinde durulmuş ve mevcut veri setlerinin avantaj ve dezavantajlarından bahsedilmiştir. Kullanılan veri setlerinin işlenmesine ve barındırdıkları özellik değerlerine dair bilgiler de çalışmada sunulmaktadır.

Anomali tespiti işlemin için kullanılan temel yaklaşımlar; Eğitimli Yaklaşımlar, Eğitimsiz Yaklaşımlar ve Yarı Eğitimli Yaklaşımlar ve Hibrid Yaklaşımlardır. Son yıllarda yapılan çalışmalar doğrultusunda birden fazla yaklaşımın birlikte kullanılması ile oluşturulan sistemlerin başarı oranı daha yüksek olabilmektedir. Bu çalışmada Hibrid Yaklaşımlar açıklanmış ve bu tarz yaklaşımların avantaj ve dezavantajlarından bahsedilmiştir. Son olarak bir sistemin geçerli olabilmesi için ne gibi özelliklere sahip olması gerektiği ve başarı değerlendirme kriterlerinden listelenmiştir.

BİLGİLENDİRME

Bu çalışmanın geliştirilmesinde katkı sağlayan Normshield ve BGA Security/Türkiye firmalarına teşekkürler.

KAYNAKÇA

[1] Symantec 2017 Internet Security Threat Report https://www.symantec.com/security-center/threat-report (Son Erişim Temmuz 2017)

[2] Number of Internet Users (2016) - Internet Live Stats, http://www.internetlivestats.com/internet-users/ (Son Erişim Temmuz 2017)

[3] S. Kumar and E. H. Spafford, "An application of pattern matching in intrusion detection," The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Tech. Rep. CSD-TR-94-013, June 17, 1994.

[4] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Network anomaly detection: methods, systems and tools." Ieee communications surveys & tutorials 16.1 (2014): 303-336.

[5] 2015 Cyber Attacks Statistics http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Son Erişim Temmuz 2017)

[6] H. G. Kayacik, A. N. Zincir-Heywood, and M. I. Heywood, "Se-

lecting features for intrusion detection: A feature relevance analysis on kdd 99 intrusion detection datasets," in Proceedings of the Third Annual Conference on Privacy, Security and Trust, October, pp. 1-6, 2005.

[7] "KDD cup 1999 data," October 1999. [Online]. Available:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (Son Erişim Temmuz 2017)

[8] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," in Proceedings of the 1998 USENIX Security Symposium, pp. 1-15, 1998, USENIX Association.

[9] R. Storlkken, "Labelling clusters in an anomaly based ids by means of clustering quality indexes," Master's thesis, Faculty of Computer Science and Media Technology Gjvik University College, Gjvik, Norway, 2007.

[10]M. V. Joshi, I. T. J. Watson, and R. C. Agarwal, "Mining needles in a haystack: Classifying rare classes via two-phase rule induction," SIGMOD Record (ACM Special Interest Group on Management of Data), Vol. 30, No. 2, pp. 91-102, 2001.

[11]I. Balabine, Velednitsky A. Method and system for confident anomaly detection in computer network traffic. Google Patents, 2015.

[12]HuW, Liao Y, Vemuri VR. Robust anomaly detection using support vector machines. In: Proceedings of the international conference on machine learning; 2003.

[13]D. Željko, Randic M, Krcelic G. Early detection of network element outages based on customer trouble calls. Decis Support Syst 2015; 73:57–73.

[14]T. Abbes, A. Bouhoula, and M. Rusinowitch, "Efficient decision tree for protocol analysis in intrusion detection," International J. Security and Networks, vol. 5, no. 4, pp. 220–235, December 2010.

[15]S. Selim, M. Hashem, and T. M. Nazmy, "Hybrid Multi-level Intrusion Detection System," International J. Computer Science and Information Security, vol. 9, no. 5, pp. 23–29, 2011.

[16]A. O. Adetunmbi, S. O. Falaki, O. S. Adewale, and B. K. Alese, "Network Intrusion Detection based on Rough Set and k-Nearest Neighbour," International J. Computing and ICT Research, vol. 2, no. 1, pp. 60–66, 2008.

[17]http://www.tcpdump.org/tcpdump_man.html (Son Erişim Temmuz 2017)

[18]https://www.snort.org/ (Son Erişim Temmuz 2017)

[19]M. S. A. Khan, "Rule based Network Intrusion Detection using Genetic Algorithm," International J. Computer Applications, vol. 18, no. 8, pp. 26–29, March 2011.

[20]J. E. Dickerson, J. A. Dickerson, "Fuzzy network profiling for intrusion detection" NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, 301-306, (2000).

[21]R. C. Chen, K. F. Cheng, Y. H. Chen, and C. F. Hsieh, "Using Rough Set and Support Vector Machine for Network Intrusion Detection System," in Proc. First Asian Conference on Intelligent Information and Database Systems. Washington DC, USA: IEEEComputer Society, 2009, pp. 465–470.

[22]F. Esponda, S. Forrest, P. Helman, "A formal framework for positive and negative detection schemes", IEEE Transactions on Systems, Man, and Cybernetics, Part B, Cybernetics, 34(1): 357-373 (2004).

[23]K. Burbeck and S. Nadjm-tehrani, "ADWICE – anomali detection with real-time incremental clustering" in Proceedings of the 7. International Conference on Infirmation Security and Cryptology, Seoul, Korea. Springer Verlag, pp. 4007-424, 2004.

[24]A. Rasoulifard, A. G. Bafghi, and M. Kahani, Incremental Hybrid Intrusion Detection Using Ensemble of Weak Classifiers, in Communications in Computer and Information Science. Springer Berlin Heidelberg, November 23 2008, vol. 6, pp. 577–584.

[25]K. Burbeck and S. Nadjm-Tehrani, "Adaptive real-time anomaly detection with incremental clustering," Inf. Secur. Tech. Rep., vol. 12, no. 1, pp. 56–67, 2007.

[26]I. Syarif, Prugel-Bennett A, Wills G. Unsupervised clustering approach for network anomaly detection. In: Benlamri R, editor. Networked digital technologies communications in computer and information science, vol. 293. Berlin Heidelberg: Springer; 2012. p. 135–45.

[27]S. Petrovic, Alvarez G, Orfila A, Carbo J. Labelling clusters in an intrusion detection system using a combination of clustering evaluation techniques. In: Proceedings of the 39th annual Hawaii international conference on System Sciences, 2006. HICSS '06, vol. 6; 2006. p. 129b–129b.

[28]C. Zhong and N. Li, "Incremental clustering algorithm for intrusion detection using clonal selection," in Proceedings of the 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application. Washington, DC, USA: IEEE Computer Society, 2008, pp. 326–331.

[29]F. Ren, L. Hu, H. Liang, X. Liu, and W. Ren, "Using density-based incremental clustering for anomaly detection," in Proceedings of the 2008 International Conference on Computer Science and Software Engineering. Washington, DC, USA: IEEE Computer Society, 2008, pp. 986–989.

[30]Ahmed M, Mahmood AN. Network traffic pattern analysis using improved information-theoretic co-clustering based collective anomaly detection. In: Security and privacy in communication networks, Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering, vol. 153. Springer International Publishing, 2014. p. 1–16.

[31]Papalexakis EE, Beutel A, Steenkiste P. Network anomaly detection using coclustering. In: Proceedings of the 2012 international conference on advances in social networks analysis and mining (ASONAM 2012), ASONAM '12, IEEE Computer Society, Washington, DC, USA; 2012. p. 403–10.

[32]Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "A K-means and naive bayes learning approach for better intrusion detection," Information Technology J., vol. 10, no. 3, pp. 648–655, 2011.

[33]S. R. Gaddam, V. V. Phoha, and K. S. Balagani, "K-Means+ID3: A Novel Method for Supervised Anomaly Detection by Cascading KMeans Clustering and ID3 Decision Tree Learning Methods," IEEE Trans. Knowl. Data Eng., vol. 19, no. 3, pp. 345–354, Mar 2007.

[34]L. Khan, M. Awad, and B. Thuraisingham, "A New Intrusion Detection System Using Support Vector Machines and Hierarchical Clustering," The VLDB Journal, vol. 16, no. 4, pp. 507–521, October 2007.

[35]E. B. Lennon, "Testing intrusion detection systems.", iTL Bulletin, IT Laboratory, NIST, pp. 1-4, July, 2003.

[36]S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," in Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece, November 2000.

[37]Bhuyan, Monowar H., Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Survey on incremental approaches for network anomaly detection." arXiv preprint arXiv:1211.4493 (2012).

[38]C. C. Hsu and Y.-P. Huang, "Incremental clustering of mixed data based on distance hierarchy," Expert Syst. Appl., vol. 35, no. 3, pp. 1177–1185, 2008. [Online].

[39]K. Burbeck and S. Nadjm-tehrani, "ADWICE - anomaly detection with real-time incremental clustering," in In Proceedings of the 7th International Conference on Information Security and Cryptology, Seoul, Korea. Springer Verlag, pp. 4007-424, 2004.

Türkçe İçerikli Web Sayfaları için Zafiyet Tespit ve Önleme Modeli

Vulnerability Detection and Prevention Model for Turkish Web Pages

Şeref SAĞIROĞLU
Gazi Üniversitesi,
Bilgisayar Müh. Bölümü
ss@gazi.edu.tr

Onur AKTAŞ
Gazi Üniversitesi,
Bilgi Güvenliği Müh. Bölümü
posta@onuraktas.net

Abstract :

Nowadays, web applications provide contents to users from shopping to health or from information acquisition to entertainment. In addition to the content provided, personal data are collected from users and used for different purposes. Any violation in the both the collection of data and the operation of the web application might cause damage or give harm to the users or institutions. In order to prevent violations or to determine weaknesses in advance, it is necessary to detect or identify the threats in web pages or applications. In this study, Turkish words which are frequently used in Turkish webpages and applications are examined to detect any vulnerability that might give harm to the system in use. Finally, a new model is proposed to prevent the possible threats.

Index Terms: *web application, cyber security, vulnerability detection, exploits, model, prevention.*

Özet :

Günümüzde web uygulamaları alışverişten, sağlığa, bilgi ediniminden eğlenceye kadar bir çok alanda son kullanıcılara içerik sağlamaktadır. Sağlanan içeriklerin yanında kullanıcılardan önemli veriler toplanmakta ve farklı amacalar doğrultusunda bu veriler kullanılmaktadır. Gerek toplanan verilerin gerekse web uygulamanın işleyişindeki bilgi güvenliği ihlalleri maddi ve manevi zarara neden olmaktadır. Bu ihlalleri önleme amacıyla web uygulamalarındaki tehditleri belirlemek ve zafiyetleri önceden tespit ederek önlemek gerekmektedir. Bu çalışma da web tabanlı Türkçe uygulamalarda sıklıkla kullanılan Türkçe kelimelerin analizi ve bu kelimelerin kullanılması ile oluşabilecek zafiyetler incelenmiş, olası tehditler ile ilgili tespitlerde bulunulmuş giderilmesine yönelik model önerilmiştir.

Anahtar Kelimeler: web uygulama, siber güvenlik, zafiyet tespiti, sömürü, model, korunma.

I. GİRİŞ

Web uygulamalarındaki bilgilerin gizliliği, erişilebilirliği veya bütünlüğü yapılan siber saldırılar tarafından tehlikeye girebilir. Bilgi güvenliğinin gizlilik, bütünlük ve verinin kullanılabilirliği olmak üzere üç temel amacı vardır [1]. Gizlilik yalnızca yetkili erişimlerin olması gerektiği anlamını taşımaktadır. Bilgiye yetkisiz olarak yapılan ve istenmeyen tüm erişimler gizlilik bileşenini tehlikeye sokar. Erişilebilirlik istenilen zamanda ve istenilen şekilde bilgiye ulaşılabilmesi anlamını taşımaktadır. Bütünlük ise bilginin bir parçasının veya tamamın zarar görmemesini, yetkisiz bir şekilde değiştirilmemesi demektir. Bu üç temel bileşenin tamamının sağlanması siber güvenlik açısından önemlidir. Bilgi güvenliği ihlali oluşturabilecek zafiyetlerin tespiti ile web uygulamalarındaki siber güvenlik daha ileri seviyeye taşınabilir. Zafiyetleri tespit etmek web uygulamaları hakkında bilgi toplamak ile doğru orantılıdır. Türkçe web uygulamalarında Türkçe kelime listesini kullanarak erişilebilir web sayfalarının belirlenmesi ve oluşabilecek zafiyetlerin tespiti ile web uygulamalarındaki güvenliği arttırılması amaçlanmıştır.

II. WEB TABANLI ZAFİYETLER

Bilişim sistemlerin güvenilir bir şekilde çalışması için üç temel bileşen arasında denge kurmak gerekmektedir. Bu denge risk değerlendirilmesine göre yapılmaktadır. Risk istenmeyen bir olay veya sonuçlarından dolayı oluşabilecek kayıp veya zararların potansiyeli olarak tanımlanmaktadır [2]. Yapılan risk değerlendirmesi sonucu risk kabul edilebilir, azaltılabilir veya aktarılabilir. Sistemlere zarar verebilecek riskler tehditleri oluştururlar. Tehditlerin bilgi sistemlerinde etkili olabilmesi için bilgi sistemleri üzerindeki var olan zafiyetleri kullanmaları gereklidir [3]. Siber dünyada kullanılan varlıklar siber saldırganlar tarafından sürekli tehdit altındadır. Bilişim sistemlerini oluşturan varlıkların (sunucular, istemciler, yazılımlar) zafiyet oluşturan tüm alanları siber saldırganlar tarafından birer atak vektörü olarak kullanılabilmektedirler. Bilişim varlıklarına olan erişimlerin tamamı bir veya daha fazla atak vektörlerine dönüşebilirler.

Güvenlik testleri siber saldırganların gözünden iyi niyetli (beyaz şapkalı) uzmanlar tarafından hedef sistemlere yapılan saldırı simülasyonlarıdır. Bu testler sırasında zafiyetler belirlenmekte ve zafiyetlerin tetiklenmesi ile alakalı bazı çalışmalar yapılmaktadır. Testlerin sonunda hedef sistemlerin sorumluları ile paylaşılan rapor ile sistemler kötü niyetli siber saldırganlar tarafından zarara uğratılmadan önce var olan zafiyetlerin tespiti ve sonrasında kapatılması amaçlanmaktadır.

Kötü niyetli saldırganlar veya beyaz şapkalı siber güvenlik uzmanları hedef sistemde öncelikle bilgi toplayarak atak vektörlerini ortaya çıkartmaktadırlar. Web uygulamalarında atak vektörleri hedef web uygulamasına alınan tüm girdiler olarak tanımlanabilir. Kullanıcı tarafından alınan girdilerin doğru iş-

lenmeyen web uygulama içerisinde işlenmesi ile bilgi güvenliği ihlali oluşmaktadır.

Hedef web uygulama içerisinde ne kadar çok bilgi toplanırsa o kadar başarılı testler gerçekleştirilebilir. Toplanan bilgilerin içerisinde web uygulama sayfaları da bulunmaktadır. Çoğu durumda yönetici paneli, uygulama yedekleri, iz kayıtları gibi kritik bilgiler içeren bağlantılar web uygulama içerisinde gösterilmez, arama motorları tarafından kayıt edilmez ve normal erişimler ile tespit edilemez. Kritik bilgi içeren veya normal erişimler ile tespit edilemeyen fakat zafiyet içeren web sayfalarının siber saldırganlar tarafından tespit edilmesi durumunda bilgi güvenliğini doğrudan etkileyecek durumlar oluşabilir. Normal yollardan tespit edilemeyen bağlantıların tespiti için bir kelime listesini deneyerek kaba kuvvet yöntemini kullanan yazılımlar bulunmakta fakat bu yazılımların başarısı içerisindeki kelime listesinin kapsamı ile sınırlı olmaktadır [4]-[5]. Türkçe web uygulamalarında kullanılan Türkçe bağlantı adları güncel olarak kullanılan zafiyet tespit yazılımlarında bulunmadığından dolayı ilgili yazılımların içerisindeki kelime listesinin kullanılması durumunda bilgi toplama aşamasında eksiklik olduğu değerlendirilmektedir.

III. BAĞLANTI TESPİTİ SONRASI OLUŞABİLECEK ZAFİYETLERİN İNCELENMESİ

Yeni bağlantı ve sayfaların tespiti sonrası oluşabilecek zafiyetlerin kritik olanları aşağıda belirtilmektedir.

A. Cross-Site Scripting (XSS) Zafiyeti

JavaScript web uygulamalarında kullanılan tarayıcı tarafında yorumlanan ve genellikle yalnızca tarayıcı tarafında çalışan bir programlama dilidir. Bu programlama dili ile çerez bilgilerine erişimden, web sitelerindeki verilere erişime kadar bir çok işlem gerçekleştirilmektedir. Saldırganların tarafından hedef sistem üzerinde JavaScript kodu çalıştırmasına olanak tanıyan zafiyetler Cross Site Scripting (XSS) olarak adlandırılmaktadır. Cross-Site Scripting saldırıları günümüzdeki web uygulamalarında en çok tespit edilen zafiyetlerden biridir [6].

B. SQL Enjeksiyon Zafiyeti

Web uygulamalarındaki dinamik sayfalarda çoğunlukla kullanıcıya sunulan bilgiler veri tabanlarından okunarak servis edilir. Veri tabanından okuma işlemi veri tabanına özel kurallar çerçevesinde gerçekleştirilir. Verilerin daha önceden belirlenen şablonlara (tablo yapıları) uygun bir şekilde ilişkisel olarak saklandığı veri tabanlarına ilişkisel veri tabanı adı verilmektedir. SQL ise ilişkisel veri tabanları içerisindeki verileri yönetme amacıyla oluşturulmuş bir programlama dilidir [7]. SQL dili web uygulamalarında kullanıldığına kullanıcıdan alınan değerler SQL sorgularına dahil edilebilir. Yazılımcıların kullanıcıdan aldığı parametreleri SQL sorgularına kullanması ile oluşan sorgulara dinamik SQL sorguları denmektedir [8]. Saldırganların dinamik sorgulara müdahale ederek hedef sistemde çalışan SQL kodlarını değiştirerek yaptığı saldırılara SQL Enjeksiyon saldırıları olarak adlandırılmaktadır. SQL Enjeksiyon saldırılarında saldırganlar tarafından hedefe farklı farklı istekler gönderilerek, veri tabanı hakkında bilgi sahibi olma, veri tabanı yöneticim parolaları ele geçirme, verileri silme, ele geçirme, veri tabanında kod çalıştırma hatta işletim sistemine komut çalıştırmaya kadar bir çok farklı zararlı işlem gerçekleştirilebilir [9].

C. Siteler Arası İstek Sahteciliği

Web uygulamaları kullanıcıları hem tarayıcının kendisinde (çerez) hem de sunucu içerisinde tuttuğu (oturum bilgisi) bazı özel değerler ile tanımaktadır. Bu değerler sayesinde üyelik işlemleri, alışveriş sepeti gibi kişiye özel işlemler web sitesinde bir tarayıcı üzerinden gerçekleştirilir. Tarayıcıda tutulan bilgiler otomatik olarak tarayıcı tarafından yapılan her istekte gönderilir. Sunucu tarafında alınan bu bilgiler gerekli kontrollerden geçtikten sonra işlemler yapılır. Yeni oturum bilgileri sunucu tarafından oluşturulup HTTP başlıkları ile tarayıcıya gönderilmektedir. Oturum bilgileri web uygulamalarında mesajlar, yorumlar, alışveriş sayfası, üyelik paneli, üye işlemleri gibi özel alanlara erişim için kullanılmaktadır. Saldırganlar hedef sistemdeki tarayıcıların oturum bilgilerini kendi çıkarları için kullanarak web uygulamalarına sanki başka kullanıcıymış gibi işlem yapabilirler. Siteler arası istek sahteciliği (Cross-Site request forgery, CSFR) web kullanıcılarına yönelik, saldırganın kurbanın tarayıcısı ile güvenilir bir web uygulamasına istenmeyen bir istek yapması ile oluşan saldırılardır [10]. OWASP tarafından 2013 yılı içerisinde yayımlanan en çok karşılaşılan zafiyetler listesinde CSRF zafiyeti sekizinci sırada bulunmaktadır [11].

D. Parola Deneme Saldırıları

Parola bilgisinin kolay tahmin edilebilir olması saldırganların ilgili web uygulamasında kimlik doğrulama aşamasını geçmesi ile sonuçlanabilir. Kullanıcılar farklı farklı web uygulamalarına üyelik açtığı halde aynı parolayı tekrar kullanma eğilimindedirler. Bu da zaman geçtikte parolaların tekrar kullanımın oranını arttırmaktadır [12]. Web sitelerine ait kullanıcı bilgilerinin ele geçirilmesi aynı parolaların tekrar kullanılmasını daha tehlikeli bir hale getirmektedir. Bazı web uygulamalarında saldırganların denemelerini önlemek için kimlik doğrulama denemelerine belirli bir limit getirilmektedir. Her ne kadar parola denemeleri için limit olsa da saldırganlar tarafından ele geçirilen önceki sızmış parola bilgileri, deneme sayısı limiti içerisinde parolanın doğru şekilde tespit edilmesi için kullanılabilmektedir [13].

E. Yetkisiz Erişimler

Kullanıcılar, uygulamalar içerisinde farklı yetkilere sahip olabilmektedir. Web uygulamalarında bu yetkiler belirli alanlara yazma, belirli alanlardan okuma veya belirli alanları silme gibi farklılıklar gösterebilmektedir. Erişim kontrolleri web uygulamalarında veriye (okuma ve yazma) ilgili kullanıcının yetkileri dahilinde kısıtlanmasıdır [14]. Yetkiler genellikle kimlik doğrulama mekanizmaları sonrasında ilgili kullanıcıya atanmakta-

dır. Yetkisiz erişim doğru bilgilere (kullanıcı adı, parola, tek girişlik parola, vb.) sahip olmadan yetkili bir kullanıcı haklarının bir kısmına veya tamamına sahip olmaktır.

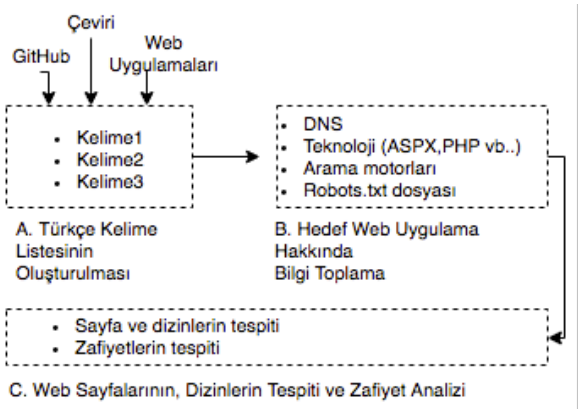
F. Dosya Çağırma Zafiyeti

Uygulamalarda yer alan kodlar içerisinde bazı durumlarda uzaktaki veya uygulama ile aynı alandaki (yerel) sistemlerden dosya çağıran kod parçaları bulunur. Bu kod parçaları web uygulaması içerisinde yapılması gereken işlerin bir kısmını veya tamamını yerine getirmek için kullanılabilir. Çağırılan dosyaların türüne göre komut çalıştırmaktan, dosya içerisindeki komutları kullanmaya kadar bir çok farklı alanlarda web uygulamalarına dışarıdan dosya çağırılabilmektedir. Bazı çalışmalar internet sitesi, dizinler veya aynı disk üzerindeki gibi farklı bir yerde bir kısım kodları çağırılmasına uzaktan dosya çağırma (remote file inclusion, RFI) zafiyeti olarak tanımlamıştır [15]. Bazı çalışmalarda ise doğru kontrollerin yapılmadığı sistemlerde, web uygulama ile aynı sunucuda olan dosyaları çağıran zafiyetlere yerel dosya çağırma (local file inclusion, LFI) zafiyetleri olarak , uzaktan aynı sunucu üzerinde olmayan dosyaların çağırıldığı zafiyetlere ise uzaktan dosya çağırma (remote file inclusion, RFI) zafiyetleri denmektedir [16]. Daha güncel çalışmalar içerisinde ve OWASP'da yerel dosya çağırma zafiyeti, uzaktan dosya çağırma zafiyeti olarak iki farklı zafiyet olarak incelenmektedir [16,17].

IV. ÖNERİLEN YÖNTEM

Gerek güvenlik testleri sırasında gerekse kötü niyetli saldırganlar tarafından yapılan sızma girişimlerinde web uygulamaları içerisinde tespit edilecek yeni atak vektörleri bütün uygulamanın ve uygulamanın bağlantılı olduğu tüm bilişim sistemleri için tehdit oluşturabilmektedir. Güvenlik testleri sırasında tespit edilemediğinden dolayı kontrol edilemeyen alanlar, yazılımcılar tarafından eski kalan unutulmuş sayfalar ya da kaynak kodu analizinde ortaya çıkmayan eksiklikler saldırganlar tarafından tespit edilmesi durumunda güvenlik ihlalleri oluştururlar. Web uygulamalarında arama motorları tarafından tespit edilemeyen, ilgili uygulama içerisindeki herhangi bir bağlantı ile erişimi olmayan gizli kalmış bölümleri tespit etmek için bir kelime listesi ile bağlantı denemesi yapan yazılımlar mevcuttur [18]. Bu yazılımlar içerisinde varsayılan olarak İngilizce kelime listesi olduğundan Türkçe yazılmış ve Türkçe kelimeleri bağlantılar içerisinde kullanan web uygulamaları için yazılımlar yetersiz kalmaktadırlar. Yapılan saldırıların ve oluşabilecek kayıpların önlenmesi için güvenlik testlerinin öneminin büyük olduğu ve gerçekleştirilen güvenlik testlerinde milli yöntemlerin kullanılmasının test sonuçlarını olumlu yönde etkileyeceği değerlendirilmektedir. Ülkemizde kurumsal bilgi güvenliği alanında yapılan ilk çalışmanın sonuç ve öneriler bölümünde milli yazılımların ve yöntemlerin geliştirilmesi ve kullanılmasına dair öneriler yer almaktadır [19].

Bu çalışma, web uygulamalarındaki bağlantılarda kullanılabilecek Türkçe kelime listesinin belirlenmesi ve Türkçe web uygulamalarında gizli kalmış, gözden kaçan yeni alanların tespit edilip güvenlik ihlalleri önlenmesini amaçlayarak üç farklı bloğa ayrılmıştır. Bu bölümler Türkçe kelime listesinin oluşturulması, hedef web uygulama hakkında bilgi toplama ve kelime listesinin gizli kalmış bölümleri tespit edilmesi amacıyla web sayfalarının, dizinlerin tespiti ve zafiyetlerin analiz edilmesidir.



Şek. 1. Yöntem Şeması

A. Türkçe Kelime Listesinin Oluşturulması

Türkçe kelime listenin oluşturulması için bir çok farklı kaynaklardan yararlanılmıştır. Kelime listesi içerisinde bulunan kelimeler çalışma sonucunu doğrudan etkileyeceği değerlendirilmektedir. Bu bölümde kelime listesi oluşturulurken kullanılan kaynaklar belirtilmiştir.

İngilizce olarak bağlantı tespiti için kullanılan listelerden çeviri ile kelime listesine başlanmıştır. Bağlantı tespiti için kullanılan Dirb adlı açık kaynak yazılım içerisinde gelen İngilizce kelime listesinden çeviriler yapılarak listenin ilk aşaması oluşturulmuştur. Rakamsal değerlerde listeye eklenerek kelime dışında rakamların kullanılması durumunda da bağlantıların tespit edilmesi amaçlanmıştır. Bu sayede tahmin edilebilir bir Türkçe bağlantı listesi ilk halini almıştır.

Açık kaynak kodların da barındırıldığı web tabanlı sürüm kontrol sistemi olan GitHub servisindeki açık kaynak web uygulamalarında kullanılan kelimelerde listeye eklenmiştir. Özellikle yönetim paneli ve alt sayfalarda kullanılan kelimeler bu çalışma sonucu listeye eklenmiş böylece web sitelerinin yönetim paneli ve alt sayfalarını tespit etmeye yönelik Türkçe kelime listesi güçlendirilmiştir.

Son olarak arama motorlarından dosya ve dizin gizlemek için kullanılan robots.txt dosyalarına erişilerek içerisindeki kelimeler tespit edilmiştir. Liste içerisinde hali hazırda bulunmayan kelimelerin, robots.txt dosyalarının analizi ile listeye eklenmiş ve liste son halini almıştır.

Türkçe kelime listesi hem zafiyet analiz araçlarına hem de açık kaynak dosya dizin tarama araçlarına girdi olarak eklenerek daha fazla bağlantı tespiti ve zafiyet tespiti için kullanılabilecektir.

Oluşturulan bağlantı listesi öncelikle Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile paylaşılacak kritik sektör ve devlet kurumlarının zafiyetleri tespit edilip giderildikten son-

ra açık kaynak olarak paylaşılacaktır.

B. Hedef Web Uygulama Hakkında Bilgi Toplama

Zafiyetlerin tetiklenmesi sonucu oluşabilecek bilgi güvenliğini ihlallerini önceden tespit etmek ve önlemek amaçlı iyi niyetli siber güvenlik uzmanları ilgili varlık üzerinde siber güvenlik testleri gerçekleştirilmektedir. Gerçekleştirilen güvenlik testleri , belirlenen kapsam içerisindeki tüm varlıkları siber saldırgan gözüyle zarar vermeden incelenip raporlanmasını kapsamaktadır. Güvenlik testlerinin ilk aşaması bilgi toplamadır. Güvenlik uzmanları hedef hakkında ne kadar çok bilgi toplayabilirse o kadar doğru bir değerlendirme yapabilirler. Tespit edilemeyen her bilginin siber saldırganlar tarafından tespit edilmesi halinde bilgi güvenliği ihlalleri ortaya çıkabilir.

2015 senesi içerisinde Imperva firması tarafından web uygulamalarına yönelik detaylı bir rapor yayınlanmıştır [20]. Raporda belirtildiği şekilde çoğu web uygulaması farklı türlerdeki siber saldırılara maruz kalmaktadır. Günümüzde kullanılan otomatik araçlar siber saldırganlar tarafından sürekli olarak web uygulamaları taranarak zafiyetler tespit edilmektedir. Bu çalışma kapsamında açılan sanal bir sunucuya web uygulaması kurulmuş ve aylar içerisinde yönetici panellerini tespit etmek veya yönetici panellerindeki yetkisiz erişimleri kontrol etmek için 1000'den fazla zararlı istek yapıldığı iz kayıtlarından görülmüştür.

Siber saldırganların zararlı aktiviteleri ya da güvenlik testleri sırasında hedef web uygulaması üzerinde bilgi toplamak atak vektörleri oluşturma aşamasında işe yaramaktadır. Bilgi toplama genel olarak aktif ve pasif bilgi toplama olarak iki bölüme ayrılmaktadır. Bir web uygulamasında bilgi toplama aşaması pasif olarak hedef sisteme iz kayıtları bırakmayacak şeklinde toplanan tüm bilgileri kapsamaktadır. Hedef web uygulamasında pasif bilgi toplama aşaması aşağıdaki maddeler ile gerçekleştirilebilir:

- Alan adı / IP kayıt bilgileri (whois)
- Sitelerin geçmişini kayıt eden servisler ile yapılan incelemeler
- Arama motorlarının kullanımı ve özel aramalar
- E-posta adreslerinin tespit edilmesi (hedefin dışında)
- DNS sorguları

Aktif bilgi toplama hedef web uygulamasına dokunan, hedef sistemde iz kayıtları bırakan tüm aşamaları kapsamaktadır ve aşağıdaki şekilde maddeler ile gerçekleştirilebilir.

- Servis bilgileri edinme
- Port tarama
- DNS kaba kuvvet saldırıları
- Web uygulama taramaları (web uygulama bilgileri)
- Kullanılan teknoloji (ASPX, ASP, PHP)
- Kullanılan alt alan adları adresleri (dns kaba kuvvet, arama motorları)
- Robots.txt dosyalarının analizi
- Arama motorundaki web sitesi ile alakalı sonuçlar

Aktif bilgi toplama adımlarından bağlantı tespiti, web uygulamalarındaki erişebilir sayfalardan bağlantı verilememiş veya arama motorları tarafından erişilemeyen bağlantıları ortaya çıkarmak için kullanılmaktadır. Çalışmanın bu bölümünde hedef web uygulama hakkında aşağıdaki bilgiler tespit edilerek tespit yüzeyi arttırılmıştır.

Pasif veya aktif bilgi toplama yöntemlerinden bazıları kullanılarak hedef web uygulama hakkında elde edilen tüm bilgiler bağlantı tespiti amaçlı kullanılacaktır.

Gizli kalmış, tespit edilemeyen bağlantıların tespit edilmesi durumunda yeni atak vektörleri oluşabilir. Bir kelime listesinin hedef web uygulamasının bağlantı adlarında denenerek incelenmesi bağlantı tespiti için kullanılan bir yöntemidir. Yeni tespit edilen bağlantılar güvenlik zafiyetleri içeriyorsa saldırganlar tarafından bu zafiyetler istismar edilebilirler. Tespit için kullanılan kelime listesi içerisindeki kelimeler tespitin başarını oranını doğrudan etkilemektedir.

Yeni bağlantı tespiti için kullanılan yazılımlarda İngilizce kelime listesi bulunmaktadır [4] [5]. İngilizce kelime listesi Türkçe uygulamalarında test edildiğinde gizli kalmış Türkçe bağlantılar tespit edilememektedir.

Web uygulamalarındaki güvenlik testlerindeki bilgi toplama aşamasında kullanılacak Türkçe kelime listesi yeni bağlantıların dolayısıyla yeni atak vektörlerinin tespit edilmesinde doğrudan etki sağlayacaktır.

C. Web Sayfalarının, Dizinlerin Tespiti ve Zafiyet Analizi

Tarayıcılar üzerinden erişilen web uygulamaları Hyper Text Transfer Protocol (HTTP) adı verilen bir protokol üzerinden çalışmaktadır. TCP/IP protokolü üzerinde uygulama seviyesinde çalışan HTTP protokolü Web'in çalışma altyapısını oluşturmaktadır [21]. Kullanıcının tarayıcısından giden istekler için HTTP protokolünün kullandığı bazı metotlar bulunmaktadır. Bu metotlar web sunucusunun gelen isteğe nasıl cevap verileceğini belirlemektedirler. GET metodu ile yapılan istekler yalnızca web sunucusu üzerinden istenilen sayfanın bilgisini alma amaçlı kullanılmaktadır. Tarayıcı tarafından herhangi bir web uygulama sayfasına GET isteği yapıldığına, istek yapılan sayfanın içeriği web sunucu tarafından kullanıcıya geri döndürülmektedir. HEAD metodu kullanıldığında ise yalnızca başlık bilgileri sunucu tarafından geri döndürülmekte, istek yapılan sayfa verisi geri döndürülmemektedir.

Web sunucularına yapılan her istek için, web sunucudan gelen cevap içerisinde bir HTTP cevap kodu bulunmaktadır. Bu cevap kodları Internet Engineering Task Force (IETF) tarafından belirlenmektedir [22]. Cevap kodları toplam 3 haneli rakamlardan oluşmaktadır ve toplam beş farklı cevap kodu türü bulunmaktadır. Web sunucusu tarafından iki ile başlayan bir cevap kodu dönmesi, cevabın başarılı bir şekilde istemciye iletildiği anlamına gelmektedir. Üç ile başlayan bir cevap kodunun sunucu tarafından iletilmesi ise yönlendirme işlemleri için kullanılmaktadır.

Web uygulamalarına erişim yaparken kullanılan bağlantılar

özel bir yapıya sahiptir. Bu bağlantı yapısının genel adına Uniform Resourse Locators (URL) denmektedir. URL değerleri internet üzerinden bağlantıyı bulmak için kullanılan sözdizimine verilen genel addır [23]. URL değerleri ile belirlenen kaynak sunucu üzerinde gerçekten fiziksel olarak olabileceği gibi mantıksal olarak da erişim sağlanabilmektedir.

Çalışma içerisinde önceden oluşturulan Türkçe kelime listesindeki tüm kelimeler hedef web uygulamasında yapılan isteklerdeki URL bilgilerine ekleme yapılarak yeni bağlantıların tespiti sağlanmıştır. Hedef web uygulamasında yapılan HTTP isteklerinde yalnızca GET veya HEAD metotları kullanılmış sunucudan dönen cevapta ise iki veya üç ile başlayan cevap kodları kayıt edilmiş ve oluşabilecek atak vektörleri ve zafiyetler incelenmiştir.

Tespit edilen bağlantıların zafiyet oluşturup oluşturmayacağını anlamak ve el ile yapılan analizleri hızlandırmak adına kritik kelimeler belirlenmiş ve bu kelimelerde tespit edilen bağlantılar içerisinde analiz yapılarak zafiyet oluşturabilecek bağlantılar belirlenmiştir.

V. DENEYSEL ÇALIŞMALAR

Gerçekleştirilen testlerde Türkçe web uygulamalarında gizli kalmış bağlantılar tespit edilmiş bu bağlantılarda çeşitli zafiyetler olduğu yapılan testlerde ortaya çıkmıştır. Bağlantıların tespit edilmesinden sonra yapılan analizlerde aşağıdaki zafiyetlere rastlanmıştır.

- Yetkisiz erişim
- Siteler arası istek sahteciliği
- Dosya çağırma sahteciliği
- Cross Site Scripting (XSS) zafiyeti
- SQL Enjeksiyon zafiyeti

Yapılan testler göstermektedir ki hedef hakkında toplanan bilgiler ve tespit edilen yeni bağlantılar yeni atak vektörleri oluşturmaktadır. Oluşan yeni atak vektörleri, zafiyetler ile birlikte bilgi güvenliği ihlallerine neden olabilir.

VI. SONUÇ

Geliştirilen yeni zafiyet tespit modelinde, Türkçe kelime listesi oluşturulmuş, bilgi toplama aşamasında yeni bağlantıların tespit edilmesi için hedef web uygulamasına istekler yapılmış ve erişilebilir bağlantıların tespiti ile zafiyetlerin analizi gerçekleştirilmiştir. Yapılan incelemelerde tespit edilen bir çok özel bağlantıda zafiyetler tespit edilmiştir. Bunun giderilmesine yönelik önerilerde bulunulmuştur.

KAYNAKLAR

[1] Akyazı, U. (2011). Gezgin Etmenler ve Doğdan Esinlenen Sezgiseller Kullanılarak Dağıtık Bilgisayar Güvenliğinin Sağlanması

[2] Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 11(7), 4332–4340.Rahalkar, S. A. (2016). Certified Ethical Hacker (CEH) Foundation Guide, 97–107. https://doi.org/10.1007/978-1-4842-2325-3

[3] Gülmüş, M. (2008). Kurumsal Bilgi Güvenliğii Yönetim Sistemleri ve Güvenliği, (D).

[4] 'GitHub Dirb', Mayıs 2017, https://github.com/seifreed/dirb

[5] 'DirSearch', Mayıs 2017, https://github.com/maurosoria/dirsearch

[6] Buja, G., Bin Abd Jalil, K., Bt Hj Mohd Ali, F., & Rahman, T. F. A. (2014). Detection model for SQL injection attack: An approach for preventing a web application from the SQL injection attack. Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on, 60–64.

[7] Elshazly, K., Fouad, Y., Saleh, M., & Sewisy, A. (2014). A Survey of SQL Injection Attack Detection and Prevention. Journal of Computer and Communications, 2(8), 1–9.

[8] Mavromoustakos, S. (2016). Causes and Prevention of SQL Injection Attacks in Web Applications, 1–5.

[9] Tandel, N., & Patel, K. (2014). Mitigation of CSRF Attack, 3(6), 1416–1420.

[10] Owasp, '2013 Top 10 List', Mayıs 2017, https://www.owasp.org/index.php/Top_10_2013-Top_10

[11] Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06, 44.

[12] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. Proceedings 2014 Network and Distributed System Security Symposium, (February), 23–26.

[13] Bocić, I., & Bultan, T. (2016). Finding access control bugs in web applications with CanCheck. Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering - ASE 2016, 155–166.

[14] Gonz, H. F., Polit, U., San, D., & Potos, L. (2008). Types of hosts on a Remote File Inclusion (RFI) botnet, 105–109.

[15] Begum, A., Hassan, M., Bhuiyan, Y., & Sharif, H. (2016). RFI and SQLi Based Local File Inclusion Vulnerabilities in Web Applications of Bangladesh, 1(December), 12–13.

[16] Owasp, Haziran 2017, https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

[17] Tajbakhsh, M. S., & Bagherzadeh, J. (2015). A sound framework for dynamic prevention of Local File Inclusion. In 2015 7th Conference on Information and Knowledge Technology, IKT 2015.

[18] 'DirBuster – Brute Force Directories & Files Names', Haziran 2017, https://www.darknet.org.uk/2011/11/dirbuster-brute-force-directories-files-names/

[19] Vural, Y. (2007). Enterprıse Informatıon Security And Penetration Testing, 249.

[20] 2015 Web Application Attack Report, Mayıs 2017, https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf

[21] Charles K., "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference", No Starch Press, 2005, Sayfa : 1315-1316.

[22] Hypertext Transfer Protocol, Mayıs 2017, https://www.ietf.org/rfc/rfc2616.txt

[23] Uniform Resource Locators, Mayıs 2017, https://www.ietf.org/rfc/rfc1738

Ev ve Ofis Ağına Katılan Cihazların Güvenliğinin Artırılması için Basit Makina Öğrenmesi Yöntemiyle Ağ Geçidi Üzerinde Güvenlik Çözümleri Oluşturulması

Security Solutions for Home Networks Using Machine Learning Alporthms

Tamer Say
Gazi Üniversitesi, Fen Bilimleri Enstitüsü
Bilgi Güvenliği Mühendisliği
Ankara, Türkiye
tamer.say@gazi.edu.tr

Mustafa Alkan
Gazi Üniversitesi, Fen Bilimleri Enstitüsü
Bilgi Güvenliği Mühendisliği
Ankara, Türkiye
alkan@gazi.edu.tr

İbrahim Alper Doğru
Gazi Üniversitesi, Fen Bilimleri Enstitüsü
Bilgi Güvenliği Mühendisliği
Ankara, Türkiye
iadogru@gazi.edu.tr

Murat Dörterler
Gazi Üniversitesi, Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği
Ankara, Türkiye
dorterler@gazi.edu.tr

Abstract

Nowadays, when people hear about cyber security or information security, they mostly consider it as enterprise cyber attacks or worldwide cyber security incidents, only. Recently, individuals have been hit by massive, global cyber security attacks, not only enterprises. Cyber attacks like phishing, ransomware are the most common. Individuals get bribed when their files get encrypted by very complex algorithms just after either they are deceived by a phishing attack or their devices gets exploited by a vulnerability. Numbers of devices that are communicating via internet are increasing exponentially. Home networks need better protection with these new, wide variety devices. In this research, we investigated characteristics of common cyber security attacks and current home network gateways with newly added devices and their challenges. Our research proposal includes simple machine learning algorithms and open source hardware and software solutions with how to implement them on home gateways.

Index Terms

Home Networks, Internet of Things, Modem Security, Cyber Attacks, Security Policies.

Özet

Günümüzde siber güvenlik veya bilgi güvenliği denildiğinde akla ilk olarak kurumsal ağlarda gerçekleştirilen siber saldırılar ve savunma yöntemleri gelmektedir. Son yıllarda kurumsal ağların yanı sıra ev ve ofis kullanıcıları da büyük çaplı saldırıların hedefi haline gelmiştir. Oltalama saldırıları ve fidye talebinde bulunan yazılımlarla yapılan saldırılar oldukça yaygınlaşmıştır. İnternet kullanıcıları çeşitli yöntemlerle kandırılarak cihazlarında bulunan dosyaları şifrelenmekte ve bu şifrelemelerin çözülmesi karşılığı fidye talep edilmektedir. İnternete bağlanan cihaz sayısı her geçen gün hızla artmakta ve nesnelerin interneti kapsamında yeni geliştirilen cihazlarla saldırı çeşitleri artmaktadır. Ağa katılan bu yeni cihazların, mevcut cihazlarla birlikte güvenliğinin sağlanması oldukça önemlidir. Bu çalışmamızda son yıllarda sıkça görülen saldırıların önlenmesi ev ve ofis cihazları güvenliğinin artırılması için ağ geçidi üzerinde sağlanabilecek çözüm önerileri sunulmakla birlikte, ev ve ofis ağına yeni katılan cihazların basit makine öğrenmesi yöntemleri ve açık kaynak çözümler ile daha güvenli bir şekilde iletişim kurmalarının sağlanması ve olası tehlike durumlarında daha aktif, hızlı çözümlerin oluşturulabilmesi önerisi sunulmuştur.

Anahtar Kelimeler

Ev Ağları, Nesnelerin İnterneti, Modem Güvenliği, Siber Saldırı, Güvenlik Politikası.

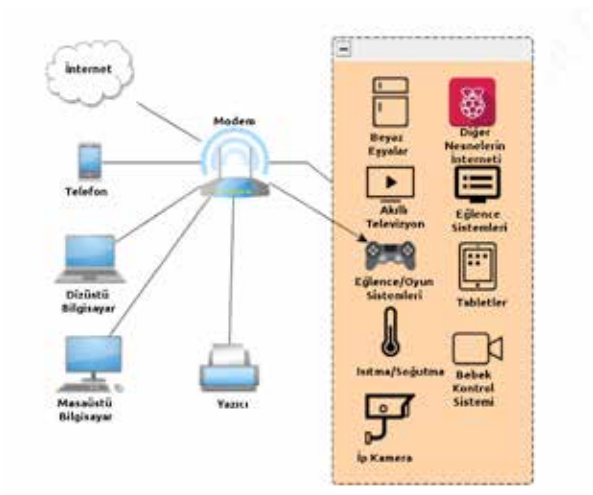
I. GİRİŞ

Ağlar ve cihazlar, kişilerin ve kurumların verilerini tutmak için kullanılan ortamlardır. İlk olarak bilgisayar güvenliği olarak ortaya çıkan günümüzde ise bir ağa bağlı olmasına bakılmaksızın tüm dijital cihazların güvenliğini kapsayan siber güvenlik, ağlarda ve cihazlarda bulunan verilerin güvenliği ile ilgilenen alandır. Siber güvenlik denildiğinde genellikle akla büyük sistemlerin, kurumsal ağların ve devletlerin dijital ortamdaki güvenliği gelmektedir. Gelişen teknoloji ile bu yargı tamamen değişmiş ve internete bağlanabilen çeşitli birçok cihazla birlikte bu tanım, çok daha geniş bir alanı kapsar hale gelmiştir. Arabalar, evler (akıllı evler), saatler, beyaz eşyalar, dijital

sensörler gibi birçok cihaz artık dijital dünyada yer edinmiş ve birer internet elemanı cihazlar olarak günümüzde bilinmektedir.

Nesnelerin interneti olarak adlandırılan bu cihazlar günümüzde hayati öneme sahip alanlarda dahil olmak üzere birçok alanda kullanılmaktadır. Bu cihazların çeşitliliğinin ve oluşturdukları internet trafiğinin artması bu cihazların yönetilebilirliğini zorlaştırmış ve birçok tehlikeyi de beraberinde getirmiştir. Dolayısıyla bu cihazların güvenliğinin sağlanması ve sürdürülebilir olması oldukça kritik bir öneme sahiptir.

Evlerimizde kullandığımız modemler cihazlarımızın internet bağlanmasını sağlayarak dış dünya ile iletişim kurmamızı sağlamaktadır. İnternet, faydalarının yanı sıra virüsler, yazılım açıklıkları, kötü niyetli kişilerin aktiviteleri gibi birçok sebepten ötürü sürekli bir tehdit olarak da görülmelidir. İnternet bağlantısını sağlayan modemler evlerimizde bulunan tüm cihazların birbirine bağlanabildiği ortak bir noktadır. Bu noktada oluşacak bir güvenlik problemi tüm internet trafiğinin dinlenmesine, kaydedilmesine veya incelenerek parola ve benzeri değerli bilgilerin ele geçmesine yol açabilir. Diğer yandan bu noktada sağlanabilecek güvenlik çözümleri işletim sistemi, yazılımı, türevi farketmeksizin tüm cihazların güvenliğinin sağlanmasına da olanak sağlayacaktır. Modemlerin yönetilebilirliği ise oldukça zordur ve doğru bir şekilde yapılandırılamaları global bir sorun olarak görülmektedir [1]. Yüzde yüz güvenlik gibi bir yargı mümkün olmamasına karşı, en başarılı ve sürekli güvenlik çözümleri uygulamak her zaman amaç edinilmelidir [2]. Modem, bu noktada internet ve diğer ağ cihazları arasında bir katman olarak bulunmakta ve katmanlı yapılar ile güvenliğin sağlanabilmesi açısındanda oldukça önemli bir konumdadır [3]-[4].



Şekil-1 Ev ve Ofis ağı cihazları örneği [5]

Bu çalışmamızda internet bağlantısı kurabilen mevcut cihazlarımız bilgisayar, cep telefonları gibi cihazların yanı sıra ev ve ofis ağımıza katılımı son zamanlarda gerçekleşen nesnelerin interneti cihazlarınında ağ geçitleri üzerinde güvenliklerinin sağlanması ve bu güvenliğin sürekli sürdürülebilirliği incelenmiş, yeni çıkan saldırılara karşı hızlı çözüm üretilmesi ve sürekli aktif savunma mekanizması oluşturulması için öneriler sunulmuştur.

II. EV AĞLARıNıN KARAKTERİSTİĞİ

Evlerimizde kullandığımız modemler ülkemizdeki internet altyapısında kullanılan internet iletişim için DSL teknolojisini kullanmaktadır. Kullandığımız modemlerde bir çeşit DSL Router görevi görmektedirler. Basit donanımlar üzerine geliştirilirler ve yönlendirici işletim sistemleri [6] bulundururlar. Genellikle üzerinde kablosuz internet (WiFi) dağıtımı sağlayan donanımlar bulunduran modemler, üzerinde basit güvenlik duvarı çözümüde bulunduran diğer ağ cihazlarına internetin dağıtımını sağlayan cihazlardır. Modemlerin üzerinde bulunan güvenlik duvarları, ağ saldırılarını önlemeye yöneliktir. İzinsiz bağlantılara karşı koruyucu amacıyla bulundurulan güvenlik duvarları iç ağın güvenli olmasını sağlamak içinde konumlandırılmış basit çözümlerdir [7]. Düşük maliyetle üretilmek istenmeleri sebepli modemlerde bulunan güvenlik duvarı ve diğer güvenlik çözümleri çok kapsamlı değildir. Düşük bant genişliğindeki internet trafiğini yönetmek için geliştirilen modemler, biraz karmaşık saldırılarda hizmet dışı kalabilmektedir.

III. EV KULLANıCıLARıNA YÖNELİK SİBER SALDıRıLAR

Son yıllarda ev kullanıcılarına yönelik doğrudan gerçekleştirilen ve ev kullanıcılarının cihazları aracı kullanılarak başka hedeflere gerçekleştirilen saldırılar da artışlar gözlenmektedir. Araştırmalara göre daha kolay hedefler olmaları sebebiyle ev kullanıcılarının kötü niyetli kişiler tarafından hedef olarak en fazla seçilen vektörlerden olduğu belirtilmektedir [8].

Ev kullanıcılarına yönelik en sık gerçekleştirilen siber saldırı tipleri, fidye yazılımları, oltalama saldırıları ve mobil zararlı yazılımlarla gerçekleştirilen saldırılar olarak öne çıkmaktadır [9]. Araştırmalara göre, mobil cihazların yüksek etkileşimli cihazlar olmalarına rağmen, mobil saldırılarda yaygınlaşmanın artmasının ve saldırılardaki başarı oranlarının yüksek olmasının en büyük nedeni, güvenlik zincirinin en zayıf halkası olarakta belirtilen insan kaynaklı olduğu belirtilmektedir [10].

Şekil-2 Yıllara göre yeni mobil zararlısı sayısı [11]

Fidye yazılımları (ransomware) ise son yıllarda kullanıcılara karşı doğrudan yapılan siber saldırılardan en çok rastlanılan saldırılar arasındadır. Kişilerin cihazlarına oltalama saldırıları

veya son dönemlerde görülen, Wannacry, Petya, NotPetya siber saldırılarında olduğu gibi [12-14] çeşitli yazılım zafiyetleri kullanılarak gerçekleştirilen ve cihazlara bulaştıkları anda güçlü şifreleme algoritmaları kullanarak dosyalar üzerinde şifreleme yaparak kullanılmaz hale getiren ve bu şifrelemelerin çözülmesi karşılığı olarak fidye talep eden yazılımlardır. İlk örnekleri CryptoLocker [15] ismi ile anılmaya başlayan fidye yazılımları günümüzde birçok cihaza bulaşmakta, veri kaybına ve maddi kayıplara yol açmaktadır.

Ünlü güvenlik firması Symantec'in güncel raporlarına göre ev kullanıcıları, fidye yazılımları ve mobil zararlı uygulamalar ile hedef alınmakta ve zarara uğratılmaktadır [16].

Çeşitli güvenlik ve haber kaynaklarına göre de hedef alınan ev kullanıcıları üzerinden ve ev kullancılarına karşı doğrudan birçok siber saldırı mevcuttur ve bu tür saldırıların katlanarak artacağı belirtilmektedir [17].

Oltalama saldırıları, fidye yazılımlarındanda önce çok yaygın şekilde gerçekleştirilen siber saldırıların başında gelmekteydi. Bir içeriğin klonu oluşturularak, kişilerin bu sayfalar üzerinden esas gidilmesi istenilen sayfalara giriş yapıyormuş gibi kandırılmaları veya kişilere asılsız vaatler ile virüslü dosyalar indirmeleri sağlanarak gerçekleştirilebilen bu yöntem, oldukça kolay uygulanabilen ve insan kandırma temeline yatması sebebiyle sosyal beceriler ile uygulanabilen bir siber saldırı tipidir. Fidye yazılımlarının büyük bir kısmının yayılma şekli de oltalama saldırılarından faydalanarak gerçekleştirildiğinden oltalama saldırılarının artış oranı önceki yıllara göre çok daha fazla olduğu gözlemlenmektedir. Kaspersky Lab araştırmalarına göre günümüzde gereksiz ve zararlı (spam) eposta trafiği tüm eposta trafiğinin %58,31'ini [18] oluşturmaktadır.

Ev kullanıcılarını doğrudan hedef almasa da birer saldırı elemanı olarak aracı şekilde kullanarak DDoS (distributed denial of service) ve Botnet ağlarına katılmalarını sağlanması ile hedeflere toplu saldırılar gerçekleştirilmesi son zamanlarda gündemde olan diğer siber saldırı tiplerinden birisidir. Çeşitli amaçlarla, kişilerin ele geçirilmiş cihazlarını toplu şekilde, uzaktan bir komuta merkezinden yönetilmesi sonucu yüksek trafik oluşturarak hizmet dışı bırakmaya yönelik saldırılar gerçekleştirilmektedir. En belirgin örneği, Mirai ddos saldırıları olarak geçen, varsayılan parolası değiştirilmemiş nesnelerin interneti cihazlarını ele geçirmiş kişiler tarafından gerçekleştirilen ve tarihin en büyük ddos saldırısı olarakta belirtilen saldırı tipidir [19],[20].

Literatürdeki bazı çalışmalarda [2],[3],[21] sunulan öneriler ticari güvenlik yazılım ürünlerine dayalı olup sadece yazılımsal olarak önerilmesi eksiğiyle birlikte evlerde kullanılacak güvenli modem veya modem için güvenlik katmanı oluşturacak ekstra bir cihaz için çok yüksek maliyet ortaya çıkması optimal bir çözüm olmayacağı öngörülmektedir. Diğer yandan bazı çalışmalarda [7],[22] önerilen yöntemler günümüzde geçerliliğini kaybetmiş veya güncel olmayan teknoloji ve protokollere dayanmaktadır.

Araştırmalara göre [23],[24] ev ağlarına karşı gerçekleştirilen saldırıların sayılarında ve çeşitlerinde çok yüksek bir artış söz konusudur. Tespit edilebilen saldırı tiplerinden tamamı ev kullanıcılarını doğrudan hedef saldırılar arasında yer almaktadır.

Ev kullanımı için uygun yazılımlar, ZoneAlarm, Norton, HSSIN ve benzeri uygulamalar cihaz bağımlı çalışan, bulunduğu cihaz üzerinde güvenlik sağlayan uygulamalardır. Bir masaüstü bilgisayar için uygun bir çözüm olan bu tür yazılımlar mobil platformları veya günümüzde gittikçe yaygınlaşan nesnelerin interneti cihazlarını desteklememektedir.

IV. SİBER SALDıRıLARıN ETKİLİ OLMASıNDAKİ ETKENLER

Günümüzde her üç siber saldırı denemesinden birinin başarılı olduğu ve bu saldırıların %95 oranında insan hatasının bir sonucu ile başarıya ulaştığı belirtilmektedir [25]. Siber saldırıların gerçekleşmesinde ve etkili olmasında şu etkenler öne çıkmaktadır;

- Donanım güncelliğinin sağlanamaması,
- Yazılım güncellemelerinin gerçekleştirilmemesi,
- Bilinçsiz kullanıcı,
- Hatalı veya eksik yapılandırmalar,
- Ulusal ve uluslararası düzenlemelerde eksiklik,
- Uluslararası yaptırımların etkisiz olması,
- Sağlayıcıların altyapı yetersizliği,
- Güncel saldırılara karşı adaptasyon eksikliği,
- Bilginin paylaşımı noktasında otoriter eksiklik.

A. Donanımsal Kısıtlar ve Eksiklikler

Nesnelerin interneti cihazlarına yönelik saldırıların karakteristik yapıları incelendiğinde henüz bu kategoride bulunan cihazların güvenlik açısından çok yetersiz kaldığı söylenebilir. Düşük güç tüketimi ve basit donanımsal yapıları nedeniyle bu tür cihazlar üzerinde bir güvenlik çözümü üretmek oldukça zordur. Özellikle donanımsal olarak sensörler gibi daha küçük ve basit yapılarda bu durum daha zor ve karmaşıktır [26],[27].

Akıllı televizyonlar üzerine yapılan bir araştırmada, akıllı televizyonlardaki, güvenlik sorunlarının nedeni olarak,

- Antivirüs yazılımı bulunmaması,
- Güvenlik duvarı gibi bir çözümün bulunmaması,
- Yazılım güncelleme desteğinin yeterince hızlı olmaması,
- Güvenlik güncelleştirmelerinin öneminin düşük tutulması sebepli geç verilmesi maddeleri belirtilmiştir [28].

Basit işletim sistemlerini çalıştırması için geliştirilmiş basit donanımlara sahip olmaları sebebiyle akıllı televizyonlar üzerinde bir güvenlik çözümünün geliştirilmesi çok fazla mümkün olmadığından uygulanması gereken çözümlerin bu cihazlar dışında gerçekleştirilmesi zorunluluğu göze çarpmaktadır. Aynı durum tüm nesnelerin interneti cihazları içinde geçerli-

dir. Düşük güç tüketimi ve basit donanım, karmaşık güvenlik çözümleri için yetersiz kalmaktadır.

Yapılan çalışmalar [29-31] ve gerçekleştirilen saldırılar incelendiğinde [2],[32-33] evlerde ağ geçidi görevi gören modemler üzerinde nesnelerin interneti cihazlarını da kapsayan daha güçlü bir güvenlik katmanı sağlanması oldukça doğru bir çözüm olacaktır. Ağ geçidi üzerinde sağlanacak güvenlik önlemleri ile mevcut ağ cihazları bilgisayarlar, cep telefonları, akıllı saatler ve televizyonlar gibi cihazlarda doğrudan daha güvenli bir ağ ortamına sahip olacaktır.

B. Yazılımsal Kısıtlar ve Eksiklikler

Ev ağları kablolu ve kablosuz iletişim teknolojilerini birlikte içermektedir. İnternete bağlanabilen tüm cihazlar bir ağ geçidi üzerinden bir İP (Internet Protokolü) tahsis edilerek iletişim kurar. İnternet erişiminin sorunsuz ve kesintisiz yapılmasını sağlayan modemler, üzerlerinde bulunan DHCP sunucuları ile kendisi ile iletişime geçen cihazlara İP sağlayarak ağ oluşturur ve kimlik doğrulama mekanizmalarını tamamlamaları halinde bu cihazların internete bağlanmalarına veya iç ağda diğer cihazlar ile iletişim kurulmasına olanak sağlanmış olur. Modemlerin dış dünya ile iletişim kurabildikleri yanlızca bir İP adresleri olur. İç ağda ise her cihazın modemle ve diğer cihazlarla iletişime geçebildiği belirli bir aralıktan belirlenen İP havuzundan aldığı bir İP adresi olur.

Doğal internet trafiği oluşturmanın dışında, ağ üzerinde İP adreslerini manipüle eden cihazlar olması durumunda eğer ağ geçidi üzerinde gerekli güvenlik önlemleri alınmaz ise ağ trafiği;

- Dinlenebilir,
- Kaydedilebilir,
- Yönlendirilebilir,
- Engellenebilir,
- Değiştirilebilir,
- Bütünlüğü bozulabilir,
- Zararlı hale getirilebilir.

Sadece iç ağda birbirleri arasında iletişimde olan cihazlarla sınırlı kalmamak üzere, internet iletişimi kuran cihazlar için de ağ trafiğinde aynı tehlikeler söz konusudur. Bu yüzden ağ geçidi üzerinde gerekli önlemlerin alınması önemlidir. Ağ trafiği üzerinde belirtilen güvenlik tehditleri gerçekleştirilerek gözlemlenen başlıca siber saldırı tipleri, İP sahteciliği (IP spoofing), ARP sahteciliği (ARP spoofing), ARP zehirlemesi (ARP Poisining), DHCP sahteciliği (DHCP spoofing) ve trafik tünelleme/yönlendirme (traffic tunneling/routing) gibi saldırılardır [34].

Bu tür saldırılar için çözüm ağ geçidi üzerinde yapılandırma işlemlerinin yapılabilmesine olanak sağlayan yazılım/işletim sisteminin bulunması ve doğru bir şekilde yapılandırılmasıdır.

Sadece basit ve statik kurallar üzerine kurulu güvenlik duvarı çözümleri tek başına aktif bir güvenlik çözümü olarak yeterli kalmayabilir. Yeni tehditlere karşı kendisini güncel tutabilen yazılımlar ancak doğru güvenlik çözümü olarak kabul edilebilir.

C. Yasal Düzenlemeler

Siber güvenlik ve bilgi güvenliği konuları geçtiğimiz son birkaç yıl içerisinde önemi anlaşılmış fakat henüz yeterli aksiyonların alınmadığı alanlardır. Siber güvenlik üzerine yazılı ilk eylem planları 2000'li yılların başında yazıya dökülmüş ve hayata geçirilmiştir [35]. İlk olarak Rusya ve Amerika'nın yayınladığı eylem planları ülkemizde ilk olarak 2013 yılında yayınlanmıştır. Bu eylem planına göre SOME (Siber Olaylara Müdahale Ekibi) ekipleri planı hayata geçirilmiştir [36]. Günümüzde USOM (Ulusal Siber Olaylara Müdahale Merkezi) olarak isimlendirilen BTK'ya (Bilgi Teknolojileri ve İletişim Kurumu) bağlı birim, güncel siber güvenlik tehditlerini paylaşmakta ve duyurular yayınlamaktadır. Ayrıca zararlı trafik oluşturan adresleride güncel olarak yayınlayan bu birim, yazılımsal olarak kolayca entegre edilebilir çözümler sunarak güvenlik birimleri için kolaylıklar sağlamaktadır. Fakat bu çözümler ancak uygulandığında noktada başarılı sayılabililir. Güvenlik duyurularının, uyarılarının ve bilgi paylaşımlarının olduğu USOM platformu, evlerde sağlanabilecek güvenlik çözümlerine bireyler seviyesinde bir katkı sağlamamaktadır. USOM tarafından yayınlanan listeler ve uyarılar ev güvenliğini sağlamada kullanılan çözümlerde kullanılmamaktadır.

https://www.usom.gov.tr/url-list.xml (1)

Ülkemizde ev kullanıcılarına internet sağlayıcısı olarak üç büyük firma ve yerel küçük firmalar bulunmaktadır. Bunlar, Turkcell (Superonline), Türk Telekom ve Vodafone firmalarıdır. Yasal düzenlemeler ile sağlayıcıların kullanıcı profiline göre güvenli internet hizmeti çözümleri getirmeleri sağlanmıştır. Bunun yanı sıra çeşitli güvenlik çözümlerini ekstra ücretler ile sundukları bilinmektedir. TCP/IP'nin çaresiz kaldığı noktalar arasında özellikle sahtecilik (spoofing) konuları önemli bir konumdadır [37] [38]. Birçok yapı üzerinde, genellikle UDP protokolü kullanılarak, SYN, ACK, FIN (flood) ve İP sahteciliği gibi siber saldırıların gerçekleştirilmesi oldukça basittir. Bu konularda yasal düzenlemeler bulunmaması sebebiyle zafiyetli yapılarda bu tür saldırılar yapılabilmektedir. Daha tehlikelisi ise Botnet ağları üzerinden gerçekleştirilen bu tür saldırıların sistemler üzerinde etkisi çok daha yüksek olmaktadır.

6698 numaraları Kişisel Verilerin Korunması Kanunu ile belirtilen tüm maddelere uygunluğun sağlanması, geliştirme açısından önemlidir. Bu yüzden geliştirilmesi düşünülen veya herhangi bir bilgi trafiği üreten bir sistemde kişisel bilgilerin bulunmaması ve mahremiyetin sağlanması esas alınmalıdır.

V. ÇÖZÜM ÖNERİSİ

Gelişen teknolojiler ile birlikte ev ağlarımızdaki cihaz sayısı ve çeşitliliği artmıştır. Farklı karakteristiklerde birçok cihaz bu-

lunmaktadır. Bütün bu cihazları ortak noktada buluşturan ise internete bağlanmalarını sağlayan modemlerdir. Modemler üzerinde güvenliği sağlanması ve mevcut modemlerin üzerinde geliştirmeler sağlayarak güvenliğin artırılması oldukça optimal bir çözüm olacaktır. Yapılan çalışmalarda incelendiğinde [39],[40],[20] özellikle son yıllarda sayıları artan nesnelerin interneti cihazlarıyla birlikte ev modemlerine veya diğer ağ cihazlarına ek, daha güçlü ve esnek bir güvenlik çözümü geliştirmek ve kullanmak kaçınılmaz olmuştur.

A. Açık Kaynak Kullanımı Önerisi

Açık kaynak kodlu ve özgür yazılım geliştirmek, teknoloji dünyasında aslında uzunca bir süredir var olan fakat son yıllarda daha çok popüler hale gelen bir yazılım geliştirme metodolojisidir. Bir yazılımın özgür olarak adlandırılabilmesi için yazılımın kullanıcının temel özgürlüklerine önem vermesi, kullanıcıyı ön planda tutması ve kullanıcıyı kısıtlamaması gerekmektedir. Kullanıcılara, çalıştırma, kopyalama, dağıtma, inceleme ve geliştirme özellikleri sunan yazılımlar özgürdür [41]. Açık kaynak kodlu yazılımlar geliştirilmek istenmesinde bir çok sebep bulunabilir, bunlardan başlıcaları, kalite, topluma katkı sağlama, ortak çalışılabilirliği sağlama, açıklık (şeffaflık), esneklik ve özelleştirilebilirliktir [42]. Açık kaynaklı yazılımların daha güvenli olup olmadığı ile ilgili tartışmalar sürmekle birlikte birçok ülke ve kuruluş bu konuda açık kaynaklı yazılımların tarafı olmaktadır. Bunlardan başlıcaları şu şekildedir;

- Amerika, açık kaynak kodlu yazılım platformu oluşturarak kamudaki kurumlarda bu yönde bir kullanım eğilimi oluşturmayı hedeflemektedir [43].
- Bulgaristan, kamuda kullanılacak tüm yazılımlar için açık kaynak kodlu olmayı zorunlu tutmaktadır [44].

Ülkemizde ise, kamuda açık kaynak kodlu yazılımların kullanımı ile ilgili Kalkınma Bakanlığı tarafından yapılan bir çalışmada, açık kaynak kodlu yazılımların kamu için öneminden aşağıdaki maddelerle sınıflandırılarak bahsedilmektedir [45].

- Güvenilirlik; Sistemin kullanıcı müdahalesi olmaksızın çalışabilir olması
- Kalite; Kodlamadaki toplam hata sayısının azlığı
- Güvenlik; Yazılımın diğer etkenlere göre sağladığı koruma
- Esneklik; Yazılımın müşteri taleplerine yanıt verebilirliği, değişikliklere açık olması
- Proje Yönetilebilirliği; Yazılım geliştirme sürecinin yönetilebilirliği
- Açık Standartlar; Yazılımlar aracılığı ile oluşturulan parçaların modülerliği
- Vazgeçme/Cayma Maliyeti; Bir yazılımdan diğerine geçme maliyetinin düşük olması
- Toplam Maliyet; Yazılımın kurulumu, bakımı ve vazgeçilmesi içi gerekli toplam maliyet
- Kullanıcı Dostu Olması; Yazılımın kolay kullanım imkanı sunması

Artan popülerliği ve güvenlik esaslı olmaları sebebiyle açık kaynak kodlu yazılımların her geçen gün daha fazla tercih edileceği ve açık kaynak kodlu yazılım geliştirmenin daha ön planda tutulabileceği söylenebilir.

Açık kaynak donanım ve yazılım tercihi ile birlikte geliştirilecek uygulama için güvenliğin daha iyi bir şekilde sağlanması, dünya üzerindeki tüm geliştiricilerden destek alınabilmesi, geliştirme katkısı elde edilmesi ve kodun herkes tarafından incelenerek en başarılı kod parçacıkları tercih edilerek birlikte geliştirmeye olanak sağlanmasıyla mümkündür. Açık kaynak kodlu olması bir yazılımı daha güncel tutmak ve daha stabil tutmak için oldukça önemli bir artıdır. Zamanla ihtiyaç olarak doğan özellik eksikliklerinin veya hatalı parçaların dünya üzerindeki herkes tarafından katkı sağlanarak tamamlanması oldukça önemli bir tercih sebebidir.

A.1 Donanım Seçimi

Ev ağları ve küçük/orta büyüklükteki işletmelerin ağları için ağ trafiği çok yüksek değerlerde değildir. Ülkemizde sağlayıcılar tarafından sağlanan en yüksek hızların 100 Mbit/s civarında olduğu bilinmektedir. Çok yüksek değerler olmayan bu bant genişliğini işleyebilen ve yönetebilen, ucuz ve kapsamlı donanımlar mevcuttur. Günümüzde uygulama geliştirmede popüler ve küçük nesnelerin interneti ağı oluşturmak için kullanılan tek kart bilgisayarlar bu tür bir platform geliştirmede yeterli donanımsal özelliklere sahiptir. Günümüzde küçük, tek kart bilgisayarlar (board) olarakta adlandırılan bu cihazların başlıcaları, Raspberry Pi, Orange Pi, PcEngine ve yerli kart Poyraz gibi donanımlardır. Bu tür cihazlar modemlerle birlikte veya modem yerine, ağ geçidi görevinde kullanımaları noktasında doğru bir çözüm olacaktır. Linux ve Unix türevi işletim sistemlerini çalıştırabilmeleri sebebiyle bu tür donanımlar esnek bir yapı sunarak üzerlerinde kapsamlı geliştirmeler yapılmasını da mümkün kılmaktadır.

A.2 Yazılım Seçimi

Günümüzde çeşitli ağ işlemlerini yerine getirmek üzere geliştirilmiş birçok işletim sistemi bulunmaktadır. Bunların birçoğu Linux veya Unix türevi işletim sistemleri olarak göze çarpmaktadır. En çok bilinen ve kullanılan yönlendirici, modem ve güvenlik duvarı görevinlerini üstlenmek için kullanılan işletim sistemleri; Pfsense, OpenWrt, VyOs ve Endian Firewall işletim sistemleridir [46]. PfSense işletim sistemi ve bütünleşik güvenlik çözümü açık kaynak kodlu olup 2004 yılından beri geliştirilen ve küçük büyük birçok yapıda kullanıldığı bilinen Unix türevi bir işletim sistemidir. Yine açık kaynak kodlu güvenlik çözümü olan Snort, saldırı tespit ve engelleme sistemi ile entegre çalışabilen pfSense, yönlendirici, yük dengeleyici ve güvenlik duvarı gibi birçok amaçla kullanılabilir. Saldırı tespit ve engelleme sistemleri olarak birçok açık kaynak kodlu

çözüm bulmak mümkündür. En bilinen çözümler, Snort, Suricata, Ossec ve Bro NIDS çözümleridir [47]. Pfsense gibi bir bütünleşik güvenlik çözümü ile birlikte kullanıldıklarında ağ trafiği üzerinde paket analizi gibi detaylı incelemeler gerçekleştirerek hızlı ve aktif çözüm üretmede daha başarılı bir uygulama haline gelebilmektedirler.

Yazılım seçiminde dikkat edilmesi gereken kurallardan birisi de uygun donanım mimarisinde çalışabilen işletim sistemi seçmek ve yazılım konusunda geliştirme uygulanacak kapsam ve detaya göre işletim sistemi performansına dikkat etmek gereklidir. Derinlemesine paket analizi (deep packet inspection) yapılabilmesi için donanım seviyesinde uygun miktarda hız ve performans gereksinim bulunmaktadır. İncelenen çalışmalar ve işletim sistemleri karakteristikleri ışığında en uygun işletim sistemi/yazılım çözümü Pfsense olarak dikkat çekmektedir fakat bu işletim sistemi donanımsal olarak belirtilen kartların büyük bir çoğunluğunda uygun mimari bulunmadığı için çalışmamaktadır. Pfsense, FreeBSD tabanlı olup AMD64 ve i386 mimarisi işlemcilerde çalışmaktadır [48]. PcEngine haricindeki kartların neredeyse tamamı ARM mimarisi işlemciler bulundurmaktadırlar. Saldırı tespiti ve engellemesi için en iyi çözümlerden birisi olan Snort, pfSense çözümü ile birlikte kullanılarak yüksek başarı elde edilmesi mümkündür.

B. Geliştirme ve Özelliklerin Belirlenmesi

Kurumsal olmayan, bilgi ve iletişim teknolojilerine sadece kullanıcılar olarak katılım sağlayan bireyler için en basit ayarla çalışabilecek, anlaşılır ve kendi kendini idame edebilen bir güvenlik çözüm geliştirilmesi kaçınılmazdır. Ortalama olarak 100Mbit/s bant genişliğine sahip ağlar için geliştirilmesi planlanan bu çözümde kullanım olarak basitlik düşünülürken, olası güvenlik sorunları için yüksek karmaşıklıkta ve büyüklükte siber saldırılarında gerçekleşebileceği unutulmamalıdır.

Geliştirme yapılırken, saldırı tespit ve engelleme sistemlerinden faydalanılmalı basit seviyede de olsa makine öğrenmesi gibi yöntemler kullanılarak karmaşık saldırı tipleri de tespit edilmeye çalışılmalıdır. Bu tür yöntemler anomali tespiti yaparak belirli bir düzene eşleşen bağlantılara karşı aksiyon, gerektiğinde zararlı bağlantıları tamamen kesen güvenlik çözümleridir. Doğru ayar yapılandırmaları yapılmayan bu sistemler ağı kullanılmaz hale getirebilmektedir. Düzgün yapılandırma yapmak bu konuda önemli hususlardandır.

	DoOS (%)	Bilgi Tarama (%)	R2L (%)	U2R (%)
Bayes	%99,62	%100	%99,35	%99,47
DVM	%100	%100	%99,42	%100
Karar Ağaçları	%99,98	%99,66	%99,70	%92.50
YSA	%100	%100	%99,88	%99,85

Tablo-1 Saldırı tiplerine göre makine öğrenmesi algoritmalarının başarı yüzdeleri

Yapılan bir çalışmada [49] farklı siber saldırı türlerine göre makine öğrenme algoritmalarının tespit yüzdeleri Tablo 1'de belirtilmiştir. Bu çalışmanın sonucuna göre en başarısız olarak nitelendirilebilecek algoritmada bile yüksek saldırı tespit edebilme oranları görmek mümkündür. Bu algoritmaların kullanılması, işlemsel olarak bir yük oluştursa da yüksek başarımları sebebiyle tercih edilmeleri gerekliliği göz önünde bulundurulmalıdır.

Geliştirme aşamasında uygulanması büyük katkı sağlayacak diğer çözümler ise şu şekildedir;

- Fidye yazılımları önleme teknikleri uygulanması
- Bant genişliği üzerindeki sınırlamalar ve kısıtlamalar (Rate Limiting)
- Erişim kontrol listeleri uygulanması
- USOM zararlı siteler listesi Uygulaması
- Shodan, NMAP, Nessus vb. uygulamaların kullanıcı ajanlarının engellenmesi
- Dünya geneli zararlı yayın yapan ip listelerin uygulanması
- Modem Güvenlik Duvarı, Keşif tabanlı ip öğrenme ve sahteciliği reddetme yöntemleri uygulanması
- Botnet ağı aktivitesinde uyarı sistemi ve önleme
- ARP sahteciliği, MAC değiştirme önleme çözümleri
- İç ağ erişim kısıtlama ve sınırlama
- Limitleme uygulamaları (limit burst) ile DDoS tespit etme ve önleme
- Zararlı eposta bağlantı tespiti ve önleme
- Spam listeleri ile entegrasyon ile zararlı site ve ip listelerinin engellenmesi
- Port numarasına / servislere göre bağlantı sayımı gerçekleştirilmesi ve düzen (pattern) tespiti ile zararlı bağlantıların engellenmesi
- Geliştirilecek donanımın ve yazılımın devre dışı bırakılması veya atlatılması gibi doğrudan üzerine gerçekleştirilecek saldırıların önlenmesi çözümleri ürteilmesi

Belirtilen tüm başlıkların uygulanması belirtilen alanlarda doğrudan bir güvenlik sağlama başarısı göstermese dahi saldırı tespit sistemi veya güvenlik yazılımlarına bilgi sağlaması, geliştirilmek istenilen çözüm için büyük oranda katkı sağlayacaktır.

Linux sistemi üzerine kurulması planlanması sebebiyle, geliştirilen sisteme USOM'un paylaştığı zararlı adresler listesi gibi yerel ve uluslararası çözümler entegre edilerek güvenlik seviyesi artırılabilir. Bu tür bir çalışma, kurumsal ağlarda eposta hizmetinde güvenlik sağlamak amacıyla geliştirilmiştir [50]. Ev kullanıcıları içinde benzer bir güvenlik katmanı sağlanması fidyeci yazılımlar ve oltalama saldırıları başta olmak üzere birçok güvenlik problemine karşı korunma sağlayacaktır.

Benzer şekilde uluslararası listelerde mevcuttur. Detaylı araştırmalar yapılarak bu tür entegrasyonların sayısı artırılabilir.

USOM tarafından sağlanan bu hizmetin ağ geçitleri üzerindeki entegresi ise oldukça kolaydır, belirtilen site adresleri için web ve eposta sunucuları ip adresleri belirlenerek, ip adresleri içinse doğrudan engelleme yapılması mümkündür.

Kurumsal ağlarda log kayıtlarını toplayarak, anlamlandırılmasını sağlayan ve bu log korelasyonlarına göre gerekli uyarı mekanizmalarını gerçekleştiren güvenlik sistemlerine SIEM (Security Information and event management) denir. SIEM sayesinde, siber olayların tespiti kolaylaşır ve uyarı mekanizmaları ile erken müdahale mümkün olur. Ev ağları için, ev kullanıcıları siber olayarlara müdahale kabiliyetinde değildir fakat internet sağlayıcıları bu kapasite ve kabiliyete sahiptir. Ayrıca, bir seviyeye kadar otonom müdahale modemler tarafından da çeşitli algoritmalar kullanılarak gerçekleştirilebilir. Erişim sağlayıcılarının anomaliler üzerine detaylı incelemeleri sonucu ağda çeşitli güvenlik yapılandırmaları yaparak daha güvenli internet trafiği sağlaması mümkündür. Fakat bu konuda kapsamlı bir çalışma yapılması gereklidir. Kişisel verilerin korunması kanunu çerçevesinde, mahremiyeti ihlal etmeyecek ve bu yapılandırmaları mümkün kılan altyapı çalışmaları gereklidir.

Shodan başta olmak üzere, ZoomEye, Censys, PunkSpider gibi internetteki tüm ip adreslerini tarayarak, bulunan tüm bilgilere göre veritabanı oluşturan arama motorları kötü niyetli kişiler için tehdit oluşturmaktadır [51]. Bu tür arama motorların geliştirilme amacı eğitim ve araştırma gayesi gütmesine karşın günümüzde daha çok kişilerin siber saldırı kabiliyetlerini geliştirme çabası ile testler ve denemeler yaptıkları platformlar haline gelmişlerdir.

Shodan üzerinde Türkiye'de tespit edilen tüm İP adreslerini listelemek için bu arama etkileti kullanaılabilir:

country:"TR" araması

https://www.shodan.io/search?query=country%3A%22TR%22 (2)

Türkiye için yaklaşık dört milyon kayıtın bulunduğu bu veritabanı, kötü niyetli kişiler için oldukça iyi bir kaynaktır. Bu tür kaynakların erişiminde kısıtlamaların bulunması ve modemler üzerinde bu tür aramalar gerçekleştiren arama motorları ve zafiyet tarama sistemlerinin imzalarına göre engellemelerin getirilmesi başarılı bir çözüm olacaktır. Linux tabanlı işletim sistemlerinde bulunan iptables, bu tür güvenlik kuralları ve politikaları oluşturulmasına olanak sağlamaktadır.

Iptables -I INPUT -p tcp --dport 8080 -m string --algo bm --string shodan -j DROP (3)

Bu şekilde oluşturulabilecek kurallar ile User-Agent bazlı engellemeler yapılabilir.

Iptables -I INPUT -s 222.111.0.0/255.255.0.0 -j DROP (4)

Bu şekilde oluşturulabilecek bir kural ile de bu tür arama motorlarının kullandığı İP adresleri bloğu engellenerek bilgi toplanmasının önüne geçilmiş olunur.

Kritik öneme sahip diğer bir parça ise bulunduğu konum gereği basit seviyede kalsa bile makine öğrenmesi yöntemleri ile güvenlik araçlarını akıllı hale getirmek daha akılcı bir çözüm olacaktır. Güncel çalışmalardan birkaçı incelendiğinde, basit seviyede [49] [52] makine öğrenmesi ile geliştirilecek çözümler bile saldırı tespit etmede etkin rol oynayacaktır. Önemli bir nokta, kullanılacak cihazın işlem ve depolama kapasitesine göre doğru algoritma tercihi ve öğrenme sürecinin mevcut veri setleri ile bir seviyeye kadar getirilmiş olmasın diğer bir deyişle eğitilmiş olması büyük katkı sağlayacaktır. Diğer bir yandan saldırganların makine öğrenmesi tekniklerini atlamak üzerine çalışmalarınında [53] olduğunu da hesaba katarak çeşitli yöntemleri bir araya getirmek daha başarılı bir çözüm olacaktır.

VI. DEĞERLENDİRME VE SONUÇ

Ev kullanıcıları son yıllarda birçok siber saldırı tehditi ile karşı karşıya kalmıştır. Global çapta gerçekleştirilen bu saldırılar kişilerin cihazlarına zarar vermekle kalmamış fidye talebi içeren daha karmaşık ve güçlü yapıda saldırılara evrimleşmiştir. Mirai DDoS saldırısında görüldüğü gibi yüksek sayıdaki ele geçirilmiş cihaz kullanılarak çok büyük kurumsal ağların hedeflenmesi ve saldırı sonucunda hizmet dışı bırakma işleminde başarı elde edilmesi, CryptoLocker, Wannacry gibi kişilerin bilgisayarındaki dosyaların çok güçlü şifreleme yöntemleri ile şifrelenerek fidye talep edilmesi saldırılarında ancak fidye taleplerinin karşılanması ile çözümün sağlanabilmesi gibi örnekler nedeniyle ev kullanıcılarının, kurumsal ağlar kadar güvenlik gereksinimi duyduğu apaçık görülmektedir.

Bu çalışmamızda ev ve ofis ağına yeni katılan cihazlarla birlikte güvenlik konusunda yapılabilecek geliştirmeler ve zorluklar gözden geçirilmiştir. Son yıllarda ev kullanıcılarına yönelik gerçekleştirilen siber saldırıların karakteristik yapısı incelenmiştir.

Tüm bu bilgiler ışığında ev ağlarının daha güvenli hale getirilmesi için bir güvenlik çözümü geliştirmesi önerisi sunulmuştur. Açık kaynak kodlu ve makine öğrenmesi algoritmaları kullanılarak geliştirilmesi önerilen bu sistemde hem donanımsal olarak hemde yazılımsal olarak açık kaynağın sahip olduğu güvenilirlik, şeffaflık, esneklik ve kaliteli olma özellikleriyle yüksek başarı hedeflenmiştir. Yasal çerçevede de düzenlemeler önerilen bu çalışmamızda dünya çapında gerçekleştirilen saldırıların yapısı ve tahrip etkileri göz önünde bulundurularak teknik çözümler üretilmesine yönelik önerilere yer verilmiştir.

KAYNAKLAR

[1] Calvert L. K., Edwards W. K., Feamster N., Grinter R. E., Deng Y., Zhou X.,"Instrumenting Home Networks" ACM SIGCOMM Computer Communication Review, 2011

[2] Munson, S. "Defense in Depth and the Home User: Securing the Home PC", SANS Institute 2003

[3] Taylor D. S., "Multi-Layered Approach to Small Office Networ-

king", GSEC Practical Version 1.3, SANS Institute 2002

[4] Çevrimiçi: http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/ Son Erişim Tarihi: 15 Temmuz 2017

[5] Rivas M. L., Kliarsky A., "Securing the Home IoT Network" SANS Institute, 2017

[6] Yönlendiriciler, T.C. Milli Eğitim Bakanlığı, Bilişim Teknolojileri, Ankara, 2013

[7] Wang B., Lu K., Chang P., "Design and Implementation of Linux Firewall Based on the Frame of Netfilter/IPtable", The 11th International Conference on Computer Science & Education (ICCSE2016) August 23-25, Japan, 2016

[8] Çevrimiçi: https://www.itnews.com.au/news/cyber-crooks-switch-to-soft-target-home-users-60613 Son Erişim Tarihi: 15 Temmuz 2017

[9] Çevrimiçi: http://www.isaca.org/Education/Online-Learning/Pages/Webinar-2015-Mobile-Threat-Report-The-Rise-of-Mobile-Malware.aspx Son Erişim Tarihi: 15 Temmuz 2017

[10] Arabo A.,"Cyber Security Challenges within the Connected Home Ecosystem Futures", Conference Organized by Missouri University of Science and Technology, San Jose 2015.

[11] Çevrimiçi: https://www.mcafee.com/us/security-awareness/articles/mobile-malware.aspx Son Erişim Tarihi: 15 Temmuz 2017

[12] Gabriel A., Shi J., Ozansoy C.,"A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method" College of Engineering and Science, Victoria University, Australia

[13] Çevrimiçi: https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

[14] Çevrimiçi: https://motherboard.vice.com/en_us/article/evdxj4/notpetya-ransomware-hackers-decrypt-file

[15] T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, "CryptoLocker virüsü hakkında bilgi notu", Çevrimiçi: http://www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf Son Erişim Tarihi 15 Temmuz 2017.

[16] Çevrimiçi: https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0802_02 Son Erişim Tarihi: 27 Ağustos 2017

[17] Çevrimiçi: https://www.symantec.com/about/newsroom/press-releases/2017/skycure_0509_01 Son Erişim Tarihi: 27 Ağustos 2017

[18] Çevrimiçi: https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/ Son Erişim Tarihi 15 Temmuz 2017.

[19] Kolias C., Kambourakis G., Stavrou A., Voas J., " DDoS in the IoT: Mirai and Other Botnets ", The IEEE Computer Society, 2017

[20] Jerkins J. A.,"Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code", Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual

[21] Krein D., "Layers of Defense for the Small Office and Home Network" 24 Temmuz 2001, SANS Institute

[22] Rosslin J. R., Tai-hoon K., "A Review on Security in Smart Home Development", International Journal of Advanced Science and Technology, Şubat 2010.

[23] Pan Y., Liang J., Xu L., "A study on intelligent housekeeper of smart home system", 2017 9th International Conference on Measuring Technology and Mechatronics Automation

[24] Bendovschi A., "Cyber-Attacks – Trends, Patterns and Security Countermeasures", 7th International Conference on Financial Criminology 2015, United Kingdom.

[25] Çevrimiçi: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ Son Erişim Tarihi 15 Temmuz 2017.

[26] "Exploiting the Physical Environment for Securing the Internet of Things", Zenger C. T., Zimmer J., Pietersz M., Posielek J. F., Paar C., Proceedings of the 2015 New Security Paradigms Çalıştay, Sayfa 44-58, Almanya.

[27] "A Reference Architecture for the Internet of Things", Fremantle P., WSO White Paper, Ekim 2015.

[28] Ulu, A., Ciylan B.,"Akıllı Televizyonlar Üzerine Güvenlik İncelemesi" 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2016, Ankara.

[29] Çevrimiçi: "The Internet of Things and the Inevitable Collision with Product Liability PART 5: Security and the Industrial Internet Consortium" http://www.productliabilityadvocate.com/2015/11/the-internet-of-things-and-the-inevitable-collision-with-product-liability-part-5-security-and-the-industrial-internet-consortium/ Son Erişim Tarihi: 15 Temmuz 2017

[30] Çevrimiçi: "How the Internet of Things will change physical security" http://www.amsterdamsecurity.com/en/news/article/how-the-internet-of-things-will-change-physical-security/ Son Erişim Tarihi: 15 Temmuz 2017

[31] Çevrimiçi: "Mainframe and the inevitable attack of the Internet of Things" http://blogs.ca.com/2016/12/12/mainframe-inevitable-attack-internet-things/ Son Erişim Tarihi: 15 Temmuz 2017

[32] Komninos N., Philippou E., Pitsillides A., "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures", IEEE Communications Surveys & Tutorials (Volume: 16, Issue: 4, Fourthquarter 2014)

[33] Pawar M. V., Anuradha J., "Network Security and Types of Attacks in Network", International Conference on Intelligent Computing, Communication & Convergence, 2015.

[34] Ornaghi A., Valleri M., "Man in the middle attacks", Blackhat Conference - Europe 2003

[35] Çevrimiçi: https://ccdcoe.org/cyber-security-strategy-documents.html Son Erişim Tarihi: 15 Temmuz 2017

[36] Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı

[37] Osanaiye O. A., Dlodlo M., "TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment", EUROCON 2015 - International Conference on Computer as a Tool (EUROCON)

[38] Mopari I. B., Pukale S. G., Dhore M. L., "Detection and defense against DDoS attack with IP spoofing", International Conference on Computing, Communication and Networking, 2008.

[39] Saxena U., Sodhi J. S., Singh Y., "Analysis of security attacks in a smart home networks", Cloud Computing, Data Science & Engineering - Confluence, 2017 7th International Conference

[40] Ungar S. G., "Home Network Security", IEEE 4. International Workshop on Networked Appliances, 2001.

[41] İnternet: "GNU Kullanıcıları" http://www.gnu.org/gnu/gnu-users-never-heard-of-gnu.tr.html Son Erişim Tarihi: 15 Temmuz 2017

[42] http://www.pcworld.com/article/209891/10_reasons_open_source_is_good_for_business.html Son Erişim Tarihi: 15 Temmuz 2017

[43] İnternet: "The Forge.mil Program" http://www.forge.mil Son Erişim Tarihi: 15 Temmuz 2017

[44] İnternet: "Bulgaristan'da açık yazılım yasası" https://www.dunyahalleri.com/bulgaristanda-acik-yazilim-yasasi/ Son Erişim Tarihi: 15 Temmuz 2017

[45] Özdaş, M. R., Kamuda Açık Kaynak Kodlu Yazılım Kullanımı, T.C. Kalkınma Bakanlığı.

[46] Palazzi C. E., Matteo Brunati M., Roccetti M.,"An OpenWRT solution for future wireless homes", Multimedia and Expo (ICME), 2010 IEEE International Conference

[47] Albin E., Neil C. Rowe N. C., "A Realistic Experimental Comparison of the Suricata and Snort Intrusion-Detection Systems", Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference

[48] https://www.netgate.com/blog/category.html#hardware Son Erişim Tarihi: 15 Temmuz 2017

[49] Raja F., Hawkey K., Jaferian P., Beznosov K.,, Kellogg S., "BoothIt's Too Complicated, So I Turned It Off! Expectations, Perceptions, and Misconceptions of Personal Firewalls", University of British Columbia, Canada, 2010

[50] Çevrimiçi: http://blog.oguzhan.info/?p=1066 Son Erişim Tarihi: 15 Temmuz 2017

[51] Çevrimiçi: http://alternativeto.net/software/shodan/ Son Erişim Tarihi: 15 Temmuz 2017

[52] Çatak F. Ö., Mustaçoğlu A. F., "Derin Öğrenme Teknolojileri Kullanarak Dağıtık Hizmet Dışı Bırakma Saldırılarının Tespit Edilmesi", Tübitak Bilgem, Ağustos 2017

[53] Anderson H. S., Kharkar A., Filar B., Roth P., "Evading Machine Learning Malware Detection", Black Hat USA 2017, Las Vegas, Amerika, Temmuz 2017

Kısa Link Analizi ile Bir Spam Tespit Sistemi

A Spam Detection System with Short Link Analysis

Oğuzhan ÇITLAK
Institute of Science
Gazi University
Ankara, Turkey
oguzhan.citlak@gazi.edu.tr

İbrahim Alper DOĞRU
Faculty of Technology
Gazi University
Ankara, Turkey
iadogru@gazi.edu.tr

Murat DÖRTERLER
Faculty of Technology
Gazi University
Ankara, Turkey
dorterler@gazi.edu.tr

Abstract

today, people's quality of life with the development of technology increases. Ads, information and invoce messages or random incoming an E-mail / Short Message Service (SMS) have usually a web page link in them. Short link services, goo. gl, bit. ly, and so on, are used instead of long addresses of websites in order to save the meaning of the message and the number of characters. Because of using these short link services, users can visit spam websites without any notice. A spam website can easily hide itself using short link services and unaware user can face it. Users exposed to bad software from malicious websites. Therefore, services like as Google Safe Browsing actively work around the world. That service to identify unsafe websites and notify users work around the world and keep the records of spam websites in their own databases. In work we had conducted, malicious websites, identified in the Google Safe Browsing database, could hide themselves using short link services. Malicious short links listed at first in our study. Then, we developed a software to convert short links to long web addresses. In our software, these addresses automatically checked in the Google Safe Browsing database to be spam or not. Users, received malicious short links in SMS/e-mail, have become aware of malicious spam sites and we had recommendations for users to avoid malicious webs.

Index Terms

Short Links, Spam, Malicious Web Sites, Short Link Services, Google Safe Browsing

Özet

Teknoloji, insanların yaşam kalitesini arttırtır. Reklamlar, bilgi ve fatura mesajları veya rastgele gelen bir e-posta / kısa mesaj genellikle bir web sayfası bağlantısını içeriğinde içerir. Kısa link servisleri, goo. gl, bit. ly, vb. web sitelerinin uzun adreslerinin yerine mesajın anlamını ve karakter sayısını korumak için kullanılır. Bu kısa link servisleri kullanıldığı için, kullanıcılar spam web sitelerini uyarı almaksızın ziyaret eder. Bir spam web sitesi, kısa bağlantı servislerini kullanarak kendini kolayca gizler ve habersiz kullanıcı bu site ile karşılaşır. Kullanıcılar, kötü niyetli web sitelerine ait kötü yazılımlara maruz kalırlar. Google Safe Browsing, tüm dünyada aktif olarak çalışan bir servistir. Güvensiz web sitelerini belirlemek ve kullanıcıları uyarmak için dünya genelinde çalışır ve spam web sitelerinin kayıtlarını kendi veri tabanlarında saklarlar. Yaptığımız bu çalışmada, Google Safe Browsing veri tabanında spam olarak işaretlenen web sitelerinin, kısa link servislerini kullanarak kendilerinin gizleyebildikleri gösterilmiştir. Çalışmamızda ilk önce zararlı kısa linkler listelenmiştir. Ardından, kısa link adreslerini uzun web adlarına dönüştüren bir yazılım geliştirilmiştir. Yazılımımızda, bu adresler otomatik olarak Google Safe Browsing veri setinde spam ya da spam olmadıkları kontrol edildi. İçerisinde zararlı link bulunan SMS/e-mail alan kullanıcılar zararlı spam sitelerin farkına vardılar ve kullanıcılara kötü niyetli weblerden kurtulabilmeleri için tavsiyelerde bulunulmuştur.

Anahtar Kelimeler

Kısa Linkler, Spam, Kötü Niyetli Web Siteleri, Kısa Link Hizmetleri, Google Safe Browsing

I. INTRODUCTION

Globalization and constantly developing technology are the most important features of recent years [1]. The numbers of mobile smartphones, tablets, and smart devices, namely, laptops, smart machines are constantly increasing. Nowadays, these devices easily used by the people of all ages at anytime and anywhere [2].

The number of websites has increased with spreading the internet at the same time in the whole world [3]. People can easily visit the websites and many things done online on the web.

These online transactions can be listed internet banking, e-shopping, e-mail services and e- payment services. It is obviously clear that online transactions made faster and easier through on the internet [4]. There are hundreds of millions of websites on the internet. Some of these websites created for conventional firms, some for the service of government agencies and some for personal purposes. In addition to this, hundreds of thousands of news sites, shopping sites, ads sites, and the promotions of products sites are on the internet.

Each of the websites is needed its own domain name [5]. When we enter this domain name in the web browser from

anywhere in the world, we have access to the relevant web page.

There are some short link services on the internet. Some of them can be listed goo.gl, bit.ly, bc.vc and x.co. In addition, these services shorten the uniform resource locators, URLs, of long websites with their own encryption method. People can access web sites by clicking on short links to their phones, e-mails or in short message service, SMS. [6]. Websites with malicious intentions and websites with good intentions are on the internet at the same time [7].

The domain names of malicious websites can shortened by using short link services and emailed to people's phones as SMS or to their tablet or computer [6]. Today has widely used short link services are bit.ly, goo.gl, bc.vc, tiny.cc and x.co.

Users with these short links can click on them in the messages on their devices and they can damaged from malicious websites. The infecting of a virus, the theft of account information, or the generalization of private information can occur because of clicks on such links [8].

In the second part of our work we talked about the common problems, we explained some details in the third part; we gave some information about the malicious methods and tools. We evaluated the results obtained in the last part and we give the results of our work and give information about the issues that we think be done in the future as well.

II. FREQUENTLY PROBLEMS

A hidden link [9] or fake URLs [10] to users often seen as a popular topic or news source. It can cause users to go to a site that will damage the system or unwittingly download a virus on their devices [11].

Short links within a social network such as Twitter are frequently used Despite its frequent use, the shortcomings of the short links are present and the most complained part; It is very difficult to learn how to without open a site by clicking on a link. It is highly probable that the website entered is one of an infected site or adult site [12].

Through Google Safe Browsing, millions of URLs reviewed each day to identify unsafe websites. Hundreds of unsafe sites discovered every day. Generally, malicious websites detected and warnings shown near to websites name that are detected on Google search web browsers [13]. However, in a system that detects URLs with a malicious content, a site may be flagged as malicious, but another set of data may not mark these sites as spam [14] Talosintelligence.com and Barracuda [15] are other malicious URL detection systems.

The use of different spam URL datasets will not give exact results in spam analysis on short links. A URL that is marked as spam in a data set may not mark as malicious URL in another data set.

Inappropriate content that contains violence, pornographic videos, and images that encourage substance abuse are all frequently encountered content. Sexual abuse and bullying are two different forms of unwanted content [16]. Many interesting advertisements on the Internet and innocent Internet users who provide information to these ads not known to share unsolicited messages and images on gambling sites and matchmaking sites [17].

III. OUR METHOD AND EXPERIMENTAL WORKS

We have developed a software for spam detection with short link analysis. Besides the short link in the software we have created, normal URL addresses tested for spam analysis. Our results based on the daily updated Google Safe Browsing database. A URL / short link may be spam the day we test it in the software we develop, but after that it will update itself as Google Safe Browsing Database does not have spam on it, it may change in our end. In such a case, it may be useful to use a different spam analysis data set. However, our project based only on the Google Safe Browsing data set.

We have provided nearly 100 short link addresses via social media platforms such as Twitter, Facebook, YouTube and Instagram for testing purposes. Since these short links made by hand and we aim to test the correctness of the system we have installed, we did not need a third party application to collect short links.

The working algorithm of the software we developed shown in Figure 1.

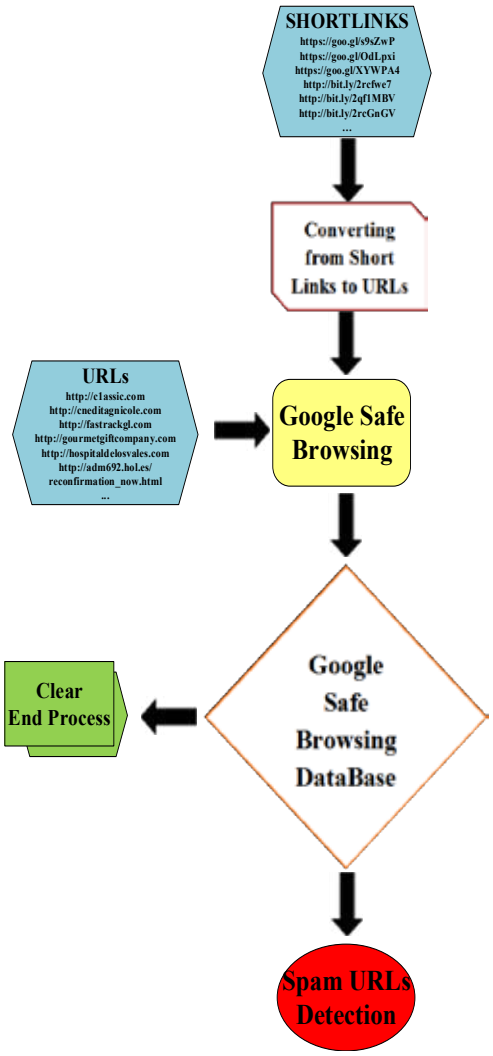


Figure 1: Software operation algorithm

The short links we have tested first converted to long URLs in our developed software. These URLs and the long URLs we suspected collected and submitted on Google Safe Browsing. Those long URLs addresses processed in Google Database, which updates itself daily, evaluated according to the result obtained. Spam URL Detection or Clear End Process shown us in results. We have analyzed the spam-detected URLs addresses through the software we have developed.

Google Safe Browsing is a large data repository that keeps spam-containing websites in their dataset and constantly updates itself [18]. A free account has created for Goo.gl and Bit.ly short link creation services. Using these accounts, I tested 20 malicious domains [19] in Table 1 and converted them to short links from long URLs

Domain Name	Goo.gl Short Link	Bit.ly Short Link
http://c1assic.com	goo.gl/s9sZwP	bit.ly/2rcESbH
http://cneditagnicole.com	goo.gl/OdLpxi	bit.ly/2qeMFYW
http://fastrackgl.com	goo.gl/XYWPA4	bit.ly/2r4FiV8
http://gourmetgiftcompany.com	goo.gl/Ab9FbQ	bit.ly/2rcfwe7
http://hospitaldelosvales.com	goo.gl/8SeNN6	bit.ly/2qf1MBV
http://adm692.hol.es/reconfirmation_now.html	goo.gl/8uFE0T	bit.ly/2rcGnGV
http://asesoresvelfit.com	goo.gl/fdcs7E	bit.ly/2qE9wyG
http://billing-customers-paypal.supportxcustomers.com	goo.gl/SCsYZa	bit.ly/2r4JO6d
http://bills-accesspp987963573-krocoko.com	goo.gl/p1Xm0d	bit.ly/2pJVqqw
http://br124.teste.website	goo.gl/0T8swy	bit.ly/2rcsOXZ
http://caixa.com.br.fgtsagendesaqueconta.com	goo.gl/50VS6g	bit.ly/2rdCKBh
http://camorg.net	goo.gl/YW1jA7	bit.ly/2qE9nv3
http://dj00.co.vu	goo.gl/MH5kmO	bit.ly/2qEeyv8
http://fb-recover-113.esy.es/	goo.gl/t3tjpl	bit.ly/2qf2gYw
http://gamesaty.ga	goo.gl/oTfOjt	bit.ly/2qeP71v
http://gfbatreilpikfdg.esy.es	goo.gl/WkVcSQ	bit.ly/2rdCMJG
http://helios3000.net	goo.gl/cnwiuP	bit.ly/2pwkaHB
http://hissoulreason.com	goo.gl/Wa3RH2	bit.ly/2pwglC1
http://httpssicredi.esy.es	goo.gl/79d0Np	bit.ly/2r4LU6f
http://kubangan-kobau88901.esy.es/	goo.gl/7pMxzx	bit.ly/2rcBv4H

Table 1: Spam domains and short link expression

The number of domains used for this malicious content increased. Our goal here is not to have many URLs, but to show that short links with malicious content detected using the Google Safe Browsing database. The short links we have obtained using Goo.gl and Bit.ly services can come out on the internet.

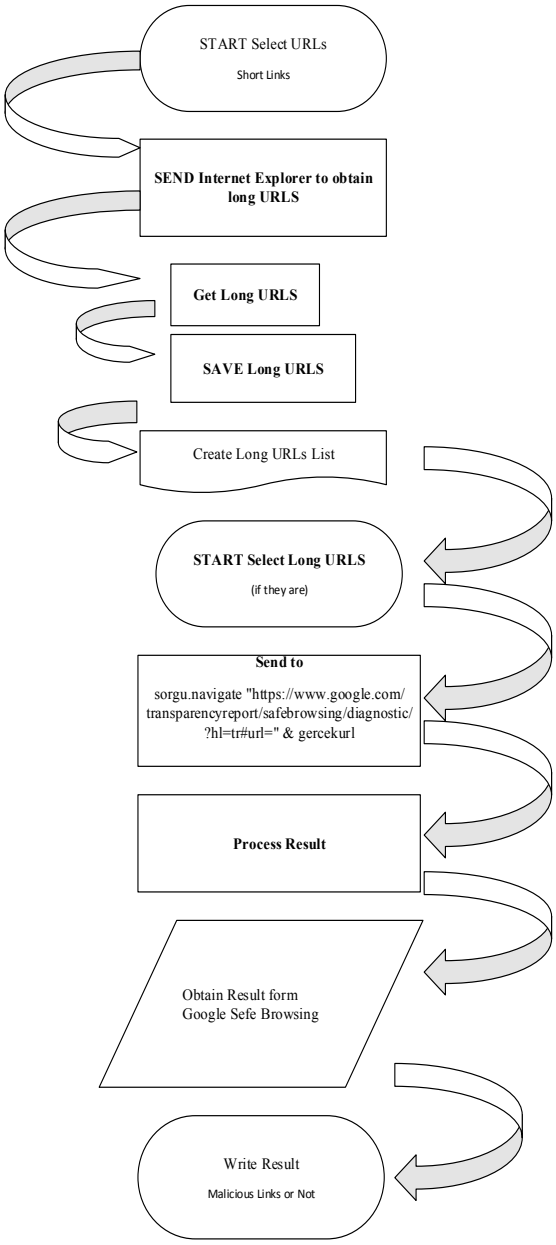


Figure 1: Software Algorithm used

Malicious content sites can hide themselves using short link services as shown in Table 1. When you are on the internet, you can see short links in short messages in the SMS, mobile phones, social accounts we have, Facebook, Instagram, Twitter, etc., in an e-mail that comes to us. It is very difficult to make a prediction about the web addresses hidden with the short link, so it is inevitable for people to click short links and go to the related website.

We will test the long web addresses of the two short links we provide in Table 2 before they are tagged as spam in Google Safe Browsing. When we do this, our software will do the operation itself and it will give us the result.

URL	Real URLs	Results	State
bit.ly/2pJBLb9	www.artemagenta.com/	Some pages on this site are not secure http://www.artemagenta.com contains malicious content, including pages with the following issues: shown same details in here	Malicious URL
bit.ly/2pKazIs	www.extrudaseal.com/	No unsafe content found	Not Malicious

Table 2: A similar picture will be generated after the execution of our code.

In Table 2, two short links are automatically analyzed and the actual URL addresses shown on the table. Actual, Google Safe Browsing has checked URL addresses and attempts to detect sites with spam content have been tried. There are no problems with nine of the twenty short link addresses analyzed according to the results in Table 2, but the remaining 11 URL addresses are marked as spam in the Google Safe Browsing database. The software algorithm we used for short link analysis is given in Figure 1.

Table 4 gives information about the link addresses and how many spams content we have analyzed. Here is an important point that should not be forgotten. The Google Safe Browsing Database is updated daily and a link with Spam may not be spam content in a subsequent update. Therefore, we did not have to compare the results we obtained with other studies. The Google Safe Browsing Database has a dynamic structure. However, Table 4 drawn up for the demonstration of our results.

Google Safe Browsing Database			
	URLs	Short Links	Total
Web Links	20	20	40
Spam	20	11	31
Not Spam	0	9	9
Total Spam Detection Range	**77.50%**		

Tablo 4: The spam numbers of the links we tested

We analyzed approximately 40 short web links. We know that they were not enough to get exact result. Nevertheless, this preliminary work gave us an idea. If we use the software tool we have developed, we can detect spam short links depending on the dynamic structure of google safe browsing.

IV. CONCLUSION

It is extremely difficult for the user to be able to understand malicious URL addresses recreated using short link services. When these short links sent to the users, they convey the malicious intentions they contain without noticing their victims. With our study, we found these spam web addresses and obtained the results.

Malicios 40 URLs addresses we manually identified in the related website [19] used for short link analysis. Sites marked as spam by Google Safe Browsing may have a long domain name as shown in Table 1. However, using the short link services, the new web site creates a link and then goes to the same web page again.

In the future, a package programming created using the coding specified in this work Short links or long URL addresses grouped together in a list to detect malicious websites in multiple databases. The Barracuda database is at least as common as Google Safe Browsing. Multiple short link analysis system that done using several similar databases will contribute to literature by detecting spam and bad malicious websites

REFERENCES

[1] Karasar, Sahin. "Eğitimde Yeni İletişim Teknolojileri-Internet Ve Sanal Yüksek Eğitim." TOJET: The Turkish Online Journal of Educational Technology 3.4 (2004).

[2] Utku, Anıl, and İbrahim Alper Doğru. "Mobil Kötücül Yazılımlar Ve Güvenlik Çözümleri Üzerine Bir İnceleme." Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji 4.2 (2016): 49-64.

[3] Bayram, Murat, and Ali Yaylı. "Otel Web Sitelerinin Içerik Analizi Yöntemiyle Değerlendirilmesi." Elektronik Sosyal Bilimler Dergisi 27.27 (2009).

[4] Chiu, Chao-Min, et al. "Determinants Of Customer Repurchase Intention In Online Shopping." Online information review 33.4 (2009): 761-784.

[5] Mockapetris, Paul, and Kevin J. Dunlap. "Development Of The Domain Name System." Vol. 18. No. 4. ACM, 1988.

[6] Klien, Florian, and Markus Strohmaier. "Short Links Under Attack: Geographical Analysis Of Spam In A URL Shortener Network." Proceedings of the 23rd ACM conference on Hypertext and social media. ACM, 2012.

[7] Zhuge, Jianwei, et al. "Studying Malicious Websites And The Underground Economy On The Chinese Web." Managing Information Risk and the Economics of Security. Springer US, 2009. 225-244.

[8] Nunez, Robert L., and Rebecca J. Hall. "Bit. Ly, Your Tinyurl Is Awe. Sm! Reinforcing Your Brand With A Custom URL Shortener." (2014).

[9] Praveenkumar, Padmapriya, et al. "Secret Link Through Simulink: A Stego On OFDM Channel." Inform. Technol. J 13 (2014): 1999-2004.

[10] Avery, John. "Uniform Resource Locator Vectors." U.S. Patent Application No. 11/733,760.

[11] Erdoğan, Görkem, and Şerif Bahtiyar. "Sosyal Ağlarda Güvenlik." Akademik Bilişim Konferansı (2014): 1-6.

[12] Boyd, Danah, Scott Golder, and Gilad Lotan. "Tweet, Tweet, Retweet: Conversational Aspects Of Retweeting On Twitter." System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.

[13] Kuo, Cynthia, et al. "Google Safe Browsing. Project At Google." Inc., June–August (2005).

[14] Keane, Justin K. "Using The Google Safe Browsing API From PHP." Mad Irish, Aug 7 (2009).

[15] Stone, Brad. "Spam Doubles, Finding New Ways To Deliver Itself." The New York Times 6 (2006): A01.

[16] Eroğlu, Yüksel, and Neşe Güler. "Koşullu Öz-Değer, Riskli Internet Davranışları Ve Siber Zorbalık/Mağduriyet Arasındaki Ilişkinin Incelenmesi." Sakarya University Journal of Education 5.3 (2015): 118-129.

[17] Altinbaşak, İpek, and Sinan Karaca. "Internet Reklamciliği Ve Internet Reklami Ölçümlenmesi Üzerine Bir Uygulama." Ege Academic Review 9.2 (2009).

[18] Bayrak, S. "Site Analiz." (2013).

[19] OpenDNS, L. L. C. "Phishtank: An Anti-Phishing Site." Online: https://www. phishtank.com (2016).

A Review on Social Bot Detection Techniques and Research Directions

Arzum Karataş
Department of Computer Engineering
Izmir Institute of Technology
Izmir, Turkey
arzumkaratas@iyte.edu.tr

Serap Şahin
Department of Computer Engineering
Izmir Institute of Technology
Izmir, Turkey
serapsahin@iyte.edu.tr

Abstract

The rise of web services and popularity of online social networks (OSN) like Facebook, Twitter, LinkedIn etc. have led to the rise of unwelcome social bots as automated social actors. Those actors can play many malicious roles including infiltrators of human conversations, scammers, impersonators, misinformation disseminators, stock market manipulators, astroturfers, and any content polluter (spammers, malware spreaders) and so on. It is undeniable that social bots have major importance on social networks. Therefore, this paper reveals the potential hazards of malicious social bots, reviews the detection techniques within a methodological categorization and proposes avenues for future research.

Index Terms

Social bots, OSN, Sybils, social bot detection.

I.INTRODUCTION

Our world has been dominated by online social networks (OSN) like Facebook, Twitter, and LinkedIn and so on. They play a pivotal role in our lives as public communication channels. They provide a platform for their users to involve, interact, and share information. Therefore, they lead a great community with the value of attracting for advertisements. Due to the popularity and rich API of OSNs, they are attractive targets for exploitations of social bots [1] as well.

A social bot is software to automate user activities. These activities can be (i) generating pseudo posts which look like human generated to interact with humans on a social network, (ii) reposting post, photographs or status of the others, and (iii) adding comments or likes to posts, (iv) building connections with other accounts. Therefore, the level of the sophistication of the bots is diverge. A social bot [2, 3] could be dummy like bots aggregating information from news, weather news, blog posts and then reposts them in the social network. On the other hand, they also can be extremely sophisticated such as infiltrating human conversations. These capabilities have pros and cons for users of OSN and they can be used for good or bad intentions.

(i). One hand, bots can be designed for good intentions. They can use to protect anonymity of members as mentioned in related work or automate and perform tasks much faster than humans, like automatically pushing news, weather updates or adding a template in Wikipedia to all pages in a specific category[4], or sending a thank-you message to your new followers out of courtesy. They can be designed to be helpful like virtual assistants for individuals such as Siri or serving a user-friendly customer service [5] for the companies and chatbots like Microsoft's Tay[6] artificial intelligence bot.

(ii). On the other hand, social bots can be designed for doing malicious activities such as spamming, malware dissemination, impersonation, Sybil attack launching and so on.

- One of the malicious functionality of social bots is the power of dissemination of misinformation. For example, Syrian Electronic Army hacks the Twitter account of Associated Press and announces the White House is under attack and Obama is injured. This fake news lead to a panic and huge loss in the stock market in 2013 [7].

- Another malicious functionality of social bots is that they are convenient way of propaganda. This malice activity is so-called astroturfing — an attempt to create a fake impression on real grassroots to support a policy, individual, product campaign [8]. Concerning this, Ratkiewicz et al.'s study [9] dissects how Twitter can be exploited by astroturfing campaigns during the 2010 U.S. midterm elections. According to Boshmaf et al.[10], as democratic communication platforms, OSN are one of the key enablers of the recent Arab Spring in the Middle East in 2011. Additionally, there is a concern whether automated propaganda sway or not 2016 elections between Trump and Clinton [11]. According to these possibilities, we can assume that social bots can be very powerful tools to fire social revolutions.

- Another obstacle is that the bots can be leveraged for getting fake rating and reviews. For example, there are influence bots that serve this purpose. Also, it is possible to find many web pages that serve fake followers and likes even for free by simply searching on any search engine. Subrahmanian et al. [3] state some politicians have been accused of buying influence on social media.

• In addition, a social bot can be malicious by impersonating actual person or an organization, i.e. identity fraud. One of the evil purpose of impersonation is to serve promoting ideologies. *Via this promotion, attackers have a power to mislead the individuals on the networks or create real-looking fake identities. Next, they are able to use them in malicious activities such as follower fraud [3, 13] or Sybil attacks consisting of large-scale bot armies(botnets) with simple OSN accounts[12].*

Hence, the main question is focused on "How we separately detect malicious activities on OSN". Many techniques are proposed to detect social bots on OSN in the literature. We review these techniques within a methodological categorization and unveil possible research avenues for each category for the social bot detection. For this purpose, Section II is reserved for the literature review on the detection techniques. Then, open problems for the social bot detection techniques are presented to envision and motivate possible researchers in Section III. Finally, the work is concluded with a small discussion on current research directions in Section IV.

II.RELATED WORK

For all reasons outlined above (malicious usages of social bots), computing community has been developing advanced techniques to detect social bots accurately. Broadly, it is possible to classify these detection techniques into three classes: (A) bot detection systems based on social network topology (i.e. structure-based) information, (B) systems based on crowdsourcing on user posts and profile analysis, and (C) systems based on feature-based machine learning methods.

A.Structure-Based (Social Network-Based) Bot Detection

Sybil accounts are the multiple accounts controlled by an adversary. The naming of "Sybil" term is coming from the subject of the book Sybil (a woman diagnosed with dissociative identity disorder [14]). Structure-based detection techniques focus on detecting Sybil accounts. These accounts are used to infiltrate OSN, steal private data, disseminate misinformation and malware. That's why, Sybil attacks are fundamental threat for social networks [15-17] . For instance, it was reported in 2015 that around 170 million fake Facebook accounts are detected as Sybil accounts, then they are deleted [18]. Whereas Sybils can be generated intentionally by users for benign purposes such as preserving anonymity; we consider solely malicious ones as Sybils from this point.

Knowing how Sybil accounts spread on the network is crucial to detect them especially for this type of detection techniques. Fundamental assumption underlying the structure-based Sybil detection is that the social networks generally shows a homophily tendency [17]. That is, two connected accounts in OSN have a tendency of having similar

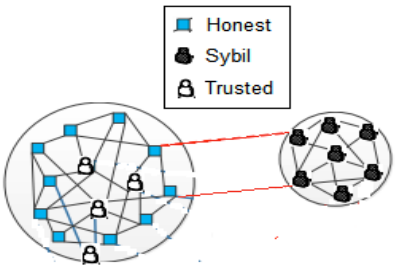


Figure 1. The social network with honest, trusted and Sybil nodes

attributes. Therefore, this assumption grounds the intuition in

Fig. 1. Here the honest and Sybil regions of graph are sparsely connected and Sybils have small number of connections to legitimate (honest) users. By large connections the Sybil communities create a fake trustworthy impression on honest members of the OSN. It may be useful to note that trusted nodes in Fig. 1 are already honest and they are specified at initialization as reference members.

There are many works to solve Sybil detection problem by using topology (structure) of the network. The analysis of network topology is a way for the detection of local communities. Let's summarize their works with respect to the methods that they employ:

- Random Walk [19]

Generally, the intuition behind leveraging random walks is that social networks are fast mixing that helps to recognize Sybils from honest accounts. Fast mixing in this context implies that short random walks starting from an honest account quickly reach other honest accounts, whereas it is hard for random walks starting from Sybils to reach the honest accounts [20]. At a high level, it can be said that the works that employ random walks label the nodes as Sybil or honest in the network from the perspective of a trusted node.

As one of the random walk-based method SybilInfer [21] , uses a combination of Bayesian inference and Monte-Carlo sampling techniques to estimate the set of honest and Sybil users. It detects a bottleneck cut between honest and Sybil regions. SybilGuard [22] adopts the assumption that malicious user can create many Sybils, but the Sybils can have few connections to honest accounts like in Fig. 1. That is, the number and sizes are bounded of the honest account. Similarly, SybilLimit [23] attempts the isolate Sybils based on random walks. It adopts the same insight with SybilGuard but offers improved and near-optimality guarantees. SybilRank [24] ranks the accounts according to their perceived likelihood (landing probability of short random walks) of being Sybil. Because, there is limited probability of escaping to Sybil region for a short random walk starting from a trusted node.

• *Markov Random Field[25] and Loopy Belief Propagation [26*] .

The assumption that social networks are fast-mixing presumes one big community or cluster to be valid. However, Mohaisen et al. [27] show that OSN are not fast-mixing generally. Similarly, Leskovec et al. [28] demonstrate that OSN have many small periphery communities that do form small communities instead of constructing one big cluster (community). Therefore, Viswanath et al. [29] state that the Sybil detection problem can be regarded as a community detection problem. Besides, Boshmaf et al. [30] point out that structure-based Sybil detection algorithms should be designed to find local community structures around known honest (non-Sybil) identities, while incrementally tracking changes in the network by adding or deleting some nodes and edges dynamically in some period for better detection performance.

Additionally, Viswanath et al. [29] discover that dependency on community detection makes more vulnerable to Sybil attacks where honest identities conform strong communities. Because Sybils can infiltrate honest communities by carefully targeting honest accounts. That is, Sybils can be hidden as just another community on OSN by setting up a small number of the targeted links. The targeted links are the links given to the community which contains the trusted node. They make an experiment by allowing Sybils to place their links closer to the trusted node instead of random nodes, where closeness is defined by ranking used by the community detection algorithm they employ. Hence, Sybil nodes are high ranked in the defence scheme. Naturally, it leads to Sybils being less likely to be detected for that attack model because Sybils are appeared as part of the local community of the trusted node.

Due to the limitations on the fast-mixing assumption, other studies are done to handle. SybilBelief [17] and SybilFrame [15] do not use random walks, instead they rely on the Markov Random Fields and Loopy Belief Propagation to estimate probabilities of users being honest. While SybilBelief can incorporate information about known honest and known Sybil nodes, SybilFrame uses a multi-stage classification mechanism using local information of users and edges with global graph structure. In this category, SybilFrame shows the best social bot detection rate with maximum 68.2% [15].

Additionally, some structure-based Sybil detection systems like SybilRank also employ "innocent by association" paradigm [31]: if an identity has an interaction with an innocent identity, then itself is innocent as well. This is a vulnerable approach for a smart attacker mimics the structure of legitimate community. The effectiveness of this paradigm is limited by the refusal of innocent users to interact with unknown identities as in the case of LinkedIn. Nevertheless, some real-world social networks like Twitter and Renren (largest OSN in China) do not represent strong trust network. Therefore, the detection schemes employed the paradigm produce high false-negative rate.

B.CrowdSourcing-Based Bot Detection

The success of structure-based Sybil detection schemes has decreased over time whereas Sybils exploit the vulnerability by which Viswanath et al. reveal (dependency on community detection vulnerability), which is stated above. For example, Jiang et al. [32] show that Sybils occasionally connect to other Sybils. Instead, they target to infiltrate communities of trusted users [33].

Wang et al. [34] proposed a new approach of applying human effort (crowdsourcing) like Amazon's Mechanical Turk [35] to label accounts. Their insight is that careful users can detect even slight inconsistencies in account profiles and posts. They propose a two-layered system containing filtering and crowdsourcing layer. They offer to use prior automation techniques such as community detection and network-based feature selection, and user reports in filtering layer to obtain suspicious profiles. Then, they apply crowdsourcing for final decision on classifying accounts either legitimate or Sybil. According to the authors, their strategy exhibits false positive and negative rates both below %1 for their simulated system that contains 2000 profiles combination of 1000 legitimate and 1000 Sybil profiles.

There are three fundamental issues related to leverage of this strategy. First, privacy of the users should be considered and personal information of the OSN users should be hidden before sharing the information with the crowd. Second, large OSN companies need to hire expert analysts additionally and small companies cannot afford it. Third, the strategy is not easy to implement for large OSN because of the existence of huge number of members. Crowd may need too much time during decision process when labelling the accounts either bot or human.

C.Machine Learning-Based Bot Detection

The more social bots are sophisticated with the rise of Artificial Intelligence (AI), the more they pose risk to even political issues. That's why, detecting the bots on OSN become a challenge. For this reason, DARPA organized a competition and social structure-based detection techniques are found useful by none of the contestants [3]. The rise of AI leads to transcendent machine learning methods as social bot detection techniques as well. The main idea behind them is to find out key characteristics of social bots to draw the border between a human actor and a machine actor. The summary of some selected works can be found below.

Chu et al. [2] make a study on profiling human, bot, and cyborgs . They observe the difference among them in terms of tweet content, tweeting behaviour, and account properties like external URL ratio. Lee et al. [36] present a study for social honeypots for profiling and filtering of content polluters in social media by using their profile features. Yang et al. [33] collect Sybil accounts from Renren as ground-truth data set. Then, they analyse it by using network-based and structured-based features such as network clustering coefficient, incoming and outgoing request rate.

SentiBot [37] is a framework for addressing the classification of human versus social bots. It relies on tweet syntax like average number of hashtags, semantics like average topic sentiment, user behaviour like tweet spread, and network-centric user features like in-degree. The authors of it regard the number of sentiment related features as key to the identification of the bots. Therefore, they also employ sophisticated sentiment analysis techniques.

"Bot or Not?" [38] is the first social bot detection framework publicly available for Twitter. Its first release is published in 2014 which is similar to other feature based detection systems. However, it analyses more than 1000 features and grouped them into 6 classes: network, user, friends, temporal, content, and sentiment. The authors of the work implement a detection algorithm heavily depends on these core features. They state that the overall all accuracy of "Bot or Not?" is 86% for simple and sophisticated social bots in 2017 [39].

It is useful to note that machine learning and the structure information of OSN together give this detection result. The best detection rate is achieved by "Bot or Not" with 86% success rate for this category.

III.OPEN PROBLEMS

Detection of the bots on OSN are challenging issue. That's why, there are some research avenues for peculiar to each category mentioned in related work.

Social networks contain big data within itself and they dynamically grow in their nature. Structure-based detection schemes usually have high running time cost even within a static (i.e., non-real time) environment. The known best computational cost for leveraging random-walk is . That's why, developing a computationally more efficient real-time graph algorithm for big data processing can be a good research avenue. Other issue is that the schemes give high false positive rates with relatively low accuracy, yet. For example, SybilFrame gives 4.2% false positives (FP), with a classification accuracy of 95.4%, and the social bot detection rate is maximum 68.2% as mentioned just above section. False positives are detrimental to user experience because real users can respond very negatively. That's why, a new learning approach can be employed algorithms to decrease FP and false negatives (FN) rates on the graph topology. As for community based-schemes, new approaches for determining trusted nodes on-the fly is another open area for the researchers. Since, structure of the network and trusted nodes are in the heart of the success of structure-based approaches.

Crowdsourcing-based detection schemes leverage human intelligence against sophisticated social bots equipped with AI power. Protecting user privacy is a challenge for crowdsourced detection techniques. That's why, a work can be done for increasing ethical awareness of the crowd. In addition, privacy preserving data mining techniques can be employed for user privacy. However, the schemes are neither effective nor applicable in terms of both time and money costs for the crowd when we regard that OSN are dynamic environments and that they contain big data.

Bots are continuously evolving by gaining new human-like behaviours with the rise of AI. As for feature-based machine learning schemes, some additional features can be explored employing the-state-of-art machine learning techniques like deep learning to distinguish a human from a bot. Another issue is if the Sybils are just controlled bots by an adversary, who the master is. That' is the big question: what is the source of these Sybils? That is, source detection of the Sybils is one of the big deals.

IV.CONCLUDING DISCUSSION

Social networks are powerful tools that connect the millions of people over the world. Therefore, they are attractive for social bots as well. Since the possible harm of social bots such as identity theft, astroturfing, content polluter, follower fraud, misinformation dissemination etc., there is a need of recognition of bots and humans each other to avoid undesirable situations based on false assumptions.

In Table 1, the detection techniques, related works, limitations for each techniques and contingent research areas are summarized. Since OSN are dynamic environment and contains big data itself, possible future solutions need to handle efficiently both big data processing and dynamic detection. Besides, the solutions should decrease FN and FP of the existing solutions while increasing accuracy as much as possible. Since structure-based techniques needs at least one trusted node, determining the trusted nodes on-the-fly can be a possible research direction. The best success rate for these techniques is maximum 68.2 %, which is achieved by SybilFrame.

As it is seen from the table, no research avenue is proposed since crowdsourcing-based techniques are expensive in both time and cost of the crowd workforce. As for machine learning-based techniques, the limitations of them are AI-boosted bots. However, the remedy of those limitations is advanced AI techniques like deep learning to determine the features to draw a line between innocent accounts and Sybils as well. Also, these techniques can be used to source detection of Sybils as a research direction. The best success rate for these techniques on the overall 86%, which is succeeded by "Bot or Not?".

With the progress of the social bot detection techniques, it is seen that the higher social bot detection rates (over 80%) are obtained with the combination of the structure-based properties of OSN and unsupervised machine learning methods. It is useful to conduct research on some possible approaches to increase the detection rate. The approaches may be (i) use of autonomous-intelligent agent based and (ii) identification-based approaches as the future directions of researches.

i.Use of autonomous - intelligent agent based approaches: For example, detection and identification of community

Table 1. Summary of detection techniques and research directions

Table 1. Summary of detection techniques and research directions

Detection Approaches	Related Work	Accuracy	Limitations	Open Research Areas
Structure-Based	• SybilInfer • SybilGuard • SybilLimit • SybilRank • SybilBelief • SybilFrame	• 68.2 %	• OSN contains big data inside. • OSN are a dynamic environment • Need of decreasing FN, FP rates • High running time cost • Need of at least one trusted node	• Developing more efficient big data processing algorithms • Dynamic or real-time detection methods • Considering new methods to decrease FN and FP rates • Determining trusted nodes on-the fly
Crowdsourcing-Based	• Wang et al.'s work [34]		• Limited size analysis possibility with sampling method • Privacy issues • High running time cost of the crowd • Cost of crowd workforce	• Privacy can be preserved via privacy preserving data mining algorithms.
Machine Learning-Based	• Chu et al. 's work[2] • Lee et al. 's work [36] • Yang et al. 's work [33] • Bor or Not? • SentiBot	• 86 %	• OSN contains big data inside. • OSN are a dynamic environment • AI-powered bots • Need of decreasing FN, FP rates • Unknown source of Sybils	• Dynamic or real-time detection methods • Employing popular AI techniques (like deep learning) to detect features to distinguish a bot from an innocent account holder and handle big data. • Considering new methods to decrease FN and FP rates • Source detection of Sybils

members wit hin the community should be performed in a decentralized environment. That is, the detection and analysis tasks are distributed to the community according to the topology of OSN. In the environment, intelligent agents aware of their community boundaries and members should be present to monitor community activities based on identified characteristics.

ii.Identification-based approaches: If identification component of any type of entity is not present; any technologically and methodologically developed

method to solve this problem can be exploited by attackers. For example, intelligent agents developed

for automatic and dynamic detection of Sybils should be supported by trusted identification mechanisms. If this does not happen, intelligent agents will be targeted and the attacker will not be detected, and innocent accounts might be declared as Sybil. This possibly result in another attack problem.

In this paper, three classes of social bot detection techniques (i.e., structure-based, crowdsourcing-based and feature-based machine learning detection techniques) on OSN, their limitations and detection rates are reviewed. After examination, it is seen that the most effective and popular one is feature-based machine learning techniques among them. However, the rise of AI for development of sophisticated bot creations, the bottlenecks of real-time big data processing and the need of source detection for a global identification system lead us to find out a novel solution. Therefore, research avenues on social bot detection techniques are reviewed, and prospective methods to be able to increase the social bot detection rates are proposed with the intention of opening the doors for researchers to exploit.

REFERENCES

[1]S. K. Dehade and A. M. Bagade, "A review on detecting automation on Twitter accounts," Eur. J. Adv. Eng. Technol, vol. 2, pp. 69-72, 2015.

[2]Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?," IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 811-824, 2012.

[3]V. Subrahmanian, A. Azaria, S. Durst, V. Kagan, A. Galstyan, K. Lerman, et al., "The darpa twitter bot challenge," arXiv preprint arXiv:1601.05140, 2016.

[4](2016, September 12). Wikipedia:Creating a bot. Available: https://en.wikipedia.org/wiki/Wikipedia:Creating_a_bot

[5]C. Freitas, F. Benevenuto, S. Ghosh, and A. Veloso, "Reverse engineering socialbot infiltration strategies in twitter," in Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, 2015, pp. 25-32.

[6]E. Ferrera, "The Rise of Social Bots," ed, 2016.

[7]D. Mail, "Syrian Electronic Army linked to hack attack on AP Twitter feed that 'broke news' Obama had been injured in White House blast and sent Dow Jones plunging," ed, 2013.

[8]A. Bienkov, "Astroturfing: what is it and why does it matter?," in The Guardian, ed, 2012.

[9]J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer, "Detecting and Tracking Political Abuse in Social Media," ICWSM, vol. 11, pp. 297-304, 2011.

[10]Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 93-102.

[11]B. Schreckinger. (2016, September 30,2016) Inside Trump's 'cyborg' Twitter army. Available: http://www.politico.com/story/2016/09/donald-trump-twitter-army-228923

[12]Abokhodair, N., Yoo, D., & McDonald, D. W. (2015, February). Dissecting a social botnet: Growth, content and influence in Twitter. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (pp. 839-851). ACM.

[13]O. Goga, G. Venkatadri, and K. P. Gummadi, "The doppelgänger bot attack: Exploring identity impersonation in online social networks," in Proceedings of the 2015 ACM Conference on Internet Measurement Conference, 2015, pp. 141-153.

[14]Sybil attack. Available: https://en.wikipedia.org/wiki/Sybil_attack

[15]P. Gao, N. Z. Gong, S. Kulkarni, K. Thomas, and P. Mittal, "Sybilframe: A defense-in-depth framework for structure-based sybil detection," arXiv preprint arXiv:1503.02985, 2015.

[16]D. Mulamba, I. Ray, and I. Ray, "SybilRadar: A Graph-Structure Based Framework for Sybil Detection in On-line Social Networks," in IFIP International Information Security and Privacy Conference, 2016, pp. 179-193.

[17]N. Z. Gong, M. Frank, and P. Mittal, "Sybilbelief: A semi-supervised learning approach for structure-based sybil detection," IEEE Transactions on Information Forensics and Security, vol. 9, pp. 976-987, 2014.

[18]J. Parsons. (2015, September 12). Facebook's War Continues Against Fake Profiles and Bots. Available: http://www.huffingtonpost.com/james-parsons/facebooks-war-continues-against-fake-profiles-and-bots_b_6914282.html

[19]K. Pearson, "The problem of the random walk," Nature, vol. 72, p. 294, 1905.

[20]B. Carminati, E. Ferrari, and M. Viviani, "Security and trust in online social networks," Synthesis Lectures on Information Security, Privacy, & Trust, vol. 4, pp. 1-120, 2013.

[21]G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Nodes using Social Networks," in NDSS, 2009.

[22]H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in ACM SIGCOMM Computer Communication Review, 2006, pp. 267-278.

[23]H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008, pp. 3-17.

[24]Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro. (2016). SybilRank. Available: http://www.tid.es/research/areas/sybil-rank

[25]G. R. Cross and A. K. Jain, "Markov random field texture models," IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 25-39, 1983.

[26]K. P. Murphy, Y. Weiss, and M. I. Jordan, "Loopy belief propagation for approximate inference: An empirical study," in Proceedings of the Fifteenth conference on Uncertainty in artificial intelligence, 1999, pp. 467-475.

[27]A. Mohaisen, A. Yun, and Y. Kim, "Measuring the mixing time of social graphs," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, 2010, pp. 383-389.

[28]J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney, "Community structure in large networks: Natural cluster sizes and the absence of large well-defined clusters," Internet Mathematics, vol. 6, pp. 29-123, 2009.

[29] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," ACM SIGCOMM Computer Communication Review, vol. 40, pp. 363-374, 2010.

[30]Y. Boshmaf, K. Beznosov, and M. Ripeanu, "Graph-based sybil detection in social and information systems," in Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on, 2013, pp. 466-473.

[31]Y. Xie, F. Yu, Q. Ke, M. Abadi, E. Gillum, K. Vitaldevaria, et al., "Innocent by association: early recognition of legitimate users," in Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 353-364.

[32]J. Jiang, C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai, et al., "Understanding latent interactions in online social networks," ACM Transactions on the Web (TWEB), vol. 7, p. 18, 2013.

[33]Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering social network sybils in the wild," ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 8, p. 2, 2014.

[34]G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, et al., "Social turing tests: Crowdsourcing sybil detection," arXiv preprint arXiv:1205.3856, 2012.

[35](2016). Overview of Mechanical Turk. Available: http://docs.aws.amazon.com/AWSMechTurk/latest/RequesterUI/OverviewofMturk.html

[36]K. Lee, B. D. Eoff, and J. Caverlee, "Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter," in ICWSM, 2011.

[37]J. P. Dickerson, V. Kagan, and V. Subrahmanian, "Using sentiment to detect bots on Twitter: Are humans more opinionated than bots?," in Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on, 2014, pp. 620-627.

[38]C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, "Botornot: A system to evaluate social bots," in Proceedings of the 25th International Conference Companion on World Wide Web, 2016, pp. 273-274.

[39]O. Varol, E. Ferrara, C. A. Davis, F. Menczer, and A. Flammini, "Online human-bot interactions: Detection, estimation, and characterization," arXiv preprint arXiv:1703.03107, 2017.

Türkçe SMS Mesajları Üzerinde Naïve Bayes Sınıflayıcı Tabanlı Spam Tespiti

Naïve Bayes Classifier Based Spam Detection on Turkish SMS Messages

Hamdullah KARAMOLLAOĞLU
Bilgi İşlem Daire Başkanlığı
Elektrik Üretim A.Ş.
Ankara, Türkiye
h.karamollaoglu@euas.gov.tr

İbrahim Alper DOĞRU
Teknoloji Fakültesi
Gazi Üniversitesi
Ankara, Türkiye
iadogru@gazi.edu.tr

Murat DÖRTERLER
Teknoloji Fakültesi
Gazi Üniversitesi
Ankara, Türkiye
dorterler@gazi.edu.tr

Mustafa ALKAN
Teknoloji Fakültesi
Gazi Üniversitesi
Ankara, Türkiye
alkan@gazi.edu.tr

***Özet*—SMS kullanımının yaygınlaşması ile birlikte ortaya çıkan en önemli problemlerin başında spam SMS mesajları gelmektedir. Bu çalışmada, Makine Öğrenmesi yöntemlerinden Multinominal Naïve Bayes (MNB) Sınıflayıcı yardımıyla spam içeren SMS mesajlarının tespit edilmesi amaçlanmaktadır. Çalışmada, MNB Sınıflayıcı Metodunun eğitim aşamasında kullanılmak üzere 420 spam ve 430 spam olmayan olmak üzere toplam 850 adet Türkçe yazılmış SMS mesajından oluşan TurkishSMS isimli veri seti kullanılmıştır. Çalışmanın başarım oranının tespiti için ise 200 spam ve 200 spam olmayan olmak üzere toplam 400 adet SMS mesajı niteliğindeki ifadeden oluşan sorgu veri seti çeşitli internet sitelerinden derlenerek oluşturulmuştur. Yapılan çalışma neticesinde %97.5'lik doğruluk oranı ile spam SMS mesajlarının tespiti ve sınıflandırılması gerçekleştirilmiştir.**

***Anahtar Kelimeler*—SMS spam tespiti, SMS spam filtreleme, Naïve Bayes Metodu, Naïve Bayes Sınıflayıcı**

***Abstract*—Spam SMS messages are one of the most important problems that arise with the widespread use of SMS. This study aims to identify SMS messages containing spam with the help of Multinomial Naïve Bayes (MNB) Classifier from Machine Learning methods. In the study, a dataset named TurkishSMS consisting of 850 Turkish messages, which include 420 spam and 430 non-spam, is used for the MNB Classifier training phase. A query dataset consisting of 400 SMS message-like expressions, which include 200 spam and 200 non-spam, is collected from various internet sites to determine the performance ration of the study. As a result of the study, detection and classification of spam SMS messages is performed with an accuracy rate of 97.5%.**

***Index Terms*—SMS spam detection, spam SMS filtering, Naïve Bayes Method, Naïve Bayes Classifier**

I. GİRİŞ

Kısa Mesaj Servisi (SMS) mobil haberleşmede kullanılan en yaygın iletişim teknolojilerden birisidir. Mobil telefon kullanımının yaygınlaşması ile birlikte SMS mesajı trafiği de her geçen gün artmaktadır. 2016 yılı sonu itibariyle Türkiye'de toplam 75.061.699 mobil abone bulunmaktadır. Türkiye'de 2016 yılı dördüncü üç aylık dönemde gönderilen/alınan SMS mesajı sayısı ise yaklaşık 23.617 milyon civarındadır [1]. SMS kullanımının bu denli yaygınlaşması bir takım problemleri de beraberinde getirmiştir. Bu problemlerin başında istenmeyen (spam) SMS'ler gelmektedir.

Spam SMS'ler genellikle firmalardan gelen reklam amaçlı mesajlar, bahis veya pornografik içerikli yasadışı internet sayfalarına yönlendirme yapan mesajlar ile propaganda amaçlı gönderilmiş mesaj içeriklerinden oluşmaktadır. Bu tür istem dışı gönderilmiş spam SMS'ler mobil telefon kullanıcılarını boş yere meşgul ederek rahatsızlık vermekte, mobil telefonların mesaj kutularını gereksiz işgal etmektedir.

Spam SMS gönderen işletmelerin önüne geçebilmek için Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 12 Nisan 2016 tarihinde yapılan düzenleme ile BTK aracılığı ile işletmelere tahsis edilen dört haneli Numara Taşınabilirliği Yönlendirme Kodunun, işletmeciler tarafından mobil telefon kullanıcılarına gönderilmek istenen SMS mesajlarının sonuna eklenmesi zorunlu kılınmıştır. Bu kod sayesinde spam SMS'in hangi işletmeci tarafından gönderildiği bilgisine ulaşılabilmektedir [2].

Çalışmada Türkçe içerikli SMS mesajları içerisinde spam olanların tespit edilerek sınıflandırılması için makine öğrenmesi yöntemlerinden MNB Sınıflayıcı kullanılmıştır.

Makalenin ikinci bölümünde spam SMS tespiti hakkındaki mevcut çalışmalar ele alınmış, üçüncü bölümde çalışmada kullanılan yöntemler üzerinde durulmuştur. Dördüncü bölümde deneysel sonuçlar verilmiş, son bölümde ise sonuçlar hakkında değerlendirmelerde bulunulmuştur.

II. MEVCUT ÇALIŞMALAR

Sethi ve Bhootna tarafından yapılan çalışmada, spam SMS tespiti için Bayes Sınıflandırıcı yönteminden yararlanılmıştır. 100 adet SMS mesajı eğitim amaçlı, 100'den fazla SMS mesajı ise sınıflandırma ve test işlemleri için kullanılarak %97,4'lik bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [3]. Ezpeleta vd. tarafından yapılan spam SMS tespiti çalışmasında, sözlük tabanlı duygu analizi ve

TextBlob Sınıflandırıcıdan yararlanılmıştır. Veri seti olarak 492 pozitif ve 394 negatif veri içeren 'SemEval-2013' ile 747 spam ve 4827 normal mesaj içeren 'SMS Spam Collection' veri seti kullanılmıştır. Sonuçta %98.76'lık bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [4]. Yang vd. tarafından Bayes Sınıflandırıcı kullanılarak yapılan çalışmada eğitim ve test işlemleri için 2000 spam ve 2000 spam olmayan mesaj kullanılmıştır. Sonuçta %97.90'lık bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [5]. Bozan vd. tarafından yapılan çalışmada 'SMS Spam Collection' veri seti kullanılarak Naïve Bayes Sınıflandırıcı, Karar Destek Makinesi (SVM) ve K-En Yakın Komşu (k-NN) metotları yardımıyla spam SMS tespiti amaçlanmıştır. Sonuçta Naïve Bayes Sınıflandırıcı kullanılarak %97.55, SVM kullanılarak %98.61 ve k-NN kullanılarak %93.35'lik bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [6]. Akbari ve Sajedi tarafından 747 adet spam ve 4825 adet spam olmayan SMS mesajı içeren veri seti kullanılarak GentleBoost metodu yardımıyla yapılan spam SMS tespiti çalışmasında %98.30'luk bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [7]. Li ve Zeng tarafından 12000 spam ve 8000 spam olmayan SMS içeren veri seti kullanılarak Vektör Uzay Modeli yardımıyla yapılan çalışmada yaklaşık %89'luk bir başarı oranı ile spam SMS tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir [8].

Literatürdeki spam SMS tespitine ilişkin çalışmalar incelendiğinde çeşitli dillerde yazılmış SMS mesajlarından oluşan veri setleri kullanıldığı ve ilgili problemin çözümünde genellikle makine öğrenmesi yöntemleri ile sözlük tabanlı yöntemlerin tercih edildiği görülmektedir. SMS mesajlarında kullanılan dilin yapısal ve kökensel özellikleri, eğitim ve sorgu aşamasında kullanılan veri setlerinin boyutu ve çalışmada kullanılan yöntemlere göre çalışmaların başarım oranlarının değiştiği görülmektedir.

III. YÖNTEM

Çalışmada spam SMS'lerin tespiti için makine öğrenmesi yöntemlerinden MNB Sınıflayıcı metodu kullanılmıştır. MNB sınıflayıcının, kategorik verilerin sınıflandırılmasında kullanılan basit ve hızlı bir teknik olmasının yanı sıra sınıflandırılacak belgelere ilişkin terim frekansı vb. değerlerinin metoda ilişkin hesaplamalarda kullanılıyor olması doğru sınıflandırma başarımını artırdığı için çalışmada kullanılması tercih edilmiştir.

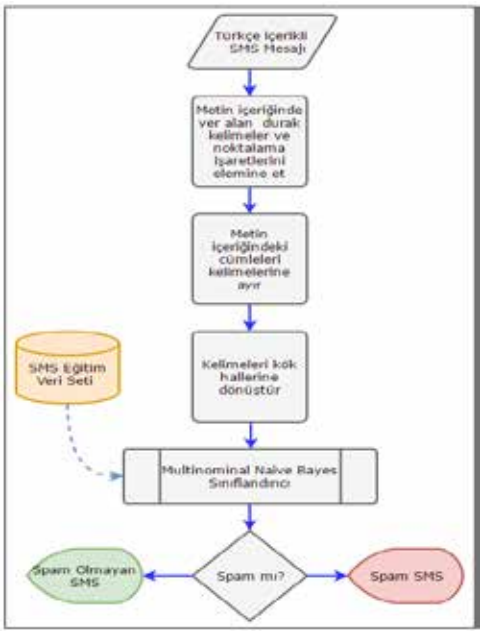
MNB Sınıflayıcı metodunda eğitim amacıyla yararlanılmak üzere, spam ve spam olmayan olarak sınıflandırılmış Türkçe içerikli SMS mesajlarından oluşan TurkishSMS [9] isimli eğitim veri seti kullanılmıştır. Çalışmanın başarısının test edilmesi için ise çeşitli internet sitelerinden elde edilmiş, SMS gönderimine uygun 200 adet reklam içerikli spam mesaj ile 200 adet normal içerikli mesaj içeren TurkishSpamSMS[1] isimli sorgu veri seti oluşturulmuştur. Tablo 1'de spam ve spam olmayan SMS mesajı örnekleri görülmektedir.

[1] mobseclab.gazi.edu.tr/datasets/TurkishSpamSMS

TABLO I. SPAM VE SPAM OLMAYAN SMS MESAJI ÖRNEKLERİ

Spam SMS Mesajı	Spam Olmayan SMS Mesajı
Herkes bedava içerik elde etmeyi sever. Biz de bedava içerik dağıtmayı seviyoruz. O zaman tam birbirimize göreyiz! Sana özel dağıtılan hediye içerikleri için tıkla: https://...	Merhaba, ben spor salonuna yeni yazılacağım. Hoca bana beslenme ve antrenmanın öneminden bahsetti. Kilolu olduğun için yağ yakman lazım dedi. Acaba bana bu konu hakkında teorik olmayan kitap tavsiye eder misiniz?

Bu çalışmada önerilen yönteme ait işlem adımlarını gösteren akış diyagramı Şekil 1'de görülmektedir.



Şekil 1. Çalışmaya ait işlem adımlarını gösteren akış diyagramı

Önerilen yöntemde sınıflandırma öncesi veri setindeki mesajlar bir ön işlem aşamasına tabi tutulmaktadır. Bu aşamada, eğitim veri setinin içeriğinde yer alan SMS mesajlarındaki bütün harfler küçük harfe dönüştürülmekte ve bu mesajlarda geçen gereksiz noktalama işaretleri ile durak kelimeler elemine edilmektedir. Daha sonra ilgili mesajlardaki ifadeler Zemberek API kullanılarak kelimelerine ayrıştırılmaktadır. Bu kelimeler yine Zemberek API yardımıyla köklerine indirgenmektedir. Zemberek, Türk dilleri için geliştirilmiş açık kaynak kodlu bir Doğal Dil İşleme (DDİ) kütüphanesidir [10].

Tablo 1'de yer alan örnekteki SMS mesajlarının ön işlem aşamasından sonraki normalize edilmiş hali Tablo 2'de görülmektedir.

TABLO II. ÖN İŞLEM AŞAMASINDAN GEÇİRİLMİŞ SMS MESAJLARI

Ön İşlem Aşamasından Geçirilmiş Spam SMS Mesajı	Ön İşlem Aşamasından Geçirilmiş Spam Olmayan SMS Mesajı
herkes bedava içerik elde et sev biz bedava içerik dağıt sev o zaman tam birbiri sen özel dağıt hediye içerik tık	merhaba ben spor salon yeni yaz hoca ben besle antrenman önem bahset kilo ol yağ yak lazım de acaba ben konu teorik ol kitap tavsiye et

Tablo 2'de görüldüğü gibi ön işlem aşamasında normalize edilerek standart bir yapı haline getirilen Türkçe içerikli SMS mesajları spam tespiti yapılmak üzere, eğitim veri seti yardımıyla eğitilmiş MNB Sınıflayıcı ile test edilmektedir. Test aşamasından çıkan sonuca göre ilgili SMS mesajlarının spam olup olmadığı belirlenmektedir.

A. Naïve Bayes Sınıflayıcı

Naïve Bayes (NB) Sınıflayıcı, Bayes Kuralını temel alan bir sınıflandırma metodudur. NB sınıflandırıcı bir olayı meydana getiren her bir etkenin, ilgili olaya olan etki olasılığının hesaplanması ve olayın meydana gelmesinde belirleyiciliği fazla olan etkenin tespit edilmesinde kullanılır [11].

Bayes Kuralı, *A* ve *B* rastgele iki olay olmak üzere bu olaylara ilişkin koşullu olasılıklar (sonsal) ile marjinal (önsel) olasılıklar arasındaki ilişkiyi ifade etmektedir. Eşitlik 1'de Bayes Kuralı görülmektedir.

$$P(A \mid B) = P(B \mid A) \times P(A)/P(B) \quad (1)$$

$P(A)$ *A* olayının önsel olasılığını, $P(B)$ *B* olayının önsel olasılığını temsil etmektedir. Önsel olasılık, bir olay hakkında veriler toplanmadan önce ilgili olaya ilişkin başlangıç olasılığını ifade etmektedir. $P(A|B)$ *B* olayının gerçekleşmesi durumunda *A* olayının ortaya çıkma olasılığını, $P(B|A)$ *A* olayının gerçekleşmesi durumunda *B* olayının ortaya çıkma olasılığını ifade etmektedir. $P(B|A)$ olaylara ilişkin veriler toplandıktan sonra *B* olayına ilişkin olasılığı ifade ettiği için sonsal olasılık olarak adlandırılmaktadır [12].

B. Naïve Bayes Sınıflayıcı Modelleri

Sınıflandırma işlemlerinde NB Sınıflayıcı Modelleri, çok terimli model olarak adlandırılan Bernoulli Naïve Bayes (BNB) Sınıflayıcı Modeli ile belgelerdeki terim frekansı değerlerini kullanarak hesaplamalar yapılan Multinominal Naïve Bayes (MNB) Sınıflayıcı Modeli'dir.

1) Bernoulli Naive Bayes (BNB) Sınıflayıcı Modeli

BNB Sınıflayıcı modelinde belgeler ikili (binary) şekilde ve özellik vektörü formatında ifadelendirilir. Eğer bir terim bir belgede yer alıyorsa 1, yer almıyorsa 0 ile temsil edilir [13]. Tablo 3'te bir belge örneğine ait içerik bilgileri ile BNB Sınıflayıcı için kullanılmak üzere belirlenen sözcük kümesi (*S*) ve ilgili belge içeriğine ait özellik vektörü (d^B) görülmektedir.

TABLO III. BNB İÇİN ÖZELLİK VEKTÖRÜNÜN OLUŞTURULMASI ÖRNEĞİ

Belge İçeriği (*B*)	**Sözcük Kümesi (*S*)**	**BNB Özellik Vektörü (d^B)**
Bedava oyun, bedava mobil uygulamalar ile sürpriz kampanya, hediye çekilişleri ve hediye kuponlar için sayfamızı ziyaret ediniz.	bedava	1
	kampanya	1
	fırsat	0
	hediye	1
	sürpriz	1
	indirim	0

Tablo 3'te görüldüğü gibi, sözcük kümesi *S*={bedava, kampanya, sürpriz, hediye} ve belge içeriği *B*="Bedava oyun, bedava mobil uygulamalar ile sürpriz kampanya, hediye çekilişleri ve hediye kuponlar için sayfamızı ziyaret ediniz." olan bir yapı, BNB Sınıflayıcı modelinde d^B=(1,1,0,1,1,0) şeklinde ifade edilmektedir.

BNB Sınıflayıcı kullanılarak belge sınıflandırma olasılık değeri Eşitlik 2'deki gibi hesaplanmaktadır.

$$P(D_i|C) \sim P(b_i|C) = \prod_{t=1}^{|V|} \left[b_{it} P(w_t|C) + (1 - b_{it}) \left(1 - P(w_t|C)\right) \right] \quad (2)$$

Eşitlik 2'de, C sınıflandırılacak belgenin ait olabileceği sınıfı (SMS spam tespiti için, spam ve spam olmayan olmak üzere iki sınıf belirlenmektedir.), D_i sınıflandırılması yapılmak istenilen i. belgeyi temsil etmektedir. $|V|$ bir sınıfa ait olan belgelerde yer alan toplam kelime sayısını, b_i i.belgeye (D_i) ait özellik vektörünü, w_t ise D_i belgesi içerisindeki *t.* terimi ifade etmektedir. b_{it} b_i özellik vektöründeki *t.* terimi ifade etmektedir. b_{it} eğer w_t terimi D_i belgesinde mevcutsa *1*, mevcut değilse *0* değerini almaktadır. $P(w_t|C)$ w_t teriminin *C* sınıfındaki ağırlık değerini ifade etmektedir. $P(w_t|C)$ değeri Eşitlik 3'teki gibi hesaplanmaktadır.

$$P(w_t \mid C = k) = (n_k(w_t))/N_k \quad (3)$$

Eşitlik 3'te, $n_k(w_t)$ w_t teriminin geçtiği belge sayısını, N_k ise ilgili sınıfa (C) ait toplam belge sayısını ifade etmektedir.

2) Multinominal Naïve Bayes (MNB) Sınıflayıcı Modeli

MNB Sınıflayıcı modeline göre belgeler, sözcük kümesinde yer alan terimlerin ilgili belgelerde geçme sıkılıkları (kelime frekansı) dikkate alınarak oluşturulan özellik vektörü ile ifadelendirilir [14].

Tablo 4'te bir belge örneğine ait içerik bilgileri, MNB Sınıflayıcı için kullanılan sözcük kümesi (*S*) ve ilgili belge içeriğine ait özellik vektörü (d^B) görülmektedir.

TABLO IV. MNB İÇİN ÖZELLİK VEKTÖRÜNÜN OLUŞTURULMASI ÖRNEĞİ

Belge İçeriği (*B*)	**Sözcük Kümesi (*S*)**	**MNB Özellik Vektörü (d^B)**
Bedava oyun, bedava mobil uygulamalar ile sürpriz kampanya, hediye çekilişleri ve hediye kuponlar için sayfamızı ziyaret ediniz.	bedava	2
	kampanya	1
	fırsat	0
	hediye	2
	sürpriz	1
	indirim	0

Tablo 4'te görüldüğü gibi MNB Sınıflayıcı için belirlenen sözcük kümesindeki kelimelerin ilgili belge içeriğinde yer alma sıklıkları (kelime frekansı) dikkate alınarak oluşturulan özellik vektörü (d^B)=(2,1,0,2,1) şeklinde ifade edilmektedir.

MNB Sınıflayıcı'ya göre belge sınıflandırma olasılık değeri Eşitlik 4'deki gibi hesaplanmaktadır.

$$P(D_i|C) \sim P(x_i|C) = \frac{n_i!}{\prod_{t=1}^{|v|} x_{it}!} \prod_{t=1}^{|v|} P(w_t|C)^{x_{it}} \quad (4)$$

Eşitlik 4'te C sınıflandırılacak belgenin ait olabileceği sınıfı (SMS spam tespiti için spam ve spam olmayan olmak üzere iki sınıf belirlenmektedir.), D_i sınıflandırılması yapılmak istenilen *i.* belgeyi, $|v|$ bir sınıfa ait olan belgelerde yer alan toplam kelime sayısını, w_t D_i belgesi içerisindeki *t.* terimi x_i D_i belgesine ait özellik vektörünü ifade etmektedir. x_{it} x_i özellik vektörüne ait *t.* eleman olup, w_t teriminin D_i belgesinde geçme sayısını temsil etmektedir. $n_i = \sum_t x_{it}$ D_i belgesindeki toplam kelime sayısı ile hesaplanmaktadır. $P(w_t|C)$ w_t teriminin C sınıfındaki ağırlık değerini ifade etmektedir. $P(w_t|C)$ Eşitlik 5'teki gibi hesaplanmaktadır.

$$P(w_t|C) = \frac{1+\sum_{i=1}^{N} x_{it}}{\sum_{j=1}^{|v|}\sum_{i=1}^{N} x_{ij}} \quad (5)$$

Eşitlik 5'te N belgede geçen toplam terim sayısını ifade etmektedir. $P(w_t|C)$ bir terimin bir belgede yer alma sayısının ($\sum_{i=1}^{N} x_{it}$), ilgili terimin yer aldığı belgedeki terimlerin sayısı ile tüm belgelerde yer alan terimlerin toplamına ($\sum_{j=1}^{|v|}\sum_{i=1}^{N} x_{ij}$) oranı ile hesaplanmaktadır.

IV. Deneysel Çalışma

Çalışmada, MNB Sınıflayıcı metodunda eğitim amaçlı yararlanılmak üzere, Uysal vd. tarafından oluşturulmuş 420 adet spam ve 430 adet spam olmayan Türkçe SMS mesajı içeren TurkishSMS [9] isimli veri seti kullanılmaktadır. Geliştirilen sistemin başarımının test edilmesi aşamasında, sorgu veri seti olarak kullanılmak üzere çeşitli internet sitelerinden elde edilen ve el yordamı ile sınıflandırılan, 200 adet spam ve 200 adet spam olmayan olmak üzere, SMS mesajı niteliğinde Türkçe yazılmış ifadeler içeren TurkishSpamSMS isimli veri seti oluşturulmuştur.

Kullanılan veri setlerine ait içerik bilgileri Tablo 5'te görülmektedir.

TABLO V. Çalışmada Kullanılan Veri Setlerine Ait Bilgiler

	Eğitim Veri Seti	Sorgu Veri Seti
Spam SMS Sayısı	420	200
Spam Olmayan SMS Sayısı	430	200
Toplam SMS Sayısı	850	400
Genel Toplam SMS Sayısı	1250	

Tablo 5'te görüldüğü gibi çalışmada MNB Sınıflayıcı metodunda kullanılmak üzere toplamda 1250 SMS mesajından oluşan eğitim ve sorgu veri seti kullanılmaktadır.

Yapılan çalışmaya ait karmaşıklık matrisi Tablo 6'da görülmektedir.

TABLO VI. Karmaşıklık Matrisi

		Gerçek Değerler	
		Spam SMS	***Spam Olmayan SMS***
	Spam SMS	Doğru Pozitif (a)	Yanlış Negatif (b)
	Spam Olmayan SMS	Yanlış Pozitif (c)	Doğru Negatif (d)

Tablo 6'daki karmaşıklık matrisinde yer alan veriler yardımıyla çalışmanın başarım oranlarının belirlenmesi için kullanılan değerlendirme ölçütlerine (Doğruluk, Duyarlılık, Seçicilik, Yanlış Pozitif Oranı, Yanlış Negatif Oranı, F-Ölçütü) ilişkin hesaplamalar Eşitlik 6-11'de görülmektedir.

$$Doğruluk = (a+d)/(a+b+c+d) \quad (6)$$

$$Duyarlılık\ (Doğru\ Pozitif\ Oranı) = a/(a+c) \quad (7)$$

$$Seçicilik\ (Doğru\ Negatif\ Oranı) = d/(b+d) \quad (8)$$

$$F - Ölçütü = 2a/(2a+b+c) \quad (9)$$

$$Yanlış\ Pozitif\ Oranı = b/(b+d) \quad (10)$$

$$Yanlış\ Negatif\ Oranı = c/(a+c) \quad (11)$$

Eşitlik 6-11'deki hesaplamalara ilişkin elde edilen sonuçlar Tablo 7 ve Tablo 8'de görülmektedir.

TABLO VII. Çalışmanın Başarım Oranları

Değerlendirme Ölçütü	Çalışmanın Başarım Oranı
Doğruluk	(192+198)/(192+8+1+198) = 0.975
Duyarlılık (Doğru Pozitif)	(192)/(192+1) = 0.995
Seçicilik (Doğru Negatif)	(199)/(8+199) = 0.961
Yanlış Pozitif Oranı	(8)/(8+199) = 0.039
Yanlış Negatif Oranı	(1)/(192+1) = 0.005
F-Ölçütü	(2*192)/[(2*192)+8+1] = 0.977

TABLO VIII. Çalışmanın Hata Oranları

Değerlendirme Ölçütü	Çalışmanın Hata Oranı
Yanlış Pozitif	(8)/(8+199) = 0.039
Yanlış Negatif	(1)/(192+1) = 0.005

Tablo 7 ve Tablo 8'de görüldüğü gibi yapılan çalışmanın başarım ve hata oranlarının belirlenmesinde ilgili değerlendirme ölçütleri kullanıldığında; Doğruluk Değeri: %97.5, Duyarlılık Değeri: %99.5, Seçicilik Değeri: %96.1, F-Ölçütü: %97.7, Yanlış Pozitif Değeri: %3.9 ve Yanlış Negatif Değeri: %0.5 olarak elde edilmektedir.

V. Sonuç ve Değerlendirme

İstek dışı SMS mesajı trafiği oluşturarak kaynak ve zaman israfına neden olan spam SMS mesajları, haberleşme teknolojisinin en önemli problemleri arasında yer almaktadır.

Çalışmada, Tablo 5'te yer alan veri setleri kullanılarak MNB Sınıflayıcı metodu yardımı ile Türkçe yazılmış SMS mesajları içerisinde spam olanların tespit edilerek

sınıflandırılması amaçlanmıştır. Yapılan çalışma sonucunda, %97.5 oranında bir doğruluk oranı ile spam SMS mesajlarının tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Gelecekte makine öğrenmesi ve sözlük tabanlı yöntemlerin bir arada kullanıldığı hibrit yapılar kullanılarak, Türkçe içerikli SMS mesajları üzerinde spam tespiti yapılmasına yönelik çalışmalar planlanmaktadır.

KAYNAKLAR

[1] Türkiye Elektronik Haberleşme Sektörü Üç aylık Pazar Verileri Raporu, 2016 Yılı 4.Çeyrek (Ekim-Kasım-Aralık), Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Mart 2017.

[2] Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar Tarihi: 12.04.2016, Karar No:2016/DK-YED/211.

[3] G. Sethi, and V. Bhootna, "SMS spam filtering application using Android." Int. J. Comput. Sci. Inf. Technol.(IJCSIT) 5.3 (2014): 4624-4626.

[4] E. Ezpeleta, U. Zurutuza, and J.M.G. Hidalgo, "Short Messages Spam Filtering Using Sentiment Analysis." International Conference on Text, Speech, and Dialogue. Springer International Publishing, 2016.

[5] Y.Yang, R. Hu, C. Qiu, G. Sun and H. Li, "A Spam Message Detection Model Based on Bayesian Classification." International Conference on Emerging Internetworking, Data & Web Technologies. Springer, Cham, 2017.

[6] Y.S. Bozan, Ö. Çoban, G.T. Özyer ve B. Özyer, "Metin Sınıflandırma ve Uzman Sistem Tabanlı İstenmeyen Kısa Mesajların Filtrelenmesi SMS Spam Filtering based on Text Classification and Expert System."

[7] F. Akbari, G. Z. Parast and H. Sajedi, "SMS spam detection using selected text features and boosting classifiers." Information and Knowledge Technology (IKT), 2015 7th Conference on. IEEE, 2015.

[8] W. Li and S. Zeng, "A Vector Space Model based spam SMS filter." Computer Science & Education (ICCSE), 2016 11th International Conference on. IEEE, 2016.

[9] A. K. Uysal, S. Gunal, S. Ergin and E. S. Gunal, "The impact of feature extraction and selection on SMS spam filtering." Elektronika ir Elektrotechnika 19.5 (2013): 67-72.

[10] A. A. Akın and M. D. Akın, "An Open Source Natural Language Processing Library for Turkic Languages: Zemberek." Electrical Engineering 431 (2007): 38.

[11] Ç. Kaya ve O. Yıldız, "Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz." Marmara Fen Bilimleri Dergisi 26.3 (2014): 89-104.

[12] Z. Pawlak, "A rough set view on Bayes' theorem." International Journal of Intelligent Systems 18.5 (2003): 487-498.

[13] A. McCallum and K. Nigam, "A comparison of event models for Naïve bayes text classification." AAAI-98 workshop on learning for text categorization. Vol. 752. 1998.

[14] J. Chen, H. Huang, S. Tian and Y. Qu, "Feature selection for text classification with Naïve Bayes." Expert Systems with Applications 36.3 (2009): 5432-5435.

Implementation and Evaluation of Improved Secure Index Scheme Using Standard and Counting Bloom Filters

Leyla Tekin
Department of Computer Engineering
Izmir Institute of Technology
Izmir, Turkey
leylatekin@iyte.edu.tr

Serap Şahin
Department of Computer Engineering
Izmir Institute of Technology
Izmir, Turkey
serapsahin@iyte.edu.tr

Abstract

This paper presents an improved Secure Index scheme as a searchable symmetric encryption technique and provides a solution that enables a secure and efficient data storage and retrieval system. Secure Index scheme, conceived by Goh, is based on standard Bloom filters (SBFs). Knowledge of the limitations of SBFs, such as handling insertions but not deletions, helps in understanding the advantages of counting Bloom filters (CBFs). Thus, we have extended this scheme by adding a new algorithm so that CBFs can also be applicable. Unlike the old scheme, our scheme can handle dynamic update of a document by updating the existing index without rebuilding it. Moreover, we give a complementary comparison of both filters in our scheme. Finally, a detailed performance evaluation shows that our scheme exhibits similar performance with regard to the query overhead and the false positive probability and is quite efficient than the old scheme with regard to the update overhead by allocating more space.

Index Terms

Searchable symmetric encryption, keyword search, indexes, bloom filters, counting bloom filters, data privacy, dynamic update, cryptography, security.

I. INTRODUCTION

In recent years, vast amounts of data are produced by several sources such as millions of digital sensors, social media applications, smart phones, financial transaction records etc. Thanks to many capabilities offered by cloud computing, data owners and organizations have extensively moved their huge datasets from traditional local data centers to the cloud so that they can utilize the possibilities of greater flexibility and lower cost. However, this requires to be kept their sensitive data on remote untrusted servers and introduces new security and privacy challenges that needs to be handled. Therefore, these data are encrypted before sending to the untrusted servers in order to protect the data confidentiality. Although data encryption ensures data confidentiality, it certainly prevents the server from operating on the data, especially searching over it.

The search functionality enables a data user to receive the related data with a keyword from a remote data server. The proposed solutions to perform a keyword search over the encrypted data are (i) downloading all the stored data to the user side, decrypt it locally and search the keyword over the decrypted data and (ii) allowing the server to decrypt the data and search the keyword, and return the related results to the user. The first approach downloads the entire data when a keyword search is performed, even if a very small part of the data is related to the search keyword. Hence, it leads to an increase in communication overhead. The second approach allows the server to know the secret key and plaintext.

On the other hand, various searchable encryption schemes have been developed to support searching over encrypted data in a secure and efficient way. Tang [4] presents a systematic study on search in encrypted data. Three application scenarios, which have motivated a number of theoretical searchable encryption schemes, are described in that paper. These application scenarios are: (i) search in outsourced personal database, (ii) email routing service and (iii) matching in internet-based PHR (personal healthcare records) systems.

In the first scenario, there can be a user who may want to access her personal database anytime and anywhere. Thus, the user can outsource her database to a third-party service provider. To provide a privacy-preserving solution, the user can encrypt her database and outsource the ciphertext to the service provider. Then, she can send a search query to the service provider which search the query in the encrypted database and return the encrypted contents related to the search criteria. In the second scenario, there can be an email service provider which offers secure email service to its users. In this situation, a user can have all her mails encrypted using her public key which may be known by every entity. Later on, she can submit a search query to the service provider which search the query in encrypted emails and send back the interesting emails to the user. In the third scenario, an internet-based PHR system can allow users to store, access, edit and also share their PHRs. A PHR data of a user can have a lot of sources. Since PHRs are sensitive information, there should be a secure solution to meet the privacy problem. For this, the user can have her PHR data encrypted under her public key using an encrypted search scheme. Then, the user can authorize third-party servers to match her encrypted data.

In addition to the above application scenarios, two categorizations for search schemes over encrypted data are pre-

sented in [4]. The first categorization is based on whether a scheme supports full-domain or index-based search. In full-domain setting, a search will check every data item one by one for some criteria. In index-based search, the search criteria is tested based on index(es) rather than the contents of all data items. Furthermore, in terms of the second categorization, the schemes can be modeled using either symmetric or asymmetric setting. The first symmetric-setting scheme, proposed by Song et al. [5], allows only the client to create the searchable encrypted data and trapdoors. The first asymmetric-setting scheme, introduced by Boneh et al. [6], enables every entity to create the encrypted data, but only the client can generate valid search trapdoors.

The study in this paper matches the first application scenario explained above and focuses on a searchable symmetric encryption scheme which performs index-based search. We have chosen Secure Index scheme, developed in [2], to implement searches on encrypted documents. The scheme is based on (standard) Bloom filters (SBFs) that are fast probabilistic data structures for representation of a set in order to answer membership queries. However, Bloom filters do not support element deletions. Unlike Bloom filters, counting Bloom filters (CBFs) are able to support element additions and deletions dynamically. In this manner, we have proposed an improved scheme of Secure Index that can allow dynamic updates on documents without rebuilding operation.

The rest of the paper is organized as follows. Section II gives information about the research background on standard and counting Bloom filters. Section III describes our enhanced Secure Index scheme. Section IV presents the system algorithms. In Section V, we point out performance evaluation. Finally, we discuss related work and conclude the paper in section VI and VII, respectively.

II. BACKGROUND

In this section, we will provide a detailed background on standard and counting Bloom filters by describing the properties and operations of the filters, analyzing the mathematical model for false positive probability and deciding trade-offs between performance parameters.

A.Bloom Filters

Bloom filters are introduced by Burton Bloom in 1970 [1]. A Bloom filter is a fast probabilistic data structure that allows to test whether an element is a member of a set in a limited memory space. Although it is more space-efficient to represent a set than other data structures like linked lists, arrays, hash tables etc., it does not always produce 100% correct results. It can result in false positives that occur when it suggests that an element is in a set even if the element is not, but the bloom filter does not lead to false negatives. The basic Bloom filter supports two operations that involve adding elements to the set and querying for the membership of elements.

Now, let us look at the detailed description of a Bloom filter. The filter is a bit array of length m to represent a set S = {s1, …, sn} of n elements. It uses k distinct independent hash functions h1, …, hk, each of them maps some element to the interval [1, m] with a uniform random distribution. All bits are firstly set to 0. Then, to insert each element si in the set S, the array bits at positions h1(si), …, hk(si) are set to 1 on the bit array. Some bits can be set to 1 multiple times by coincidences for different elements. To test whether an element q belongs to the set S, the array bits corresponding to the positions h1(q), …, hk(q) are checked. If at least one bit is set to 0, then q is definitely not a member of S. However, if all the checked bits are set to 1, then q is a member of the set S with a high probability. This means that there is some probability of a false positive.

The false positive probability that occurs in a Bloom filter can be calculated under the assumption that a hash function chooses each array position with equal probability, as specified in [7]. Before quantifying the probability, some notations to be used are examined: m = the number of bits in the Bloom filter, n = the number of elements in the set, k = the number of hash functions, and fp = the false positive probability.

After defining the notations, now we will demonstrate how the false positive probability can be calculated. During the insertion of an element into the filter, the probability that a specific bit is set to 1 by a hash function is (1/m). So, the probability that this specific bit is not set to 1 by a hash function is (1–1/m). Since there are k hash functions, the probability of not setting the bit to 1 after all the hash functions are applied is $(1–1/m)^k$. After inserting all elements of the set into the filter, the probability that the bit is still 0 is $(1–1/m)^{kn}$. Therefore, the probability that the bit is 1 can be found as $1– (1–1/m)^{kn}$. A false positive can occur for an element that is not in the set if each of the k array positions obtained by the hash functions is 1. Hence, the false positive probability fp can be estimated, as in

$$fp = (1 – (1 – 1 / m)^{kn})^k \approx (1 – e^{– kn / m})^k. \quad (1)$$

For fixed m and n, the value of k that minimizes fp can be computed by setting the derivative of the equation with respect to k to 0, which gives the optimal value of $k_{opt} = \ln 2 * (m/n)$. So, using the optimal k, the false positive probability is $(1/2)^k \approx 0.6185^{m/n}$. The required array size m for the desired number of elements n and false positive probability fp is given by $m = – (n* \ln(fp)) / (\ln 2)^2$. It means that for a fixed false positive probability fp, there is a linear relationship between the array size m and the number of inserted elements n.

As can be seen in the Equation 1, fp varies according to three parameters: m, n and k. We test the mathematical formula of the false positive probability with different values for these parameters in order to see the behavior of the theoretical mathematical model, and draw the graphs shown in Fig. 1.

As a result, the variation of the fp with respect to the parameters can be illustrated in Fig. 1: (i) if m increases, fp decreases, (ii) if n increases, fp also increases and (iii) if k increases for fixed m and n, fp at first decreases, then reaches a minimum, then increases. Therefore, there exists a trade-off between three performance metrics which are computation

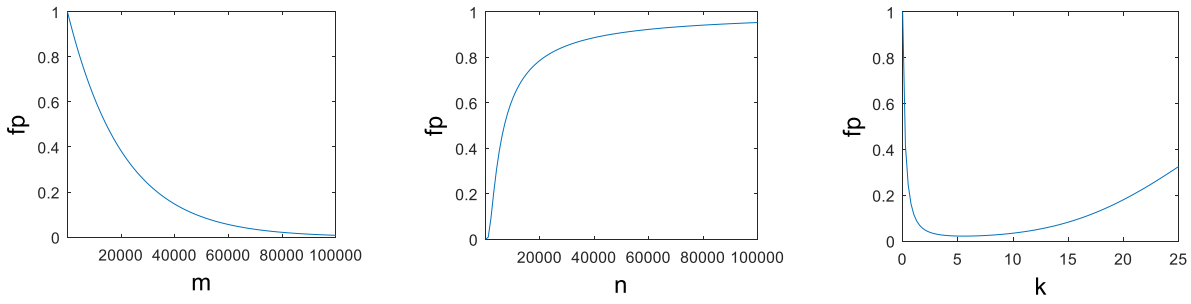


Fig. 1. The changes of fp with respect to m, n and k. (a) fp as a function of m. (b) fp as a function of the n. (c) fp as a function of k using fixed m and n values. In (a) and (b), an optimal number of hash functions has been assumed.

time (corresponding to k), storage cost (corresponding to m) and probability of error (corresponding to fp).

B.Counting Bloom Filters

Standard Bloom filters do not allow element deletions by resetting ones back to zeros because there can be coincidences and a bit can be set by multiple elements. To address such a problem, Fan et al. [3] propose counting Bloom filters in which an array of counters are used instead of bits. Initially, all counters are set to 0. When an element is inserted, the relevant counters are incremented and when an element is deleted, the relevant counters are decremented. To answer whether an element is contained in a set, check if all the counters corresponding to the hash functions are nonzero. In this context, a counter keeps track of the number of elements currently hashed to that location. The selection of counter size is also important to avoid counter overflow. According to the work in [7], four bits are enough for most applications.

The structure of a counting Bloom filter is similar to that of a standard Bloom filter. Hence, it can represent a set of n elements with m counters using k independent hash functions. Also, it can yield a false positive probability, which does not depend on the counter size, as in Equation 1.

III. PROPOSED SOLUTION: IMPROVED SECURE INDEX SCHEME

Secure Index scheme introduced in [2] consists of four algorithms such as Keygen, Trapdoor, BuildIndex and SearchIndex. The scheme uses (standard) Bloom filters to track words in documents. A Bloom filter represents a static set. Therefore, the scheme updates a document by regenerating the Bloom filter index of the document. On the other hand, a counting Bloom filter can represent a dynamic set. In this study, we add a new algorithm which is UpdateIndex to the scheme. This new algorithm uses counting Bloom filters, and so supports dynamic updates on documents more efficiently by just updating the existing counting Bloom filter index of the document. So, in the below algorithms other than UpdateIndex, both standard and counting Bloom filters can be used.

Keygen(s): The key generation algorithm takes a security parameter s and generates a pseudorandom function f and a master private key $K_{priv} = (k_1, \ldots, k_r)$.

Trapdoor(K_{priv}, w): This algorithm takes the master key Kpriv and word w as input, and outputs the trapdoor for word w by calculating the r pseudorandom functions which are computed efficiently from the word and one part of the master key. So the trapdoor can be shown as:

$T_W = (f(w, k_1), \ldots, f(w, k_r))$.

BuildIndex(D, K_{priv}): The algorithm focuses on index generation. Given a document D including a unique identifier D_{id} and a list of words, and the master key, it generates an index for the document D_{id}.

The steps to create the index for the given document and master key are given below:

First, for each unique keyword w_i in the document:

1) The trapdoor is calculated using the Trapdoor(K_{priv} ,w_i) algorithm, so the trapdoor is:

$T_{wi} = (x_1 = f(w_i, k_1), \ldots, x_r = f(w_i, k_r))$.

2) Trapdoors are not directly inserted to the Bloom filter against correlation attacks. Therefore, the codeword C_{wi} is calculated using the generated trapdoor and the identifier of the document, which ensures the creation of different codewords representing the same word for different documents. The codeword for wi in document Did is:

$C_{wi} = (y_1 = f(D_{id}, x_1), \ldots, y_r = f(D_{id}, x_r))$.

3) The codeword $\{y_1, \ldots, y_r\}$ can be inserted into the Bloom filter of the document D_{id} by setting 1s to the bit positions corresponding to $\{y_1, \ldots, y_r\}$.

Next, the algorithm continues with the blinding the Bloom filter that starts by computing an upper bound u on the number of tokens in the document. The Goh's paper [2] suggests one token for every byte in the document after it has

been encrypted.

Then, v is determined as the number of unique words in the document, and now the bloom filter is blinded by inserting (u – v)*r random 1's. It equals to adding (u – v) random words into the filter, except for the computing any pseudorandom function.

Finally, the index $I_D = (D_{id}, BF)$ is returned as the index for the document D_{id}.

SearchIndex(Tw, ID): It takes the trapdoor $T_W = (x_1, \ldots, x_r)$ for word w and the index $I_D = (D_{id}, BF)$ for document D_{id}.

To test whether the document contains the keyword or not, the following steps are performed:

1) The codeword for word w is calculated using the given trapdoor and D_{id} in a similar manner as described above:

$C_{wi} = (y_1 = f(D_{id}, x_1), \ldots, y_r = f(D_{id}, x_r))$.

2) Test if all bits at positions $\{y_1, \ldots, y_r\}$ in the Bloom filter are set to 1.

3) If the Bloom filter's reply is positive, then output 1. Otherwise, output 0.

UpdateIndex(D, D', K_{priv}, I_D): The algorithm takes two versions of a document which are the previous version D and the updated version D', the master key and the index of the document.

This algorithm is valid when counting Bloom filters are used in the scheme. The steps to update the taken index are explained below:

Firstly, the counting Bloom filter CBF is obtained from the index.

Then, for each unique keyword w_i that is included in the previous version D, but not included in the updated version D' of the document:

1) The trapdoor is calculated with the Trapdoor(K_{priv}, w_i) algorithm.

2) The codeword is computed using the trapdoor and the document id.

3) The codeword is deleted from the filter.

Next, for each unique keyword w_i that is not included in the previous version D, but included in the updated version D' of the document, the trapdoor and codeword are calculated, and inserted into the filter.

As the last step, the index $I_{D'} = (D_{id}', CBF)$ is returned as the index for the document D_{id}'.

IV. IMPROVED SECURE INDEX APPLIED TO ENCRYPTED SEARCH

Until now, theoretical background on standard and counting Bloom filters are investigated, and our improved Secure Index scheme is given. Now, in this section, we will mention how the search system can be created. Actually, Goh [2] explained how Secure Index scheme can be applied to search on encrypted documents and described the system algorithms using the setup, search and update algorithms. But, our system has some differences, specifically in update algorithm. Then, our system consists of five algorithms: setup, search, add a document, delete a document and update a document.

Algorithm 1 – Setup

This algorithm is run on the user side to set up the system, in which either standard or counting Bloom filters can be used. The user has n documents which will be outsourced to the server. The algorithm consists of the following steps:

1) Firstly optimal Bloom filter parameters should be selected. Then, the user runs the Keygen(s) algorithm with the chosen parameters to get the pseudo-random function f and the master private key K_{priv}.

2) An integer $i \in [1, n]$ is associated with each document as its unique identifier.

3) An index is built for each document D_{id} by invoking the BuildIndex(D_{id}, K_{priv}) algorithm.

4) Each document is compressed and encrypted using standard encryption algorithms. Finally, the encrypted documents along with their indexes are uploaded to the server.

Algorithm 2 – Search

When the user wants to search the document collection stored on the server for the word y, the two steps are required as follow:

1) The user generates the trapdoor T_y using the Trapdoor(K_{priv}, y) algorithm and sends T_y to the server.

2) The server checks every index I_{Di} by calling SearchIndex(T_y, I_{Di}) algorithm to find all documents that contain the word y. Then, all matching documents are returned to the user.

Algorithm 3 – Add a document

If the user wants to add a new document to the document collection:

1) A unique identifier is assigned to this document.

2) Then, an index is built for this document by using the BuildIndex algorithm.

Algorithm 4 – Delete a document

The deletion algorithm includes:

1) Deleting the document and its index from the server.

Algorithm 5 – Update a document

When the user wants to update a document, the user takes the encrypted version of the related document from the server. Whether downloading the index for the document or not, depends on using standard or counting Bloom filters.

If standard Bloom filters are used, the steps to update the document are explained in detail below:

1) The encrypted document is decrypted and the document is updated.

2) A new index is created for this document with a new document identifier.

3) The document is encrypted again.

4) The new index and encrypted document are sent to the server.

If counting Bloom filters are used, the user also retrieves the counting bloom filter index of the related document from the server. The steps to update the document can be listed as follows:

1) The first step is similar to that of the standard Bloom filter.

2) The user has the previous and updated version of the document, thereby the UpdateIndex algorithm can be called to update the counting Bloom filter index.

3) The document is re-encrypted.

4) The updated index and the encrypted document are transmitted to the server.

V. PERFORMANCE ANALYSIS

We implement the system based on our enhanced scheme using java language on an Intel Core i5-2410M 2.30 GHz CPU with 4GB RAM running Windows 10 operating system. Both user and server operations are performed on the single machine so we do not consider latency that may occur in practice. We use HMAC-SHA1 for the keyed hash function, which has been suggested in the original scheme and AES-128 with CBC and PKCS5 padding for encryption.

To evaluate the proposed scheme, we mainly compare standard Bloom filters with counting Bloom filters in our scheme in terms of four performance metrics which are: (i) the false positive probability, (ii) the query overhead, (iii) the storage overhead and (iv) the update overhead. For this, all operations are performed in memory. Furthermore, operations such as encryption, which are the same for both the filters, are not taken into account in comparisons.

We conduct some experiments on a real data set of 500 RFC (Request for comments) [8] files that are numbered from 2001 to 2500 with a total size about 26 MB and some experiments on our own data set which are created from RFC files. The RFC file set includes a large number of technical and organizational keywords about the Internet and many of these keywords are unique to the file in which they are used.

We use Apache Lucene [9] to extract keywords from each RFC file by tokenizing the text, converting the characters to lowercase, removing stopwords and reducing words to a root form, namely stemming. Therefore, when a keyword is searched, initially all these operations are performed on this keyword, and then the corresponding trapdoor and codeword are computed.

In order to measure the performance of the certain pieces of our code correctly, we utilize from Java Microbenchmark Harness (JMH) [10] which is a powerful tool to build, run and analyze micro-benchmarks. We write benchmark codes for our scenarios and execute them by specifying some parameters, such as the number of warmup and measurement iterations, the benchmark mode, and so on. Now, we will explain five cases detailedly below.

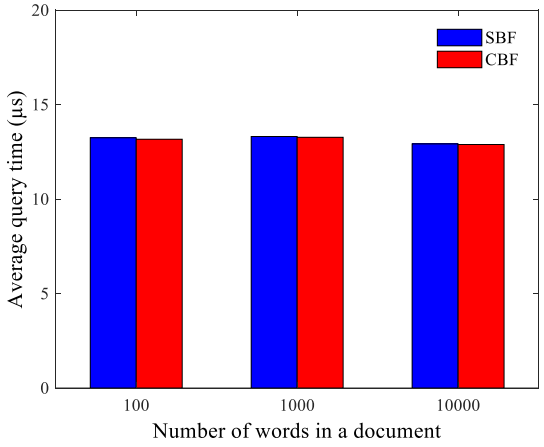


Fig. 2. Average query time (µs) vs. number of words in a document

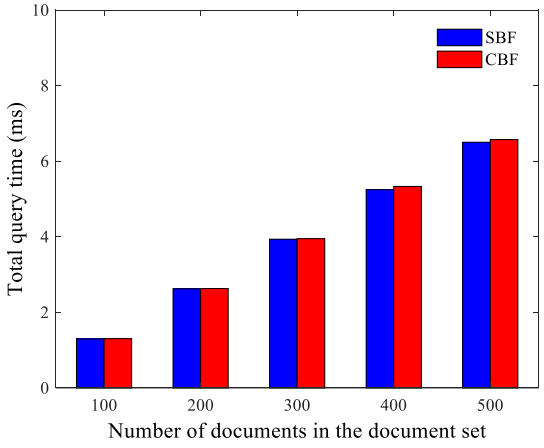


Fig. 3. Total query time (ms) vs. number of documents in the document set

A. Case 1: Average query time (µs) against file size (or number of words in a document)

In this experiment, 3 files of different lengths, such as 100, 1000 and 10000 keywords, are derived from the keywords in the RFC files. The keyword "algorithm" is selected to search on the encrypted files. In both the Bloom filters, number of hash functions r is kept at 5. This search procedure is repeated 100 times and the average results are calculated.

Figure 2 gives information about how much average query time of two filter types in µs is spent for different file sizes. From the figure we demonstrate that SBF has almost the same average query time as CBF for all file sizes. This reason is that the number of hash functions in both of the filters is kept at the same value which is 5. We also see that file size does not affect the query time.

B. Case 2: Total query time (ms) against number of documents in the document set

For this experiment, we use 5 subsets of 20%, 40%, 60%, 80%, and 100% of the RFC files to show impact of the number of documents in the document set on the total query time. We choose the keyword "communicate" to search on the en-

crypted subsets of files. In the both Bloom filters, number of hash functions r is kept at 5 as in case 1. The search procedure is repeated 25 times and then total query times are computed.

Figure 3 illustrates total query time of the filters for different number of documents in the document set. According to the figure, SBF has almost the same total query time as CBF for different number of documents due to keeping the number of hash functions in both of the filters at a certain level. Moreover, as shown in the figure, the query time of the filters increases linearly with the number of documents.

C. Case 3: Update time (ms) against number of added words

In this experiment, 3 different-length files are derived from the keywords in the RFC files as in case 1. We add 1, 10, 20 and 50 different words to these files in order to measure the update overhead of the two filter types. This update procedure is repeated 100 times.

Figure 4 shows the update overhead of the filters when different number of words are added to the files in three cases of 100,1000 and 10000-word files. It can be seen that CBF outperforms SBF for all cases. We also demonstrate that the update overhead of SBF dramatically increases as file size increases.

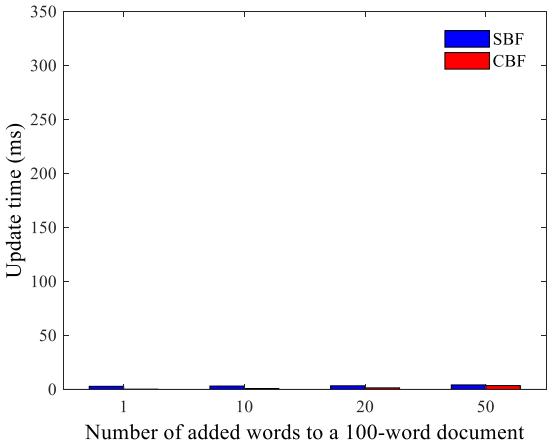
D. Case 4: Update time (ms) against number of deleted words

In contrast to case 3, now we delete 1, 10, 20 and 50 different words from the created files in order to measure the update overhead of the two filter types. This procedure is also repeated 100 times.

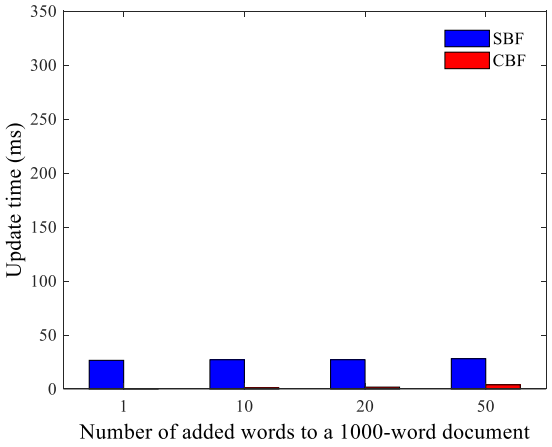
Figure 5 depicts the update overhead of the filters when different number of words are deleted from the files in three cases of 100,1000 and 10000-word files. As in the case 3, it can be viewed from the Fig. 5 that CBF outperforms SBF for all cases. Also, the update overhead of SBF grew more quickly as file size increases.

E. Case 5: Expected, currentAdded and currentDeleted false positive probability of CBF against number of added/deleted words

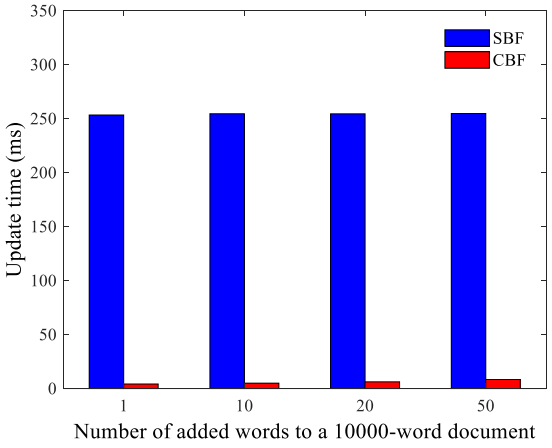
Figure 6 illustrates expected, currentAdded and currentDeleted false positive probability of CBF against number of added/deleted words to/from varying-length documents, such as 100, 1000 and 1000 words. According to the figure, false positive probability of CBF increases as words are added to the filter, and decreases as words are deleted from the filter. Additionally, the probability changes much more rapidly in the small documents.



(a)

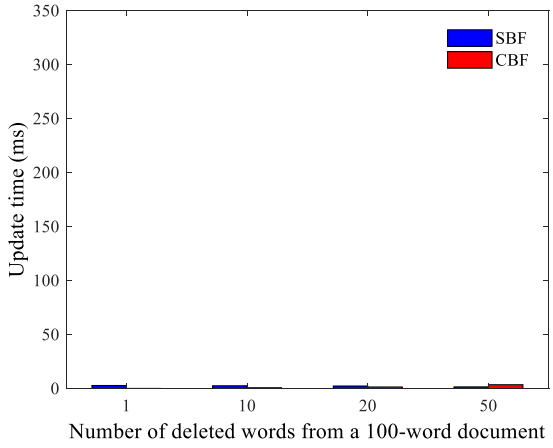


(b)

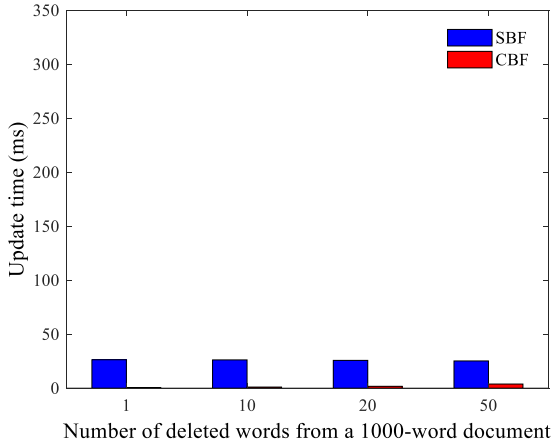


(c)

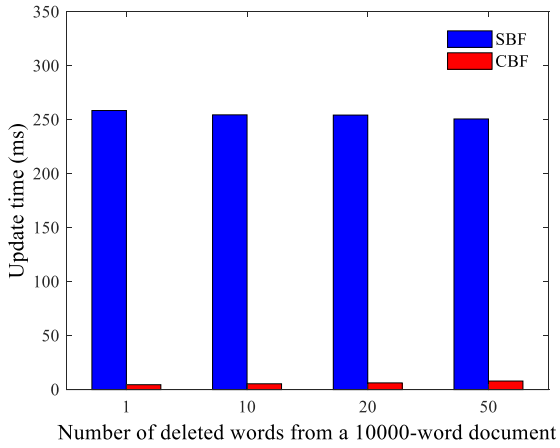
Fig. 4. Update time (ms) vs. number of added words for varying-length documents



(a)

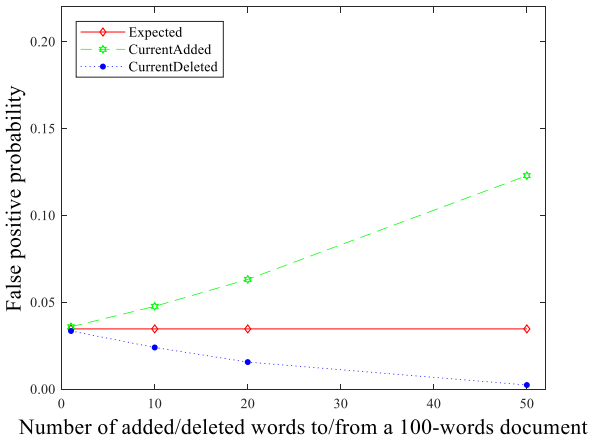


(b)

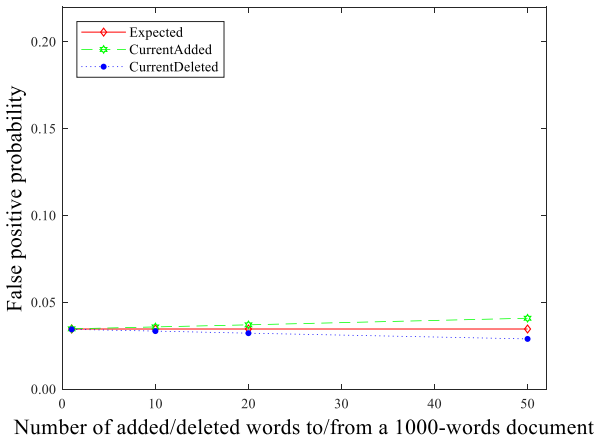


(c)

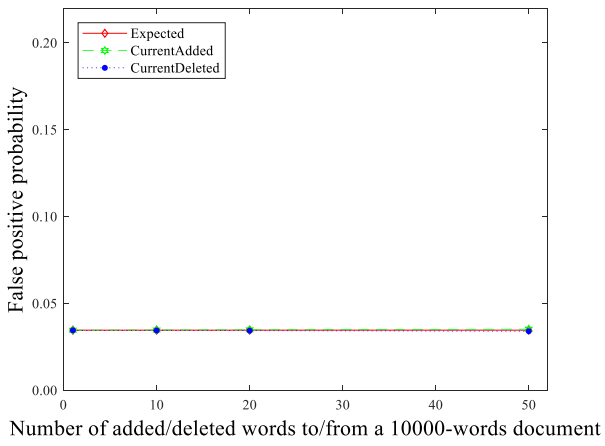
Fig. 5. Update time (ms) vs. number of deleted words for varying-length documents



(a)



(b)



(c)

Fig. 6. False positive probability of CBF vs. number of added/deleted words to/from varying-length documents

VI. DISCUSSION

Dynamic Searchable Symmetric Encryption schemes allow the document collection to be modified after setup phase. Chang and Mitzenmacher [11] proposed two schemes in which a keyword dictionary can be stored or not stored on the mobile device of the user. A masked index string is created for each document in their approach, and so the search time is linear in the number of documents as in this paper. Also, they studied secure updating of the documents. In their approach, deletion of a document along with its encrypted index is simple, but updating a document is required to delete this document with its encrypted index, and then building a new encrypted index for a new document. Whereas, in our approach updating a document can be performed by only updating the corresponding existing index of it.

The dynamic SSE schemes [12, 13, 14] are based on inverted-index so for each unique keyword a searchable index is generated. [13] and [14] support the ability to add and delete documents efficiently, however they do not take into account updating the contents of documents. If a document is added, the user will generate the add token for this document by producing values for each unique keyword in it, and then send the add token to the server which will update the encrypted index. If a document is deleted, this time the user will create a delete token and send it to the server which will update the encrypted index. [12] enables only adding new documents to the document collection as updates. In this scheme, search is logarithmic in the number of keywords, but the size of the encrypted index is large and the number of updates supported are limited.

As a result, although our improved scheme has linear search time and IND-CKA security model which provides security if search queries are independent of the previous queries, it is efficient in terms of update time.

VII. CONCLUSION

This paper suggests an improved Secure Index scheme to perform searches and updates on encrypted documents. The old scheme supports updating a document but it requires to rebuild the standard Bloom filter index of the document. On the other hand, our scheme can handle updating a document by only updating the counting Bloom filter index. Then, we implement our scheme with standard and counting Bloom filters, and compare the performance of the filters regarding different metrics. Comprehensive experiments demonstrate that the proposed scheme performs better in terms of the update overhead by achieving the same accuracy and almost the same query overhead, and using slightly larger space. Especially if large documents are used, update operation takes much less time.

REFERENCES

[1] B. Bloom. "Space/time tradeoffs in in hash coding with allowable errors", Communications of the ACM, vol. 13, no. 7, pp. 422-426, 1970.

[2] E.-J. Goh, "Secure indexes", Cryptology ePrint Archive, Report 2003/216, 2003.

[3] L. Fan, P. Cao, J. M. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," IEEE/ACM Trans. on Networking, vol. 8, no. 3, 2000.

[4] Q. Tang, "Search in encrypted data: Theoretical models and practical applications", Cryptology ePrint Archive, Report 2012/648, 2012.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," IEEE Symposium on Security and Privacy, pp. 44–55, 2000.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proceedings of the Advances in Cryptology-Eurocrypt 2004, pp. 506–522, 2004.

[7] S. Tarkoma, C.E. Rothenberg, E. Lagerspetz, "Theory and practice of bloom filters for distributed systems," IEEE Communications Surveys and Tutorials, vol. 14, no. 1, pp. 131–155, 2012.

[8] RFC, "Request For Comments Database", available at http://www.ietf.org/rfc.html.

[9] Apache Lucene, available at https://lucene.apache.org/.

[10] JMH, " Java Microbenchmark Harness", available at http://openjdk.java.net/projects/code-tools/jmh/.

[11] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third International Conference on Applied Cryptography and Network Security (ACNS), pp. 442–455, 2005.

[12] P. van Liesdonk, S. Sedghi, J. Doumen, P. Hartel,W. Jonker, "Computationally efficient searchable symmetric encryption", in Secure Data Management, Springer, Berlin, Heidelberg, 2010, pp. 87-100.

[13] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption", In the ACM Conference on Computer and Communications Security, CCS'12, pp. 965-976, 2012.

[14] R. Ramasamy, S.S. Vivek, P. George, and B. S. R. Kshatriya, "Dynamic verifiable encrypted keyword search using bitmap index and homomorphic MAC", Cryptology ePrint Archive, Report 2017/676, 2017.

Review of Evidence Collection and Protection Phases in Digital Forensics Process

Prof. Dr. Asaf VAROL
Fırat University, Technology Faculty
Software Engineering Department
Elazığ, Türkiye
varol.asaf@gmail.com

Yeşim ÜLGEN SÖNMEZ
Fırat University, Technology Faculty
Software Engineering Department
Elazığ, Türkiye
yesimulgen123@gmail.com

Abstract

This study reviews crime scene investigation, collection of evidence, and protecting evidence phases of digital forensic process based on the research in the literature. Using appropriate methods for collecting and protecting electronic evidence would contribute to digital forensics and information technology law. In order to have effective evidence analysis, the first phases of the digital forensic process need to be completed through appropriate methods. In this study, the main emphasis will be on digital forensics process as well as hardware and software utilized during this procedure.

Index Terms: Digital forensic process, collecting evidence and protecting evidence

I. INTRODUCTION

The fundamental purpose of digital forensics can be described as discovering, protecting, collecting, analyzing and presenting legal and electronic evidence that are seen as potential to solve a crime [1, 2]. Digital forensics aim to find digital evidence for numerous cases ranging from identifying the hacker on a hacking case to solving the murder [3].

In digital forensics, the purpose is not to point out a person as guilty or innocent. It aims to present numerical evidences to forensic units in other form as complete and impartial interpretation of the evidence. Determining whether a person is guilty or not will be held by judicial authorities as a result of conveying these evidences to forensic units through digital forensic processes [4].

Some fields of study in digital forensics can be listed as data recovery, data annihilation, data conversion, encryption, decryption, finding under cover files, identifying criminals with the help of IP numbers [5].

II. DIGITAL FORENSIC PROCESS

Digital forensics phases can be described as processes followed in order to find/analyze/report about forensically important information [6]. Digital forensic phases are listed in the Figure 1 [3, 4, 6, 7]; these phases are: describing evidence, which starts with the crime scene investigation, collecting evidence, protecting evidence, analyzing the evidence, and reporting and presenting the evidence.

There is a starting point for every process [8]. The process can start with an alarm from the attack determination system i.e. Intrusion Detection Systems, suspicious records on the firewall, warnings from the security system on the network, denunciation of an individual, or denunciation of any crime cases [8, 9].

Figure 1. Digital Forensics Cycle Model [6].

The purpose of value evaluation is to determine whether there will be a detailed investigation process or not [8, 9]. Later, procedures and protocols which will be applied in the crime scene are identified. People who are responsible for the security of the crime scene are first responders or digital forensics specialist. Their trainings needed in this subject depend on protocols identifying the crime scene (such as video and photograph) beforehand [8, 9]. Later, protection and collection of data phase starts. Figure 2 shows these phases.

Figure 2. Phases of Electronic Evidence Collection

A.Identification and Collection of Electronic Evidences

Figure 3 shows the steps of crime scene investigation and initial steps of evidence collection [10, 11]. In this phase, the purpose for experienced researchers is not to collect all virtual or physical evidences. They must decide what needs to be collected.

Then they must create a document and finally perform the action [8]. Having a detailed report for each collected evidence eases their verifiability and starts the chain of custody [8]. How and by whom all transport and conservation processes are conducted in accordance with laws are put under a protocol [12].

B.Protection of Electronic Evidences

Within the scope of protection of evidence, it is required to denote in which situation, where and in which conditions the evidences are collected in the crime scene. In other words, it is required to know the integrity of collected evidences [13]. This can be actualized through the conscious work of the police force in the phases of protection of evidences after gathering, identification, collection and sending them to the laboratory for investigation [14]. In Figure 4, the processes used to protect of evidence are shown.

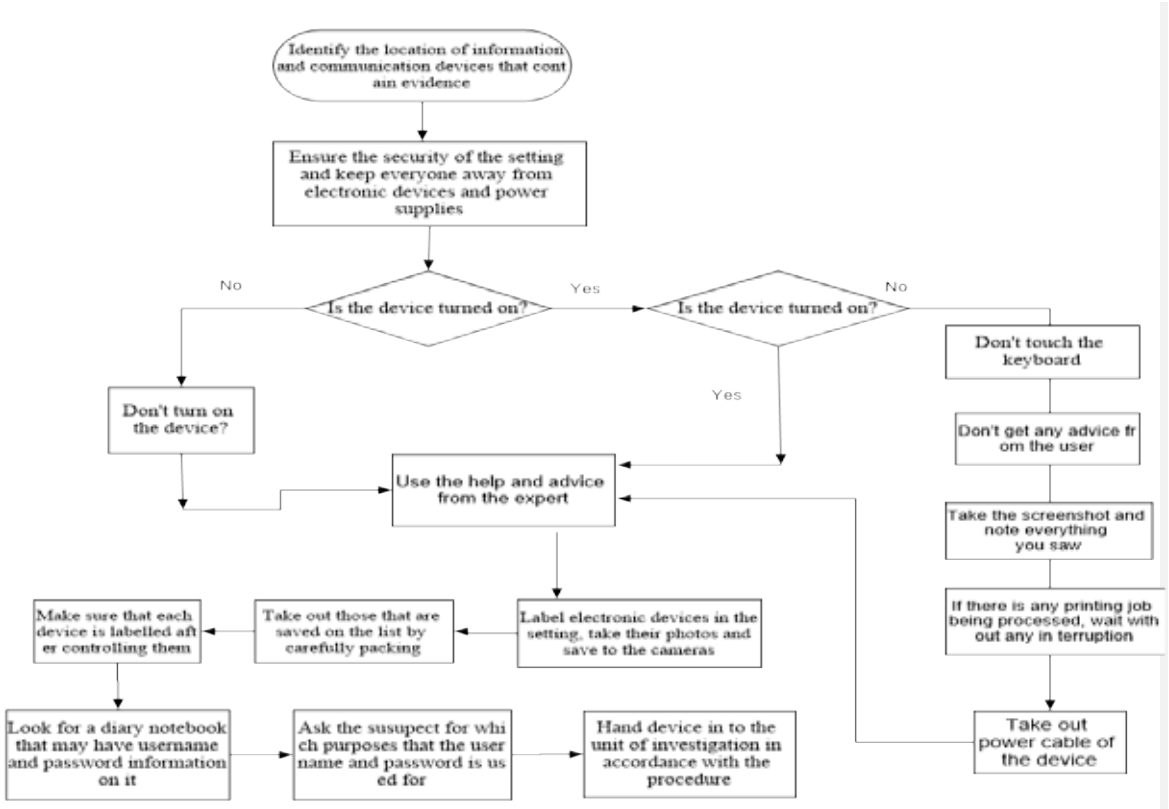


Figure 3. Crime scene investigation activity flow chart [10, 11].

Figure 4. Protection of electronic evidences

In this phase, there is digital protection and physical protection [8]. Digital protection is consisted of various mechanisms proving that the evidences have not been distorted from the first moment of their gathering and their integrity has not been lost. This process is usually done through using cryptographic techniques. Physical protection is consisted of carrying the evidences to the location of investigation without any distortion, preserving them in appropriate settings until the court date and ensuring the prevention of any distortion of the evidences while being carried to the court. In these phases, evidences are labeled, appropriately packed, and sealed [8].

C. Capturing Image

In computer criminalistics, the image (forensic image) is the name of the exact copy that is taken for investigation [3]. It is critical to obtain the copy in a way to include exactly all bits on the hard drive (bit stream back up) [13]. In other words, the content of the copied disk would be obtained as exactly the same [15]. There are two methods of capturing the image. The first is capturing image through hardware, the other is capturing image through software [16].

Hardware image capturing tools obtain the image of the evidence by following the image capturing methods on its embedded operating system through establishing a physical

data connection with the original evidence. The advantages of these products are not needing any computer and being available to capture the image in the crime scene [16]. The process of writing on the original evidence is blocked with the features of "Write Block".

Some hardware image capturing devices can be listed as following [11, 16]:

- Image Masster
- Tableu Forensic Duplicator
- Digital Intelligence
- MyKey
- Falcon
- The Rapid Image 7020
- Data Copy King
- BeeCube

There are two hardware products used in digital forensics: a write block device and an image capturing device [11].

In Figure 5, the capturing of the image through Tableau image capturing device with the help of the software in this device without needing any external computer or software is shown.

Figure 5. Copying device named Tableau TD2 [18].

The image capturing process with a write block device is shown in Figure 6. An image capturing software and computer is needed to capture image through write block device. The differences between the two are reviewed and it is reported that write blockers creates several problems [17].

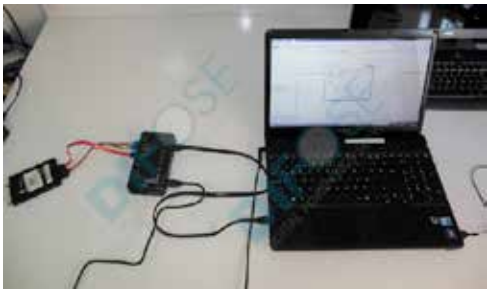


Figure 6. Write block image capturing device named Tableau T35es [18].

After getting connected to the original evidence computer through physical data connection in the image capturing process with image capturing software on the electronic environment, the image of the evidence is captured by following the steps in the image capturing software [16].

These products do not need external "Write Block" devices. In order to preserve the integrity of the original evidence, "Write Block" feature is included in the software and whether the evidence is distorted or not during the copying is determined via checksum values produced by using some verification algorithms (MD5 and SHA1 etc.) as a result of the image capturing process [16]. Some of the software image capturing devices can be listed as below [16]:

- Norton Ghost Imager
- FTK Forensic Imager
- Encase Forensic Imager
- X-Ways Imager
- Helix 3 Pro
- Win image Snapback
- AIR (Automated Image and Restore) and Guymager
- It is possible to capture RAM memory image via Belkasoft Live and Dumpit [19].
- Cellebrite UFED, XRY, Paraben, Tarantula, Flasher Box, Faraday, TULP 2G, Bitpim, Deft, Paraben's Device Seizure, Oxygen Forensics Suite and Caine mobile devices, can extract data from mobile phones, sim cards, GPS devices, navigation devices, tablet computers, and pocket computers at international standards [20].
- Moreover, Linux-based digital forensic devices such as FIREBrick can be used instead of commercial software required devices [21]. Although Paraben and Belkasoft Evidence Centre are used for instant messaging investigations, there are also new solutions being developed for instant messaging [22].

D.Write Block

Write blocks, which are used for write protection, are software or hardware products that are developed to capture and investigate images by preserving evidence integrity [11]. In case if write blocking is not used, malware such as virus, trojan, etc can attack the computer during the image capturing process and the data might be written on the evidence and it will loose its integrity [11]. In digital forensics, using hardware write blocking devices presents less risk.

E. Hash Algorithm

Hash algorithm, which is used to determine the integrity of evidence, is obtained by multiplying all 0s and 1s on the computer media with a certain algorithm [23, 24].

As a result of image capturing process, there are two different hash values automatically created by the software that is used. Acquisition hash is the hash algorithm of the original evidence device, whereas verify hash is the hash algorithm showing that the evidence integrity of the digital material is not distorted after the investigation. These two hash values should be the same. Otherwise, one may claim that the evidence is distorted. Due to the nuncupative principle of "in

dubio pro reo" (suspected defendant) in criminal justice law, even if there is evidence showing a committed crime, the suspect can't be punished even if the evidence is accidentally altered [11].

While the hash value is a value that is 32-characters long, consisted of characters including 0-9 and a-f for MD5, it is a value that is 40-characters long consisted of the same characters for SHA1 [24]. The sample MD5 and SHA1 hash values of an image obtained within the scope of a study are given below:

MD5 : e8359ebbe97f3bae584c76971059c35b

SHA-1 : 5dbd53e4e7b0f6b8dd19d084af57722da83018e9

In the phase of protecting electronic evidences,

- This sum value is given to both parties after being signed by parties [6],
- Putting evidences in anti-static materials to prevent them being exposed to static electric current [6],
- Putting them separately when packing to prevent them interact with each other [6],
- The most important point for the evidence protection is to use qualified personnel that has adequate knowledge and experience on the subject [6],
- Appropriately recording the data that are in the crime scene but not directly available and can easily fade away (volatile, deleted, idle data, network connections) [6].

In digital forensics, there are different techniques (fuzzy hashing) and new algorithms (mrsh-v2, sdhash) that are being worked on for the correlation of similar files [23]. There are also academic studies conducted on mvHash-B algorithm that is used to identify the similarities between two dataset [25].

III. RECOVERY

Before starting a complete analysis of the conserved digital evidences, it is necessary to discover deleted, hidden, transfigured data, or data that is non-displayable with current operating system or file system. This is called data recovery. This process is not conducted on original evidences, but on their duplicates (exact copies) [8].

IV. DECOMPOSITION

The purpose is to bring together the data according to their specific characteristics in order to provide easiness for the research. For instance, since the child pornography cases [26] are usually based on visual digital data, files with the extension of gif, jpeg, etc. are often brought together for investigation [8].

V. REDUCTION AND ORGANIZATION

Among the collected data, those that are directly related to the subject are vital for a digital forensics investigation. Selection criteria is carefully determined as it can be questioned during the court [8].

It is necessary to organize, group, label reduced data and place them meaningful units. The purpose is to ensure that researchers find and describe the data during the analysis and give references to them in a meaningful way during the testimonial. For this purpose, a data index is created as well [8].

VI. CONCLUSION

The first two phases of evidence capturing analysis is done through a series of hard drive and software devices whether it is open source or proprietary. These devices are continuously developing in line with the technology and changes in devices.

Among digital forensics phases, the data analysis phase is supported less. There are only a few software devices available for this phase. It is critical to obtain evidences in an accurate and credible way while analyzing the evidence. Knowing the existing applications of evidence collection and preservation phases in literature, actualizing new methods to apply these processes would make contributions to both digital forensics and information technology law. Reporting in every step, would help law enforcement units to make correct decision from the beginning of the digital forensics process, namely from first crime scene investigation to evidence collection and evidence preservation phases.

REFERENCES

[1] Ş. Sağıroğlu and M. Karaman "Adli Bilişim," Telepati Dergisi, no. 203, p. 62, 2012.

[2] Y. Kim and K. J. Kim, "A Forensic Model on Deleted-File Verification for Securing Digital Evidence," 978—1-4244-5493-8710 IEEE, 2010.

[3] A. H. Ekizer, "Adli Bilişim (Computer Forensics)," [Online]. Available: http://www.ekizer.net/content/view/16/1/. Access: 14.10.2016

[4] M. Özen and G. Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)," Ankara Barosu Dergisi, 2015.

[5] M. Z. Gündüz, Bilişim suçlarına yönelik IP tabanlı delil tespiti- IP-based evidence detection, Elazığ: Fırat Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2013.

[6] M. Orta, Bilişim Suçlarında Adli Analiz, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, 2015.

[7] L. Keser Berber, Adli Bilişim, Ankara: Yetkin Yayınlar, 2004.

[8] Y. Uzunay, "Dijital Delil Araştırma Süreci," http://slideplayer.biz.tr/slide/1918963/, Ankara, 2005.

[9] E. Casey, Digital Evidence and Compter Crime Scene, ABD: AP, 2004.

[10] T. Henkoğlu, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, İstanbul: Pusula Yayıncılık 2.Baskı, 2014.

[11] Y. Başar, Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri, Afyon Kocatepe Üniveristesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2015.

[12] R. Adams, V. Hobbs and G. Mann, "The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice," Journal of Digital Forensics, Security and Law, JDFSL., cilt

8, no. 4, pp. 25-48, 2013.

[13] R. J. Vacca, Computer Forensics, Second Edition, Charles River Media, Inc.IBSN: 1–58450–389–0, 2005.

[14] M. Kaygısız, Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği, Adalet Yayınevi Birinci Baskı, 2007, p. 4.

[15] "CHIP Online," [Online]. Available: http://www.chip.com.tr/forum/Bilisim-Suclarinin-Delillendirilmesi_t8007.html. [Access: 06 10 2016].

[16] H. Aydoğan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü Yüksek Lisans Tezi, 2009.

[17] G. Kessler and G. Carlton, "A Study of Forensic Imaging in The Absence of Write-Blockers," Journal of Digital Forensics, Security and law, JDFSL., cilt 9, no. 3, pp. 51-58, 2014.

[18] "DIFOSE Digital Forensics Services," [Online]. Available: http://www.difose.com.tr/blog/index.php/testler/89-solid-state-disk-adli-kopyasi. [Access: 06 11 2016].

[19] A. Ekim, Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2013.

[20] M. Ukşal, Mobil Cihazlarda Adli Bilişim, İstanbul: İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2015.

[21] L. Tobin and P. Gladyshev, "Open Forensic Devices," Journal of Digital Forensics, Security and law, JDFSL., cilt 10, no. 4, pp. 97-104, 2015.

[22] R. V. Voorst, M.-T. Kechadi and N.-A. Le-Khac, "Forensic Acquisition of IMVU: A Case Study," Journal of Digital Forensics, Security and Law, JDFSL, cilt 10, no. 4, pp. 69-78, 2015.

[23] F. Breitinger and İ. Baggili, "File Detection on Network Traffic Using Approximate Matching," Journal of Digital Forensics, Security and Law, JDFSL, cilt 9, no. 2, pp. 23-36, 2014.

[24] M. S. Kılıç, Elektronik Deliller ve Yapısal Özellikleri. Edit: H. Çakır and M.S. Kılıç Adli Bilişim ve Elektronik Deliller, Ankara: Seçkin Yayıncılık, 2014.

[25] D. Chang, S. K. Sanadhya and M. Singh, "Security Analysis of MVHASH-B Similarity Hashing," Journal of Digital Forensics, Security and Law, JDFSL, cilt 11, no. 2, pp. 21-34, 2015.

[26] J. Eggestein and K. Knapp, "Fighting Child Pornography: A Review of Legal and Technological Developments," Journal of Digital Forensics, Security and Law, JDFSL, cilt 9, no. 4, pp. 29-48, 2014.

Statik Analizi Kullanarak Android Kötücül Yazılım Tespit Teknikleri Üzerine Bir İnceleme

A Survey On Android Malware Detection Techniques Using Static Analysis

Pelin Şirin
Gazi Üniversitesi Bilişim Enstitüsü
Bilgisayar Bilimleri
Ankara, Türkiye
pelin.sirin@gazi.edu.tr

İbrahim Alper Doğru
Gazi Üniversitesi Teknoloji Fakültesi
Bilgisayar Mühendisliği
Ankara, Türkiye
iadogru@gazi.edu.tr

Murat Dörterler
Gazi Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği
Ankara, Türkiye
dorterler@gazi.edu.tr

Özet

Mobil cihazların günlük hayatın vazgeçilmez bir parçası haline gelmesiyle birlikte, günümüzde mobil cihazlar daha fazla hassas bilgiye hükmeder hale gelmiştir. Özellikle bu alanda kullanım bazında artan popülaritesi ve açık kaynaklı yapısıyla Android, bu hassas bilgileri paylaşan mobil işletim sistemleri arasında kendini zirveye taşımayı başarmıştır. Bu ilerleme, her ne kadar olumlu yönlere sahip olsa da, beraberinde getirdiği büyük risklerle kullanıcıları tehdit etmektedir. Gelişmiş mobil zararlı yazılımlar, kullanıcılara ait verileri onların onayını almadan edinir veya kullanırlar. Buna bağlı olarak kötücül yazılım tespit sistemleri geliştirilse de son zamanlarda gelişmiş tespitten kaçınma tekniklerini kullanan yeni nesil kötücül yazılımların ortaya çıkmasıyla, etkin tespit mekanizmaları geliştirme çabaları daha zorlu bir hal almıştır. Bu nedenle, kötücül yazılım analizi ve tespiti için etkili teknikler tasarlamak son zamanlarda daha fazla önem kazanmıştır. Bu çalışma kapsamında android kötücül yazılım tespit teknikleri arasından statik analiz yaklaşımına odaklanılarak statik analiz yaklaşım trendleri vurgulanmıştır. Aynı zamanda, gelecek çalışmalarının hala ihtiyaç duyulduğu kilit yönleri belirlenerek Android uygulamaları statik olarak analiz eden son çalışmaların net bir görünümünün sunulması amaçlanmaktadır.

Anahtar Kelimeler

Mobil Cihazlar Güvenliği, Mobil Kötücül Yazılım Tespiti, Statik Analiz, Statik Analiz Araçları.

Abstract

With mobile devices becoming an indispensable part of daily life, smartphones are privy to increasing amounts of sensitive information. Especially, with its increasing popularity and open-source nature, Android has managed to summit itself among the mobile operating systems that share this sensitive information. Although this advancement has positive aspects, it threatens the users with the great risks it brings. Sophisticated mobile malware acquire or utilize data from the users without their consent. Depending on this, efforts to develop effective detection mechanisms have become more challenging with strains employing highly sophisticated detection avoidance techniques in recently, although malicious software detection systems are developed. For this reason, designing effective techniques for malicious software analysis and detection has more and more important in recent times. In this study, by focusing on the static analysis approach among the android malware detection techniques, static analysis approach trends are highlighted. It is also aimed to present a clear view of the state-of-the-art works that statically analyzes Android applications by identifying the key directions that future work is still needed.

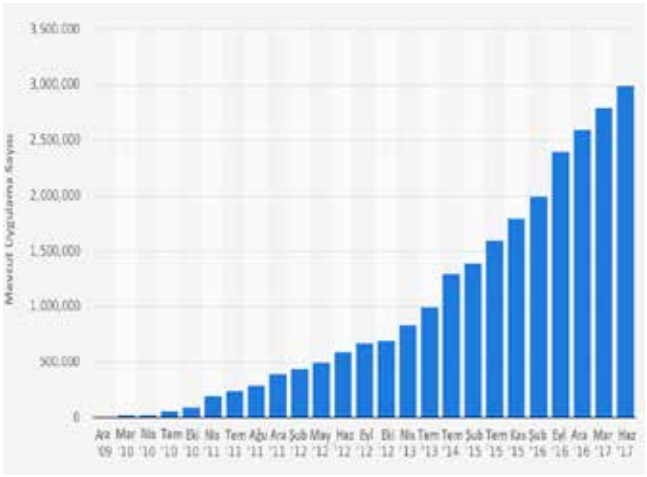
Keywords

Mobile Devices Safety, Mobile Malware Detection, Static Analysis, Static Analysis Tools, Android Security.

I. GİRİŞ

2008'de piyasaya çıkan Google'ın Android işletim sistemi, kötücül yazılım yazarlarını ilk iki yılda üzerine çekecek kadar geniş bir kullanıcı tabanına sahip değildi. Ancak, 2010 yılında artan kullanımla birlikte, kötücül yazılımlar için potansiyeli yüksek bir platform haline geldi. Günümüzde ise, Android uygulamaların sayısı her geçen yıl katlanarak büyüme eğilimi göstermektedir. Öyle ki, International Data Corporation (IDC) firmasının 2016 3. çeyrek raporuna göre; Android, akıllı telefon pazarında %86.8 gibi çok yüksek bir pay elde etmiştir[1]. Bununla birlikte, Mart 2017'de açıklanan rakamlara göre Google Play Store'daki mevcut uygulama sayısı 2.8 milyonu bulmuş durumdadır [2]. Android uygulamaları artık tüm kullanıcı etkinliklerine yayılmış olduğundan, önceden tasarlanan kötücül uygulamalar, çeşitli şiddette hasarlara neden olabilecek büyük tehditler haline gelmiştir Bu hasarlara örnek olarak uygulama çökmeleri (app crashes), kötücül yazılımların ücretli SMS göndermesiyle maddi kayıplar, özel veri sızıntılarıyla ilgili itibar sorunları verilebilir. Anti-virüs üreticileri ve güvenlik uzmanlarından gelen veriler, Android ekosistemindeki kötücül yazılımların arttığına dair düzenli olarak rapor vermektedir. Örneğin, McAfee firmasının 2017 yılında sunmuş olduğu 'McAfee Labs Threats Report' adlı raporuna göre bu tespit edilen toplam mobil kötücül yazılım sayısı 2015 yılının ilk çeyreğinde yaklaşık 4 milyon olarak tespit edilmişken, 2016'nın son çeyreğinde bu rakam yaklaşık 16 milyon seviyesine yükselmiştir [3]. Ayrıca bu kötücül yazılımların yaklaşık

%74'ü Android platformunu hedef almaktadır[4]. Android işletim sisteminin diğer mobil işletim sistemleri arasında bu denli yüksek bir oranda hedef haline gelmesi, hiç şüphesiz ki onun açık kaynak kodlu yapısı, kendi resmi uygulama mağazası Google Play'in çok sayıda ücretsiz uygulama barındırması ve bu alanda yeterli denetimin yapılmamasından kaynaklanmaktadır. Nitekim, yine McAfee firmasının bu yıl sunmuş olduğu 'Trojans, Ghosts, and More Mean Bumps Ahead for Mobile and Connected Things' adlı raporuna göre 2016 yılında, Google Play'den kullanıcılara bildirimde bulunmadan kaldırılan 4,000' den fazla uygulama tespit edilmiştir. McAfee Mobile Threat Research tarafından toplanan telemetre verileri, 500.000' den fazla cihazın hala bu uygulamaları yüklediğini ve uygulamaların aktif olduğunu göstermektedir [5]. Bu kullanıcılar ve onların çalıştıkları kuruluşlar, hala bu ölü uygulamalarda bulunan güvenlik açıklarına, gizlilik risklerine veya kötü amaçlı yazılımlara maruz kalmaktadır.



Şek. 1. Google Play Store' daki mevcut uygulama sayısı [2].

Söz konusu tehditlerle başa çıkmak için Android'in çeşitli yönleri araştırılmıştır. Sözdizim ve anlamsal hataları tanımlamak, hassas veri sızıntılarını tespit etmek ve açıkları taramak için geniş bir program analizi yelpazesi önerilmiştir. Çoğu durumda, bu analizler statik olarak gerçekleştirilir; yani, bu analiz biçimi esasen Android uygulama kodunu çalıştırmadan mağazalardaki binlerce uygulamayı hedefleyerek yalnızca ölçeklenebilirliği sağlamakla kalmaz, aynı zamanda mümkün olan tüm yürütme yollarının keşfedilmesi de garanti edilir. Maalesef, Android programlarının statik analizi basit bir uğraş değildir, çünkü analizin doğruluğunun ve eksiksiz olmasını sağlamak için Android'in farklı spesifik özniteliklerini hesaba katmak gerekir. Performans araçlarının tasarımında ve uygulanmasında yaygın engeller arasında, Dalvik bayt kodu analizi veya çevirisi ihtiyacı, çağrı diyagramı yapısını başlatmak için bir ana giriş noktasının bulunmaması ve tüm Android programının çalıştığı olay işleyicilerini (event handler) hesaba katmada kısıtlamaların olması bulunmaktadır. Bu özel zorlukların yanı sıra, Android, yansıtıcı çağrıların nasıl çözüleceği ve dinamik kod yükleme ile nasıl başa çıkılacağı gibi Java programlarının analizi için bir takım zorlukları da taşımaktadır. Bu nedenle, bu alanda gerçekleştirilen onlarca çalışmaya rağmen gelişmiş araçlar hala bazı analiz özniteliklerinin eksikliğinden dolayı zorluk çekmektedir.

Android kötücül yazılım tespitinin statik analiz alanına duyulan ilginin yoğunluğu nedeniyle, halihazırda yaklaşım ve araç üreten çok sayıda çalışma mevcuttur. Ayrıca, literatürde Android güvenliği üzerinede birçok araştırma makalesi bulunmaktadır. Ancak, bu alandaki araştırma çalışmaları incelendiğinde, tek başına statik analiz üzerine yoğunlaşarak, bu üretilen yaklaşımların bir araştırmasını yapan çalışma sayısı yok denecek kadar azdır.

Bu çalışma, Android uygulamalarının statik analizi için kapsamlı bir araştırmanın gereğini yerine getirme girişimi olup, makalenin kalan kısımları şu şekilde organize edilmiştir: Bölüm 2'de Android uygulama bileşenleri ve statik analiz teknikleri incelenerek Android uygulamalarının statik analizinin kilit yönleri hakkında ayrıntılı bir genel bakış sağlamak amaçlanmaktadır. Ayrıca, Android'e özgü statik analiz zorlukları ve kullanılan statik öznitelikler ele alınmıştır. Bölüm 3'te, ilgili araştırma yayınlarının bir dizisi belirlenerek statik analiz yaklaşımının kullanıldığı son çalışmalardan oluşan bir literatür taraması yapılmıştır. Son olarak Bölüm 4'te, Android uygulamalarında statik analiz çalışmalarının mevcut kısıtlamaları özetlenmekte ve potansiyel yeni araştırma yönleri ortaya konmaktadır.

II. ANDROİD VE STATİK ANALİZ ÜZERİNE TEMEL BİLGİLER

Statik program analizi, bir programın kaynak kodunu (veya bazı durumlarda nesne kodunu) girdi olarak alıp bu kodu yürütmeden inceleyerek ve kod yapısını, ifade dizilerini ve değişken değerlerinin farklı fonksiyon çağrıları boyunca nasıl işlendiğini kontrol ederek sonuçları veren otomatikleştirilmiş bir aracı gerektirmektedir.

Genel olarak, Android'deki zararlı yazılım tespit sistemleri hem statik hem de dinamik tespit tekniklerinin kombinasyonunu kullanmaktadır. Bu iki tespit yönteminin her ikisinin de kendine göre avantajları bulunmaktadır. Statik analizin en büyük avantajı, yazılım piyasaya sürüldükten sonra kendiliğinden ortaya çıkmayan hataları (veya zayıf noktaları) ortaya çıkarabilmesidir. Statik analiz, kötücül yazılımın çalıştırılmaması yalnızca analiz edilmesinden dolayı özellikle bellek açısından sınırlı Android cihazlarda daha kullanışlı olması nedeniyle tercih edilmektedir. Ayrıca bu analiz türü, belirli bir uygulama kod bloğunun yürütümüyle sınırlı olmayıp bir uygulamanın bütünüyle analizinin gerçekleştirilmesini sağlayabilmektedir. Buna karşın dinamik analiz tekniği esas olarak önceden tanımlanmış davranışları eşleştirme durumlu örneklerle ilgilenmektedir. Statik analizde, uygulama kodu çalıştırılmadan önce tespit sonuçları alınır. Bu nedenle kötücül davranışların gizlenmesi veya değiştirilmiş olması zordur. Ayrıca, statik analiz yönteminin hesaplama maliyetini ve uygulama verimliliğini tahmin etmek kolaydır. Ancak, dinamik analiz yöntemi dağıtım ortamından etkilenmektedir ve tespit iş yükü genellikle daha yüksektir. Bununla birlikte, statik analiz yöntemi yazılım şifreleme ve örtük fonksiyonlardan etkilenebildiğinden, kap-

samlı bir Android kötücül yazılım tespiti yapmak için dinamik analiz yönteminin de statik analizin gerekli bir tamamlayıcısı olduğu durumlar olabilmektedir. Ancak bu yazının kapsamı, statik analiz yöntemleri ile sınırlı tutulmuş, bu yöntemlerin özellikleri ve avantajları gözden geçirilmiştir.

Android uygulamalarının statik analizini yapabilmek için uygulamalar üzerinde tersine mühendislik işleminin yapılması gerekmektedir. Tersine mühendislik kullanılarak java dosyalarının içerikleri görüntülenebilmekte ve kötücül kod parçacıkları bulunabilmektedir. Tipik bir statik analiz süreci aşağıdaki adımlardan oluşur:

1) Programın alt yordamları arasındaki çağrı ilişkilerinin bir soyutlamasını göstererek analiz eden bir çağrı diyagramı (CG) oluşturulur;

2) Tüm programın yapısının daha ince ayrıntılarını içerecek şekilde bir Kontrol Akış Diyagramı (CFG) oluşturulabilir, örn, bir alt metot içindeki tüm yolların açıkça belirtilmesi;

3) CFG'ın farklı noktalarındaki değişkenlerin değerleri gibi diğer bilgiler, statik analizin daha kapsamlı olarak gerçekleştirilebilmesi (örn, veri akışı veya takma ad analizi yoluyla) amacıyla toplanabilir.

A. Android Uygulamalarının Temel Bileşenleri

Android uygulamalarının statik analizinin yapılabilmesi için öncelikle uygulamaların iç yapısının anlaşılması gerekir. Android uygulamaları dört temel bileşenden oluşmaktadır. Şekil 2, bu bileşenleri ve olası etkileşimlerini göstermektedir:

Şekil 2. Android uygulamalarının temel bileşenlerine genel bakış.

Etkinlik (Activity), bir kullanıcının uygulama ile etkileşiminde giriş noktası olarak görev yapan temel bileşenlerden biridir. Bir aktivite, kullanıcı arayüzüne sahip tek bir pencereyi ifade eder. Bu pencere üzerinde etiket, metin giriş alanları ve buton gibi program elemanları yer alır. Aktiviteler Activity sınıfından türetilir.

Servis (Service), uzun süren işlemleri veya uzaktan çalışmaları gerçekleştirmek için arka planda çalışan bir bileşendir. Servislerin bir kullanıcı arayüzü yoktur. Farklı bileşenler servisi başlatabilir, çalıştırabilir veya iletişime geçmek için servise bağlanır. Servisler Service sınıfından türetilir.

Mesaj Alıcısı(Broadcast Receiver), sistem mesajlarına işlem yapan bileşendir. Mesaj alıcıları bir kullanıcı arayüzü kullanmaz, ancak bir mesaj iletildiğini kullanıcıya bildirmek üzere bir durum çubuğu bildirimi oluşturur. Mesaj alıcıları BroadcastReceiver sınıfından türetilir ve Intent nesnesi olarak dağıtılır.

İçerik Sağlayıcı (Content Provider), uygulamaya ait paylaşılan verileri yönetir. Veriler, uygulamanın erişim sağlayabileceği web veya disk üzerindeki bir dosya sistemine veya SQLite veritabanına kaydedilebilmektedir. İçerik sağlayıcısı, uygulamaya özel bilgileri okumak ve yazmak için kullanılır. Ayrıca yetkisi olan diğer uygulamalar da bu bileşen sayesinde verileri sorgulayabilir veya değiştirebilir. Bir içerik sağlayıcısı ContentProvider sınıfından türetilir.

Android bileşenleri, bileşenler arası iletişimi (ICC) tetiklemek için kullanılan startActivity() gibi belirli metotlarla birbirleriyle iletişim kurar. Bir uygulamanın yapacağı herhangi bir işte "amacı" belirtmek için Intent sınıfı kullanılır. Intent nesnesi, kaynak bileşenin iletişim kurmasını istediği hedef bileşen hakkında bilgi içeren bir nesnedir. ICC metotları, Intent nesnesini bir parametre olarak alır ve böylelikle bileşenler arası iletişim gerçekleşir[12].

B.Statik Analizde Kullanılan Teknikler

1) Prototipik Teknikler:

Prototipik yani ilktip teknikler, 90'lı yılların başında başlayan zararlı yazılımların önlenmesi ve keşfedilmesinde kullanılan temel analiz teknikleridir. Statik analiz, nesne yönelimli programlama için prototipiktir, ancak Android'e uyarlanarak geliştirilmiştir. Elbette, Android ortamına özgü karakteristiklerden dolayı, yeni sistem semantiklerini doğru bir şekilde analiz etmek için çoğu teknik yeniden uyarlanmıştır.

a) Giriş Noktası Analizi (Entry Point Analysis): Bu analiz, bir programın nereden başlanarak çalıştırılacağını belirler. Bir program genellikle Java'da main method olarak belirtilen tek bir giriş noktası ile başlar. Android uygulamalarının ise bir main metotu yoktur. Bunun yerine, her uygulama programı, çalışma zamanında Android framework'üyle dolaylı olarak çağrılan birkaç giriş noktasını içerir. Bu nedenle, bu analiz Android için zordur.

b) Ulaşılabilirlik Analizi (Reachability Analysis): Bu analiz, bir program değişkeni v'den bir program değişkeni w'ye ulaşabilirlik durumunun, v'den itibaren, w'ye bağlı olan nesneye götüren bellek yerleri yolunu takip etmenin mümkün olup olmadığını belirlemektir[6].

c) Alan İlk değer Atama Analizi (Field-initialization Analysis): Bir program içindeki değişken atamayı veya buna bağlı olarak eksikliğini statik olarak izleyen geleneksel bir analiz yötemidir.

d) Yan Etki Analizi (Side-effects Analysis): Bu analiz, bir metodun hangi parametrelerinin yürütülmesiyle etkilenebileceğini izler.

e) Döngüsellik Analizi (Cyclicity-Analysis): Döngü içeren veri yapılarının kodunu inceleyen bir analiz tekniğidir. Bu analiz, bir değişkene değer atama eğer bir döngü içerisinde gerçekleştiriliyorsa bunu izler.

f) Yol Uzunluğu Analizi (Path-Length Analysis): Bir prog-

ram değişkeni tarafından izlenebilecek en fazla işaretçi referanstan ayırma(dereferance) sayısını izler.

g) Program Dilimleme (Program Slicing): Program dilimleme, program davranış kümesini azaltmak için program analizi alanında ortak bir yöntem olarak kullanılırken, aynı zamanda ilgili programın davranışını da değiştirmeden tutar. Program p içinde, ilgilendiğimiz bir v değişkeni verildiğinde, olası bir dilim, p'deki v'nin değerini etkileyebilecek tüm ifadelerden oluşacaktır.

h) Kusur Analizi (Taint Analysis): Kusur analizi, değişken etkisi için bir kod tabanlı analizdir. Kusur analizinin ardındaki ana fikir, kullanıcı tarafından (doğrudan veya dolaylı) değiştirilebilir herhangi bir değişkenin bir güvenlik açığı oluşturup oluşturmayacağına bakmaktadır. Daha sonra da veri-akışı analizi aracılığıyla bu değişken izlenir. Eğer kusurlu bir data olmaması gereken bir noktaya akarsa, o zaman bu davranışı durdurup yöneticilere rapor etmek gibi özel komutlar uygulanabilir.

i) İşaretçi Analizi (Pointer Analysis): Bu analiz, belirli özellikler için bellek referanslarının analizidir. Takma ad (Alias) analizi, hangi işaretçilerin birlikte aynı yığın belleğine eriştiğini izler. Paylaşım analizi, örtüşen veri yapılarına bağlı olabilecek olası değişkenleri izler. Points-to(işaretçi) analizi, bir işaretçi değişkenin çalışma zamanında refere edebileceği nesneleri hesaplar. Kaçış analizi, bir programda işaretçinin bellekte erişilebildiği yerleri izler. Şekil analizi, farklı program aşamalarında kaç referanstan ayırmanın(dereference) oluşabileceğini belirler. Bağlı, dinamik olarak tahsis edilmiş veri yapıları özelliklerini keşfeder ve doğrular.

j) Veri Akışı Analizi (Data-Flow Analysis): Veri akışı analizi, bir programdaki her satırda olası değerler kümesini hesaplamak için kullanılan bir tekniktir. Genellikle, temel blok noktalarında bilgileri hesaplamak daha kolay olduğu için, temel blok sınırları bu bilgiyi elde etmek için yeterlidir.

k) Çağrı Diyagramı Oluşturma (Call-Graph Construction): Çağrı diyagramları bir program boyunca fonksiyon çağrılarının statik diyagramlarıdır. Java'da bir program genellikle main method olarak belirtilen tek bir giriş noktası ile başlar. Main method'un kodunu hızlı bir şekilde incelemek, çağırdığı metot(ları) listeleyebilir. Ardından, bu işlemi çağrılan metotların kodu üzerinde yineleme, genelde program analizinde çağrı diyagramı olarak bilinen yönlendirilmiş bir diyagramın kurulmasını getirmektedir. Android'de ise uygulamalar, çoklu çağrı diyagramı "tipleri" ile statik olarak analiz edilebilir. Bir Etkinlik Çağrı Diyagramı (ACG), etkinlik verilerini hassas bir şekilde analiz etmek için oluşturulabilir. Bir Bileşen Çağrı Diyagramı (CCG), anlık bileşen iletişimlerini kesin olarak analiz etmek için statik olarak oluşturulabilir. Wei ve diğerleri[7], android uygulama verisinin veri akışını analiz etmek için Veri Bağımlılığı Diyagramı (DDG) kullanmaktadır. Wei ve diğerleri, bileşenler arasında örtük veri akışını daha kesin olarak analiz etmek için Bileşenler arası veri akışı (IDFG) için bir veri akış diyagramı da sunmuşlardır.

2)Statik Analiz Teknikleri:

a) İmza-Tabanlı Kötücül Yazılım Tespit Tekniği: Bu teknik, ilginç sözdizimsel veya semantik kalıpları, öznitelikleri çıkarır ve belirli zararlı yazılımların eşleştiği benzersiz bir imza oluşturur. İmza tabanlı yöntemler kötücül yazılımların bilinmeyen türlerine karşı başarısız olmaktadır. Ayrıca, imza çıkarma işlemi elle yapılmaktadır ve her kötücül yazılım varyantı için ayrı bir imza kullandığından, imza veritabanı üstel bir hızda büyüyerek üstel benzersiz imza patlaması sonucunda bu analizin etkinliği azalarak sistem kötücül saldırılara karşı açık hale gelebilir[8]. Çoğu anti virüs üreticileri, imza tabanlı kötücül yazılım tespit yöntemlerini kullanmaktadır.

b) Bileşene Dayalı Analiz Tekniği: Ayrıntılı uygulama güvenliği değerlendirmesi veya uygulama analizi gerçekleştirmede kullanılır. Bu teknikte uygulama, AndroidManifest.xml, kaynaklar ve bayt kodu gibi önemli içerikleri çıkarmak için tersine çevrilebilmektedir. Manifest dosyası, bileşenler listesi ve gerekli izinler gibi önemli meta verileri barındırır. Uygulama güvenliği ve değerlendirme çözümleri, güvenlik açıklarını tanımlamak için tanımlamaları ve bayt kodları etkileşimini kullanarak bileşenleri analiz edilmektedir.

c) İzne Dayalı Analiz Tekniği: Android uygulamaları, belirli verilere erişmek için izinlere ihtiyaç duyarlar. Uygulamalar yüklenirken uygulamanın etkinliğini sürdürülebilmesi için kullanıcılara gerekli olan bazı izinleri kabul edip etmediğini sormaktadır[9]. Hiçbir uygulama varsayılan olarak kullanıcı güvenliğini etkileyebilecek herhangi bir izne sahip değildir. Tehlikeli izin isteğini belirlemek kötücül yazılım uygulamasını ifşa etmek için yeterli değildir, ancak yine de izin eşleştirme isteği ve kullanılan izinler önemli bir risk tanımlama tekniğidir[8].

d) Dalvik-Bayt Kodu Analizi: Dalvik bayt kodu, sınıflar, metodlar ve komutlar gibi tip bilgisi içererek semantik açıdan zengindir. Tip bilgileri, uygulamanın davranışını doğrulamak için kullanılabilir. Kontrol ve veri akışına dayalı detaylı analiz, gizlilik sızıntısı ve telefon servisleri suistimali gibi tehlikeli işlevler hakkında bilgi verir [10-12]. Kontrol ve veri akışı analizi, karmaşıklaştırılmamış bir bayt kodu oluşturmak ve önemsiz dönüşüm tekniklerinin etkisini geçersiz kılmak için de yararlıdır[8].

e) Dalvik Bytecode' u Java Bytecode'a Dönüştürme: Java kaynak koduna dönüştürücüler (decompiler) ve statik analiz araçları sayısı, araştırmacıları Dalvik bayt kodunu Java bayt koduna dönüştürmeye teşvik etti. Böylece, Java kodu üzerinde statik analiz kontrol akışı, veri akışı gerçekleştirilebilmektedir.

C. Statik Öznitelikler

Android uygulama paketi (APK) dosyasının içinde java kod dosyalarının sıkıştırılmış hali olan dex dosyası ve AndroidManifest.xml dosyası bulunmaktadır. Statik öznitelikler bu paket içerisindeki özniteliklerden oluşmaktadır. Feizollah ve ark.[13] tarafından gerçekleştirilen çalışmaya göre inceledikleri 100 makaleden 45'i, deneylerini gerçekleştirmek için için

statik öznitelikleri kullanmıştır. Bu statik özniteliklerin arasında araştırmacılar, makalelerinin %36'sında Android izinlerini diğer statik özelliklerden daha fazla kullanmışlardır. Java kodu seçimi makalelerin %29'uyla ikinci gelmektedir. Aşağıdaki bölümlerde statik öznitelikler ayrıntılı olarak ele alınmaktadır.

1) Android İzin Öznitelikleri: Bir uygulama, kurulumundan önce, kullanıcıya istenen izinlerin listesini sağlar. Kullanıcı tarafından izin verilmesi üzerine, uygulama kendisini cihaza kurar. Android 4.2, 200 resmi izin tanımlanmıştır. Google bunları normal, tehlikeli, imza, imza ya da sistem olmak üzere dört gruba ayırmıştır. Bunlardan 29'u normal, 47'si tehlikeli, 63'ü izin seviyesinde, 61'i izin seviyesinde imza ya da sistem iznidir. Uygulamada, geliştiricilerin çoğu normal ve tehlikeli izinlerle uğraşır[14]. Android işletim sistemi Linux mimarisine dayalı olduğundan, izin saldırganların önündeki ilk engeldir. Java kodu kötü niyetli kod içerse de, koddaki bazı API çağrılarının çağrılmasına izin verilmesi gerekir. İzin korumalı API çağrıları, Android işletim sisteminin güvenlik özniteliklerinin bir parçasıdır. Bu nedenle, istenen izinlere dayalı olarak kötücül yazılımları tespit etmek için araştırmacıların odak noktası, diğer statik özniteliklerden daha fazla izin üzerine kurulmuştur.

Araştırmacıların Android izinlerini analiz etmede farklı yaklaşımları vardır. Bazı yazarlar, uygulamaları değerlendirmek için izinleri kullanıp bunları muhtemel risklere dayalı olarak sıralarken, çoğu sadece izinleri çıkarıp kötücül uygulamayı tespit etmek için makine öğrenimini kullanmıştır. Bazı çalışmalarda ise yalnızca istenen izinlerin analizinin kötücül uygulamaları tespit etmede yeterli olmayacağı savunulmaktadır. Bu araştırmacılar, kötücül yazılımları tespit etmek için istenen izinlere ek olarak kullanılan izinleri de analiz etmişlerdir. Backes ve ark. [15] ise bu çalışmalardan farklı olarak, mevcut güvenlik açıklarını gidermek için Android izin sistemini genişletmişlerdir. Sistemlerinin herhangi bir değişiklik yapılmadan veya root erişimi olmaksızın cihazlarda kullanılabilmesi için sistemlerinin Android izin sistemi için pratik bir uzantı olduğunu açıklamışlardır.

2) Android Java Kodu Öznitelikleri: Android mobil kötücül yazılım tespiti üzerine yapılan çalışmalarda, Android işletim sistemine ait Dalvik adlı özel bir biçime derlenen Android uygulamalarının Java kodları üzerinden çeşitli öznitelikler çıkarılmıştır. Bunun için Java kodu üzerinde çeşitli analiz yaklaşımları kullanılmıştır. Bazı araştırmacılar kötücül yazılımları tespit etmek için Uygulama Programlama Arayüzü (API) çağrıları kullanmaktadır. Her Android uygulamasının, cihazla etkileşim kurmak için API çağrılarına ihtiyacı vardır. Bir metottaki API çağrıları ardışıktır. Araştırmacılar böyle bir sırayı, o uygulamaya özgü uygulama imzası olarak değerlendirmektedirler. API çağrılarının sırasını değiştirmek, saldırganların, kod karıştırma denen kötücül yazılım tespit işlemini atlamak için kullandıkları bir stratejidir. Java kodunun kontrol akışının analiz edilmesi araştırmacılar tarafından benimsenen bir başka yaklaşımdır. Saldırganların API çağrılarının sırasını değiştirebilmesine veya tespit sisteminden kaçınmak için API çağrılarını yeniden adlandırabilmesine rağmen Java kodunun akışı değişmez ve araştırmacılar bunu daha güçlü tespit sistemleri geliştirmek için kullanır.

3) Diğer Statik Öznitelikler: Yukarıda açıklanan statik özniteliklerin yanı sıra başka statik öznitelikler de kullanılmaktadır.

a) Intent(Amaç) Filtresi: Intent nesneleri, haberi alacak yazılım bileşenine gönderilen bilgi paketidir. Yazılım bileşeni bilgi paketini alınca hem ne yapması gerektiğini hem de ihtiyacının olduğu bilgileri Intent nesnesinden okur. Bunun dışında Intent nesneleri Android için hangi bileşenin etkin hale geleceğinin belirlenmesini sağlayan bilgileri tutar. Saldırganlar, AndroidManifest.xml dosyasının intent filtresi bölümünde haberleşmenin varlığını gerektiren özel veriler göndermeleri için kötücül yazılımları komuta ettiklerinden, araştırmacılar kötücül yazılımlar için intent filtreleri kullanmaktadırlar.

b) Ağ Adresi: Saldırganlar, kötücül yazılımları kendileriyle iletişime geçerek durumlarını bildirmeleri veya kullanıcıların kişisel verilerini göndermeleri için görevlendirirler. Bu amaçla saldırganlar, kötücül yazılımın kötücül kodlarında komuta ve denetim (C&C) sunucusu olarak bilinen sunucunun adresini yerleştirirler. Araştırmacılar, Android kurulum dosyaları kodunda C&C sunucusunun ağ adresini veya IP adresini arar. Bu nedenle bazı çalışmalarda, ağ adresi statik özniteliklerden biri olarak dahil edilmiştir.

c) Stringler: Bu öznitelikler, uygulamadaki menüler veya uygulamanın bağlandığı sunucu adresi gibi Android dosyasındaki her basılabilir string ayıklanarak toplanır. Çoğu çalışmada bu stringlerin çok boyutlu uzayda vektör olarak gösterilmeleri için Vektör Uzayı Modeli (VSM) kullanılmıştır. Ardından yazarlar, verilerin anomalisini hesaplamak için Manhattan uzaklığı, Öklid uzaklığı ve Kosinüs benzerliği gibi mesafe ölçümlerini kullanmışlardır.

d) Donanım Bileşenleri: Android uygulamaları, örneğin kamera veya GPS gibi çalışmasına ihtiyaç duydukları donanım kombinasyonlarını istemektedir. Örneğin, 3G ve GPS erişimi, kullanıcının yerini saldırgana bildiren bir kötücül yazılım anlamına gelebildiğinden istenen donanım kombinasyonları, uygulamanın zararlı olduğuna işaret edebilir. Bu nedenle donanım bileşenleri, statik bir öznitelik olarak toplanabilir.

D. Statik Analizin Android'e Özgü Zorlukları

Android uygulamalarının statik analizini gerçekleştirirken, Android'in karakteristik özelliklerine bağlı olarak ortaya çıkan bir takım analiz zorlukları vardır. Bu zorluklar aşağıda sıralanmaktadır.

1) Program Giriş Noktası: Android uygulamaların, tek bir giriş noktası yerine çalışma zamanında Android çerçevesiyle dolaylı olarak çağrılan birkaç giriş noktası bulunduğundan bir statik analiz aracı için uygulamaların geniş çaplı bir çağrı diyagramını oluşturmak uğraştırıcıdır. Bunun yerine, analiz aracı öncelikle tüm giriş noktalarını aramalı ve bu diyagramların birbirine nasıl bağlanıp bağlanmadıklarına dair güvencesiz bir şekilde birkaç çağrı diyagramı oluşturmalıdır.

2) Dalvik Bytecode: Android uygulamaları Java ile geliştirilip bir Dalvik sanal makinesinde yürütüldükleri için uygulamaların Java kaynak kodlarını elde etmek her zaman kolay

olmayabilir. Uygulama paketleri(apk'lar) Dalvik bayt kodlu marketlere dağıtılır ve çok az bir kısmı açık kaynak depolarında da kaynak koduyla birlikte dağıtılır. Bu nedenle, Android için bir statik analizör, Dalvik bayt koduyla doğrudan baş edebilme veya en azından desteklenen bir formata dönüştürebilme yeteneğine sahip olmalıdır. Ancak, geliştirilen çoğu Java bayt kodu analiz araçları Android ekosisteminde kullanışsızdır[12].

3) Bileşen Yaşam Döngüsü: Android'de, bir uygulamanın farklı bileşenleri, kendi yaşam döngüsüne sahiptir. Her bileşen, ortam gereksinimlerini takip eden bileşenleri başlatmak, durdurmak ve devam ettirmek için Android sistemi tarafından çağrılan kendi yaşam döngüsü metotlarını uygular. Örneğin, arka planda bir uygulama, öncelikle sistem bellek baskısı altında olduğunda durdurabilir ve daha sonra kullanıcı onu ön plana koymaya çalıştığında yeniden başlatılabilir. Maalesef, bu yaşam döngüsü metotları doğrudan yürütme akışına bağlı olmadığından bazı analiz senaryolarının doğruluğunu engellemektedirler.

4) Bileşenler Arası İletişim (ICC): Android'de, bir uygulamanın bileşenleri, kendi bileşenleri veya başka uygulama bileşenleri arasında iletişim gerçekleştirebilmektedir. Bu iletişim genellikle aşağıda ICC metotları olarak adlandırılan özel metotlarla tetiklenmektedir. ICC metotları, hedef bileşenlerini ve istenen eylemlerini belirtmek için gerekli tüm bilgileri içeren özel bir parametre kullanır. ICC metotları, sistem tarafından işlenir. Bu nedenle, statik analizörünün, gelişmiş sezgisel yöntemleri kullanmadıkça, bileşenlerin birbirine nasıl bağlandığına ilişkin varsayımda bulunması riskli olur. Dolayısıyla, çoğu statik analizör, analizinde ICC'leri hesaba katmada başarısız olmaktadır.

5) Kütüphaneler: Android'de kütüphaneler, gerçek uygulamanın boyutunun mevcut kütüphanelerden çok daha küçük olmasına yol açan binlerce satırlık kodları içerebilir. Bu durum iki önemli zorluğa neden olur: (1) kütüphane kodunu incelemek için gerçek koddan daha fazla zaman harcayabilir; (2) analiz sonuçları, kütüphanenin "ölü kod" analizi nedeniyle çok fazla yanlış pozitif içerebilir. Örnek olarak, gereken izinler kümesini keşfetmek için tüm metot çağrılarını analiz etmek, gerçek uygulama kodu için aslında gerekli olmayan izinleri listelemeye yol açabilir.

6) Java-Kalıtımsal Zorluklar: Android uygulamaları çoğunlukla Java ile yazıldığından, Java programlarının karşılaştığı bazı zorluklar bu uygulamalar için de geçerlidir. Android uygulamalarının karşılaştığı bu zorluklar aşağıda açıklanmaktadır.

a) Çoklu iş parçacıkları(Multi-threading): Çoklu iş parçacıklı programların analizi, iş parçacıkları arasındaki etkileşimlerin etkisini karakterize etmek için karmaşık olduğundan zorlayıcıdır. Ayrıca, paralel iş parçacıklarından gelen tüm ifadelerin dağıtımını (interleaving) analiz etmek genellikle üstel analiz zamanlarına neden olur.

b) Yansıma(Reflection): Dinamik kod yükleme ve yansıtıcı çağrılar söz konusu olduğunda, mevcut durumda statik olarak bunları ele almak zordur. Çalışma zamanında yüklenen sınıfların sıklıkla uzak lokasyonlarda bulunması veya çalışma sırasında oluşturulabilmeleri nedeniyle genellikle pratik olarak analiz edilmeleri imkansızdır.

c) Yerel Kod(Native Code): Yerel kod konusunun ele alınması, farklı bir araştırma serüvenidir. Çoğu zaman, bu tür kodlar, analiz etmeyi zorlaştıran derlenmiş ikili(binary) bir formatta gelir.

d) Polimorfizm(Polymorphism): Son olarak, polimorfik öznitelikler de statik analiz için ekstra zorluklar katar. Örnek olarak, A sınıfındaki m metodunun B sınıfında override edildiğini varsayalım. A sınıfına ait a nesnesinin a.m1() metodu için, a B'den oluşturulsa bile (yani, A a=new B()) , B'deki m1()'in gerçek kod bloğu yerine A'daki m1()'in kodunu ele alacaktır. Ancak bu açık durum, çoğu statik analizör tarafından pratikte çözülmede sıkıntılı bir hal almaktadır ve bu nedenle hatalı sonuçlara yol açmaktadır.

E. Kod Gösterimleri ve Destek Araçları

1) Ara Gösterimler: Ara temsil, geleneksel olarak ara derleyici aşamaları sırasında bulunan kodun iç gösterimidir.

a) SMALI Kodu: Smali, assembler için İzlandaca terimdir. Smali bu nedenle bir Android assembly dilidir(derlemesidir). Baksmali ise disassembler(geri derleme) için İzlanda terimidir. Kod dönüşümlerinin yönüne bağlı olarak Dalvik dex formatına yukarı veya aşağı doğru dönüşüm yapmak için Smali veya Baksmali kullanılır.

b) Analiz için Watson Kütüphaneleri (WALA): IBM'in T.J. Watson Araştırma Merkezi, bir Java program analizi kitaplığı olan WALA'in orijinal geliştiricisidir. Tipik WALA istemcisi, kütüphaneleri prosedürler arası analiz yapmak için kullanır. Kod, geleneksel olarak, bir sınıf hiyerarşisi oluşturarak, çağrı diyagramı oluşturarak ve kontrol akışı düğümleri diyagramı oluşturarak analiz edilir. WALA IR, Statik Tek Atama (SSA) formundaki komutların değiştirilemez bir kontrol akış diyagramıdır.

c) Soot: R. Vallee-Rai ve ark.[27] tarafından 1999'da yapılan bir çalışmada Soot, "Bir Java Bayt Kodu Optimizasyon Çerçevesi" olarak tanıtılmıştır. Soot, Java bayt kodunu analiz etmek ve dönüştürmek için dört ara gösterim sunar: Baf, Jimple, Shimple ve Grimp. Baf, bayt kodunu basit bir şekilde işlemek için elverişli bir gösterimdir. Jimple, optimizasyon için uygun 3-adres tipli bir ara gösterimdir. Shimple, Jimple'ın SSA varyasyonudur. Grimp, kaynak koda dönüştürme ve kod denetimi için uygun Jimple'ın toplu bir versiyonudur. Soot, tek başına bir araç olduğu gibi Java bayt kodu üzerinde iyileştirmeler veya dönüşümler geliştirmek için bir çerçeve olarak da kullanılabilir [16].

Tablo I, literatürdeki yaklaşımların analizlerini desteklemek için kullandıkları yinelenen araçları sıralamaktadır. Bu tür tool'lar genellikle ortak analiz süreçlerini uygulayan (örneğin, bayt kodu formları arasında dönüştürme yapmak için ya da çağrı diyagramlarının otomatik olarak oluşturulması için) standart bileşenler olarak gelmektedir.

Tablo I aynı zamanda, ilgilendiği ara gösterim (IR) ile ilgili her bir tool bilgisini de sağlamaktadır. Android Dalvik'in kendisinin manipüle edilmesi zor ve karmaşık olduğu bilindiğinden

IR, orijinal Dalvik bayt kodunu temsil etmek ve işlemi kolaylaştırmak için basitleştirilmiş bir kod formatıdır[12].

TABLO I. ANDROİD UYGULAMALARININ STATİK ANALİZİ İÇİN TEKRARLAYAN DESTEK ARAÇLARININ LİSTESİ [12].

ARAÇ	KISA AÇIKLAMA	ARA GÖSTERİM (Intermediate Representation)
Soot[28]	Java/Android statik analiz ve optimizasyon çerçevesi	Jimple, Jasmin
WALA[a]	Java/Javascript statik analiz çerçevesi	WALA-IR(SSA-tabanlı)
Chord[29]	Java program analizi platformu	Chord-IR(SSA-tabanlı)
Androguard[30,31]	Tersine mühendislik, iyicil/kötücül Android uygulama analizi	Androguard-IR
Ded[32]	DEX'i Java bayt koduna çevirici	Class
Dare[33]	DEX'i Java baytkoduna çevirici	Class
Dexpler[34]	DEX'i Java Jimple'a çevirici	Jimple
Smali/Baksmali[b]	DEX'i Smali'ye çevirici	Smali
Apktool[c]	Android uygulamalar için tersine mühendislik aracı	Smali
dex2jar[d]	DEX'i Java baytkoduna çevirici	Class
dedexer[e]	DEX dosyaları için bir tersine çevirici	DEX-assembler
dexdump	DEX dosyaları için bir tersine çevirici	DEX-assembler
dx	Java bayt kodunu DEX'e çevirici	DEX-assembler
jd-gui[f]	Java bayt kodunu kaynak koduna dönüştürücü(aynı zamanda bir IDE)	Java
ASM[35,36]	Bir java manipülasyon ve analiz çerçevesi	Class
BCEL[g]	Java bayt kodu analizi ve enstrümantasyonu için bir kütüphane	Class
Redexer	Android uygulamalarının ikili dosyalarını işleyen bir tersine mühendislik aracı	DEX-assembler

[a] http://wala.sourceforge.net

[b] http://baksmali.com

[c] http://ibotpeaches.github.io/Apktool/

[d] https://github.com/pxb1988/dex2jar

[e] http://dedexer.sourceforge.net

[f] https://github.com/java-decompiler/jd-gui

[g] https://commons.apache.org/bcel/

III. LİTERATÜRDEKİ ÇALIŞMALAR

Android ekosisteminde kötücül yazılımların ortaya çıkmasıyla, araştırmacılar, Android kötücül yazılımı izin bilgisi, kaynak koduna çevrilmiş kodlar ve diğer kaynaklar gibi statik kaynaklara dayalı olarak tespit etmek için bir takım sistemleri önermişlerdir. Bu bölümde, literatürde yer alan son 3 yıla ait (2015-2017) bazı statik analiz çalışmaları incelenmiştir.

Yerima ve ark.[17] tarafından 2015'de yapılan bir çalışmada, Android kötücül yazılım tespitinde doğruluk oranını iyileştirmek için statik analizin avantajları, kolektif makine öğrenmesinin etkinliği ve performansı ile birleştirilmektedir. Önerilen yöntem bu alanda geliştirilen diğer yöntemlerden daha etkin bir şekilde çalışarak çok düşük bir yanlış pozitif oranıyla yüksek doğrulukta kötücül yazılımların tespitini gerçekleştirmektedir. Çalışma aynı zamanda, yeni nesil malware tespit, güvenlik ve analiz çözümleri geliştiren araştırmacılar ve uygulayıcılar için de bir rehber niteliğindedir.

Du ve ark.[19] tarafından 2015'de yapılan bir çalışmada ise geleneksel statik öznitelikleri, kontrol akış çizelgesini ve yeniden paketleme özelliklerini kullanarak çoklu kaynağa dayalı bit kötücül yazılım tespiti mekanizması sunulmaktadır. Bu mekanizmanın diğerlerinden farkı, her bir öznitelik kategorisinin öznitelik çıkarımında ve sınıflandırmada bağımsız bir bilgi kaynağı olarak düşünülmesidir.

Kabakus ve ark.[26] tarafından 2015'de yapılan bir çalışmada da, statik analiz kullanılarak, izin tabanlı bir Android kötü amaçlı yazılım tespit sistemi, APK Denetçisi sunulmaktadır. APK Denetçisi üç bileşenden oluşmaktadır. Uygulamalar ve analiz sonuçları hakkında çıkarılan bilgileri saklamak için bir imza veritabanı, son kullanıcılar tarafından uygulama analizi istekleri vermek için kullanılan bir Android istemcisi ve hem imza veritabanı hem de akıllı telefon istemcisiyle iletişim kurmaktan ve bütün analiz sürecini yönetmekten sorumlu merkezi bir sunucu. Sonuçlar, APK Denetçisinin en tanınmış kötücül yazılımları tespit edebildiğini ve yüksek doğruluk oranları elde ettiğini göstermektedir.

Fereidooni ve ark.[23] tarafından 2016'da yapılan bir çalışmada ise yüksek performanslı tespit ve kabul edilebilir bir false pozitif oranıyla Makine Öğrenmesine dayalı bir tespit modeli sunulmuştur. Çalışmanın önemi, Android cihazlar için sağlam, etkili ve verimli öznitelikleri kullanan hafif bir kötücül yazılım tespit sistemi geliştirmektir. Çalışmada ayrıca, güvenilir, büyük ölçekli ve güncellenmiş bir kötücül yazılım veri seti kullanılmıştır.

Yang ve ark.[25] tarafından 2016'da yapılan bir çalışmada, farklı kaynak ve seviyelerden öznitelikler elde ederek yoğun bir öznitelik çıkarımıyla Android uygulamalarının statik analizi gerçekleştirilmiştir. Çalışmada yalnızca classes.dex yürütülebilir dosyasından yararlanılmamış aynı zamanda manifest dosyası gibi diğer kaynak dosyalarından da öznitelik çıkarımında bulunulmuş, tek seviyede daha fazla öznitelik kullanmak yerine farklı soyutlama seviyelerindeki özniteliklerin çıkarımına odaklanılmıştır. Daha sonra bu çıkarılan öznitelikler tek bir öznitelik setinde toplanarak eğitim ve test aşamalarında kullanılmıştır.

TABLO II. LİTERATÜRDEKİ SON 3 YILA AİT(2015-2017) BAZI STATİK ANALİZ ÇALIŞMALARININ KARŞILAŞTIRMASI

Ref. No	Analiz Tipi	Kullanılan Algoritma	Öznitelikler	Veri Seti	Değerlendirme Ölçütleri	Sonuçlar (%'lik)
[17]	Statik	Naïve Bayes, Simple Logistic, Decision Tree, Random Tree, Random Forest	API çağrıları, komutlar ve izinler	McAfee dahili deposundan 2925 zararlı yazılım / 3938 zararsız yazılım	TPR,TNR,FPR,FNR, AUC, ERR, ACC	97,3-99
[19]	Statik	SVM, J48, BayesNet	Hassas ve kritik API çağrıları, kontrol akış diyagramı, yeniden paketleme teknolojisi özellikleri	Android Genom Project'ten 1260 ve Google Play'den 320 zararlı yazılım/ Google Play'den 2000 ve Chinese Market'ten zararsız yazılım	False Positive Rate (FPR), True Positive Rate (TPR), Precision ,ROC Area	97
[26]	Statik	Logistic Regression	İzinler	Android Genome Project, Drebin	Doğruluk, çeşitlilik	88 doğruluk, 92.5 çeşitlilik
[23]	Statik	XGboost, Adaboost, RandomForest,SVM with RBF kernel, K-NN, Logistic Regression, Naive Bayes, Decision Tree, Deep Learning	Intent'ler, izinler, sistem komutları, şüpheli API çağrıları, kötücül aktiviteler	Genom Project, Drebin, M0Droid, VirüsTotal' den çeşitli sayılarda zararlı ve zararsız uygulamalar (Toplamda 29,864 uygulama)	Precision, recall, F1-score, ACC, TPR, FNR, FP	97.3
[25]	Statik	Random Forest	Classes.dex'ten, AndroidManifest.xml'den çeşitli öznitelikler	Android Drebin Project'ten 550 zararlı yazılım/ Baidu Apps Market'ten 550 zararsız yazılım	False Positive Rate (FPR), True Positive Rate (TPR), Precision ,ROC Area	98.1'e kadar çeşitli doğruluk sonuçları
[21]	Statik	Random Forest, Nearest Neighbors, Decision Tree, AdaBoost, Bagging, Naive Bayes	Meta-Data	Aptoid uygulama mağazasından 2426 zararlı yazılım/ 6704 zararsız yazılım	False Positive Rate (FPR), True Positive Rate(TPR),ACC,ROC Area	93.67
[20]	Statik ve Dinamik	DApriori	Kötücül Yazılım Davranışı	Androguard ve Contagio Mobile' dan 12 uygulama	Precision, Recall	Sınırlı veri seti nedeniyle verilmemiş
[24]	Statik ve Dinamik	Deep-First	Kötücül Yazılım Davranışı	Android Genome Project	-	-
[22]	Statik	SVM, Naive Bayes, C4.5 Decision Tree, JRIP, AdaBoost	İzinler, import ifadeleri , metot çağrıları, fonksiyon argümanları ve açıklamalar	M0Droid veri setinden 200 zararlı yazılım/ 200 zararsız yazılım	Precision, Recall, F-score	95' kadar çeşitli doğruluk sonuçları
[18]	Statik ve Dinamik	Edit Uzaklığı	Intent çağrıları, Sistem çağrıları, binder çağrıları	Android Malware Genome Project, DroidAnalytics örnekleri ve contagio minidump forumlarından 3723 zararlı yazılım / Google Play'den en üst sıradaki 500 zararsız yazılım	True Positive Rate (TPR)	99

Calleja ve ark. [21] tarafından 2016'da yapılan bir çalışmada, uygulama mağazası web sitesinde ve Android

Manifest'te bulunan meta bilgileri kullanan yeni bir yöntem önerilmektedir. Bu yöntemin temel amacı uygulamaları yüklemeye gerek duymadan cihazların enfekte olmalarını önlemek amacıyla hızlı ve aynı zamanda yüksek doğrulukta tespit sağlayan bir araç geliştirmektir. Yöntem, meta verilerden önemli bilgileri elde etmek için bir metin madenciliği işlemine dayanmakta ve bu verimli ve doğru sınıflandırıcılar oluşturmak için kullanılmaktadır.

Yang ve ark.[20] tarafından 2016'da yapılan bir çalışmada, statik bir madencilik algoritması ile dinamik bir taint analizini içermektedir ve bu çalışma gerçek dünya mobil uygulamalarında test edilmiştir. Önerilen yaklaşımın ilk aşamasında statik analizle Android API'lerine ve mevcut saldırı modellerine dayalı kritik saldırı yolu tanımlanmakta, daha sonra ise mevcut saldırı modelleriyle uyumluluğu kontrol edilerek saldırı olasılığını tespit etmek amacıyla programı sınırlı ve odaklanmış bir kapsamda yürütmek için belirlenen yönlendirilmiş yolu takip etmektedir.

Lin ve ark.[24] tarafından 2016'da yapılan bir çalışmada, yine statik ve dinamik yaklaşımlar birleştirilerek, Android uygulamalarının güvenlik değerlendirmesini destekleyen, gizlenmiş URL'ler gibi gizli bilgilerini otomatik olarak çıkarmak amacıyla Android uygulamalar için zorla yürütme tekniği(forced execution teqnique) önerilmektedir. Yaklaşım, öncelikle statik analize dayalı olarak kritik işlevlere öncülük eden yürütme yollarını araştırmaktadır. Ardından, hedef uygulamanın kontrol akış koşulları izlenerek seçilen yollardaki kod zorla çalıştırılmaktadır. Bu işlemde seçilen yürütme akışlarının kritik fonksiyonlara ulaşmasını sağlamak için bir hata tolereli yürütme sanal alanı tasarlanmıştır. Bu nedenle, fonksiyonlarla ilgili önemli parametreler yüksek olasılıkla çıkarılabilmektedir. Yaklaşımın en büyük avantajı, tüm işlemin tamamen otomatik olması ve yürütülmesi için karmaşık girdi bağlamları gerektirmemesidir.

Milosevica ve ark. [22] tarafından 2017'de yapılan bir çalışmada, Android kötücül yazılımların statik olarak tespitinde makine öğrenmesine dayalı iki yaklaşım sunulmaktadır. İlk yaklaşım izne dayalı olup ikincisi bag-of-words(kelime torbası) gösterim modelini kullanan bir kaynak kodu analizine dayanmaktadır. İzne dayalı modelin hesaplama maliyeti düşük olup, bu izinler Google Play Store'dan edinilebilen OWASP Seraphimdroid Android uygulamasında, birer öznitelik olarak kullanılmaktadır.

Son olarak, Sun ve ark.[18] 2017'de yaptıkları bir çalışmada, kötücül yazılımların türevlerinin çekirdek fonksiyonlarının çalışma zamanı davranışlarının aslıyla benzer olduğu saptamış ve bunların tespit edilmesinde "çalışma zamanı" davranışını "statik yapılar" la birleştiren bir çerçeve önermişlerdir. Önerilen sistem "MONET", bir istemci ve bir sunucu modülünden oluşmaktadır. İstemci davranış izleme ve imza oluşturma görevini üstlenirken, sunucu büyük çaplı kötücül yazılım tespitinden sorumludur. Uygulama, bir saldırı tespit ettiğinde, saldırı ayrıntılarını kullanıcılara sunulmakta, otomatik olarak uyarıda bulunmaktadır.

Tablo 2, yukarıdaki çalışmaların; kullanılan algoritma, öznitelikler, veri seti, değerlendirme ölçütleri ve sonuçlarına göre bir karşılaştırmasını göstermektedir.

Tablo 2 incelendiğinde, 10 statik analiz çalışmasının 7' sinde makine öğrenmesine dayalı algoritmalar kullanılmıştır. Ayrıca, bazı çalışmalarda kullanılan statik analiz tekniği dinamik analizle güçlendirilmiş, çalışmaların genelinde Android izin öznitelikleri kullanılmıştır. İncelenen bu son çalışmalarda %80 'in altında tespit doğruluğuna sahip hiçbir çalışma bulunmamaktadır.

IV.SONUÇLAR VE GELECEKTEKİ ÇALIŞMA YÖNLERİ

Android uygulamalarının statik analizine ilişkin araştırmalar hızlı bir şekilde olgunlaşmakta, uygulama kodundaki güvenlik sorunlarının statik açıdan açığa çıkartılması için gittikçe daha gelişmiş yaklaşımlar üretilmektedir. En son çalışmaları özetlemek ve araştırma topluluğu tarafından ele alınması gereken zorlukları sıralamak için, Android uygulamaları üzerinde statik analiz kullanmayı içeren yaklaşımlarla ilgili ayrıntılı bir incelenme yapılmıştır.

Yapılan çalışmada, statik analizde etkili olan prototipik ve temel teknikler, ara gösterimler, kullanılan araçlar ve öznitelikler, Android platformunun yapısı ve onun benzersiz özelliklerinden kaynaklanan analiz zorlukları kapsamlı bir şekilde ele alınmış, güncel çalışmalara dair karşılaştırmalı bir analiz yapılarak bu çalışmaların yöneldiği noktalar ayrıntılı bir şekilde ele alınmıştır.

Statik analiz üzerine gerçekleştirilen bu incelemeden şu sonuçlar elde edilmiştir: (1) incelenen analizlerin çoğu, Android uygulamalarındaki güvenlik açıklarını ortaya çıkarmak için yapılmaktadır; (2) analizlerinde Android programlamanın en az bir karakteristik özelliğini göz önüne almada bütün yaklaşımlar eksiktir; (3) son olarak, araçlar ve veri setleri gibi araştırma katkı unsurları genellikle yayınlanmamıştır.

Gelecekteki çalışmalarda, Android programlamanın karakteristik özelliklerini göz önüne alan daha fazla çalışma gerçekleştirilmelidir. Hızlı son geliştirilen zararlı yazılımlara karşı tespit şansı çokça güçlendirilerek kod gizleme ve diğer anti-analiz tekniklerinin kötücül yazarlar tarafından kullanılmasına karşı dayanıklı ve esnek tespit mekanizmalarının geliştirilmesi amaçlanmalıdır. Ayrıca, tespit sonuçlarının performansını artırmak amacıyla öznitelikler elde etmek için daha iyi yöntemler benimsenmelidir.

KAYNAKLAR

[1] Worldwide Smartphone OS Market Share. [Visited May 2017] [Online]. Available: http://www.idc.com/promo/smartphone-market-share/os/.

[2] Google Play: number of available apps 2009-2017. [Visited May 2017] [Online]. Available: https://www.statista.com/statistics/ 266210/number-of-available-applications-in-the-google-play-store/.

[3] McAfee Labs Threats Report. [Visited May 2017] [Online]. Ava-

ilable: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf.

[4] Nokia Threat Intelligence Report, [Visited May 2017] [Online]. Available: http://resources.alcatel-lucent.com/asset/200492/.

[5] Trojans, Ghosts, and More Mean Bumps Ahead for Mobile and Connected Things, [Visited May 2017] [Online]. Available: https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2017.pdf.

[6] U. Nikolic, F. Spoto, "Reachability analysis of program variables," ACM Trans. Program. Lang. Syst., 35(4), 2014.

[7] F. Wei, S. Roy, X. Ou, Robby, "Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps," In Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security, CCS '14, USA, 2014.

[8] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, M. Rajarajan, Android Security: A Survey of Issues, Malware Penetration, and Defenses. IEEE Communications Surveys and Tutorials, 17(2), 2015, pp. 998-1022.

[9] S. Ramu, "Mobile Malware Evolution, Detection and Defense," EECE 571B, Term Survey Paper, 2012.

[10] M. Grace, Y. Zhou, Q. Zhang, S. Zou, X. Jiang, " RiskRanker: Scalable and Accurate Zero–Day Android Malware Detection," in: Proceedings of the 10th international conference on Mobile systems, applications, and services, MobiSys '12, ACM, New York, NY, USA, 2012, pp. 281–294.

[11] W. Zhou, Y. Zhou, X. Jiang, " Hey, You Get Off my Market: Detecting Malicious apps in Official and Third party Android Markets," in: Annual Network and Distributed Security Symposium, NDSS, New York, NY, USA, 2012.

[12] L. Li, T. Francois, D. A. Bissyande, M. Papadakis, S. Rasthofer, A. Bartel, D. Octeau, J. Klein, Y. L. Traon, " Static analysis of android apps: A systematic literature review," Technical report, SnT, 2016.

[13] A. Feizollah, N.B. Anuar, R. Salleh, A.W.A. Wahab, "A review on feature selection in mobile malware detection," Digit Invest, 13 (2015) 22-37.

[14] A. Bartel, Security Analysis of Permission-Based Systems using Static Analysis: An Application to the Android Stack. PhD thesis, University of Luxembourg, 2014.

[15] M. Backes, S. Gerling, C. Hammer, M. Maffei, P. v. Styp-Rekowsky, "Appguard: enforcing user requirements on android apps," in: 19th international conference on Tools and Algorithms for the Construction and Analysis of Systems, pp. 543-548.

[16] A collection of mobile security resources. [Visited May 2017] [Online]. Available: http://wiki.secmobi.com/tools/.

[17] S. Y. Yerima, S. Sezer, I. Muttik, "High accuracy android malware detection using ensemble learning," IET Information Security, 2015.

[18] M. Sun, X. Li, J. C. S. Lui, R. T. B. Ma, Z. Liang, "Monet: A User-oriented Behavior-based Malware Variants Detection System for Android," IEEE Transactions on Information Forensics and Security, Volume: 12, Issue: 5 (2017).

[19] Y. Du, X. Wang, J. Wang, "A static Android malicious code detection method based on multi- source fusion," Security And Communicatıon Networks, 2015.

[20] T. Yang, K. Qian, L. Li, D. Lo, L. Tao, "Static Mining and Dynamic Taint for Mobile Security Threats Analysis," IEEE International Conference on Smart Cloud, 2016.

[21] A. Martín, A. Calleja, H. D. Menéndez, J.Tapiador, D. Camacho, "ADROIT: Android malware detection using meta-information," IEEE Symposium Series on Computational Intelligence (SSCI), 2016.

[22] N. Milosevica, A. Dehghantanhab, K. R. Choo, "Machine learning aided Android malware classification," Computers & Electrical Engineering, 2017.

[23] H. Fereidooni, M. Conti, D. Yao, A. Sperduti, "ANASTASIA: ANdroid mAlware detection using STAtic analySIs of Applications," 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

[24] Z. Lin, R. Wang, X. Jia, J. Yang, D. Zhang, C. Wu, "ForceDROID:Extracting Hidden Information in Android Apps by Forced Execution Technique," IEEE Trustcom/ BigDataSE/ISPA, 2016.

[25] M. Yang, Q.Y. Wen, "Detecting Android Malware with Intensive Feature Engineering," 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2016.

[26] A.T. Kabakus, I.A. Dogru, C. Aydın, "APK Auditor: Permission-based Android malware detection system," Digital Investigation, 2015, 13, pp 1-14.

[27] R. Vallee-Rai, P. Co, E. Gagnon, L. Hendren, P. Lam, and V. Sundaresan, "Soot - a java bytecode optimization framework," In Proc. of the 1999 Conf. of the Centre for Advanced Studies on Collaborative Research, CASCON '99, IBM Press, 1999.

[28] P. Lam, E. Bodden, O. Lhot´ak, and Laurie Hendren, "The soot framework for java program analysis: a retrospective," In Cetus Users and Compiler Infastructure Workshop (CETUS 2011), 2011.

[29] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for Internet applications,".

[30] Anthony Desnos and Geoffroy Gueguen. Android: From reversing to decompilation. Proc. of Black Hat Abu Dhabi, pages 77–101, 2011.

[31] A. Desnos, "Android: Static analysis using similarity distance," In System Science (HICSS), 2012 45th Hawaii International Conference on, pages 5394-5403, IEEE, 2012.

[32] D. Octeau, W. Enck, and P. McDaniel, "The ded decompiler," Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, Tech. Rep. NAS-TR-0140-2010, 2010.

[33] D. Octeau, S. Jha, and P. McDaniel, "Retargeting android applications to java bytecode," In Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering, page 6, ACM, 2012.

[34] A. Bartel, J. Klein, M. Monperrus, and Y. L. Traon,"Dexpler: Converting Android Dalvik Bytecode to Jimple for Static Analysis with Soot," In ACM Sigplan International Workshop on the State Of The Art in Java Program Analysis, 2012.

[35] E. Bruneton, R. Lenglet, and T. Coupaye, "Asm: a code manipulation tool to implement adaptable systems," Adaptable and extensible component systems, 30, 2002.

[36] E. Kuleshov, "Using the asm framework to implement common java bytecode transformation patterns," Aspect-Oriented Software Development, 2007.

ISC TURKEY 2017

BİLGİGÜVENLİĞİ DERNEĞİ

Maltepe Mahallesi Tuncer Sokak
No: 2/8 06570 Çankaya-ANKARA
0 (312) 231 18 10
bilgi@bilgiguvenligi.org.tr