



BİLGİ GÜVENLİĞİ
DERNEĞİ

www.bilgiguvenligi.org.tr

20-21

September/Eylül

2013



PROGRAM

ISCTurkey 2013 PROGRAM

1.GÜN/FIRST DAY

20 EYLÜL/SEPTEMBER 2013 CUMA/FRIDAY

09:00-10:00

KAYIT/REGISTRATION

09:30-10:00

ÇAY-KAHVE ARASI/TEA/COFFEE BREAK

10:00-10:30

AÇILIŞ VE PROTOKOL KONUŞMALARI/OPENING
CEREMONY ANA SALON/
MAIN HALL - KEMAL KURDAŞ

Sn. Ahmet Hamdi ATALAY

Bilgi Güvenliği Derneği Başkanı

Sn. Prof. Dr. Ahmet ACAR

ODTÜ Rektörü

Sn. Prof. Dr. Süleyman BÜYÜKBERBER

Gazi Üniversitesi Rektörü

Sn. Dr. Tayfun ACARER

BTK Başkanı

Sn. Prof. Dr. Yücel ALTUNBAŞAK

TÜBİTAK Başkanı (*)

Sn. Binali YILDIRIM

UDH Bakanı

10:30-12:30

PANEL 1

ANA SALON/MAIN HALL - KEMAL KURDAŞ
TÜRKİYE’NİN SİBER GÜVENLİK STRATEJİ BELGESİ
VE EYLEM PLANI/ CYBER SECURITY STRATEGY
DOCUMENT AND ACTION PLAN OF TURKEY

Moderatör/Moderator - Prof. Dr. Şeref SAĞIROĞLU BGD

Dr. Hayrettdin BAHŞİ

TÜBİTAK, Siber Güvenlik Enstitü Müdürü

Gündüz ŞENGÜL

UDHB Daire Başkanı

K. Sacid SARIKAYA

BTK Daire Başkanı

Prof. Dr. Kemal CILIZ

TÜBİSAD Başkanı

Adil Zafer MÜFTÜOĞLU

TÜTED Başkanı

Ali YAZICI - ASELSAN

BGD

12:30-13:30

ÖĞLE ARASI/LUNCH BREAK

13:30-15:30

PANEL 2

ANA SALON/MAIN HALL - KEMAL KURDAŞ
BULUT BİLİŞİM GÜVENLİĞİ/CLOUD COMPUTING
SECURITY

Moderatör/Moderator: Prof. Dr. Turhan MENTEŞ, TBD

Ş. Selçuk ŞAHİN

Bünyamin KARADENİZ

F. Mehmet BOYACIOĞLU

Ömer KÖKER

Cem AKOYMAK

Necmi ÖN

TÜRKSAT

HAVELSAN

TURKCELL

VODAFONE

AVEA

NETAŞ

15:30-16:00 ÇAY-KAHVE ARASI/TEA/COFFEE BREAK

16:00-17:45

PANEL 3

ANA SALON/MAIN HALL - KEMAL KURDAŞ

SOSYAL MEDYA/SOCIAL MEDIA

Moderatör/Moderator: Prof. Dr. Nafize BAYKAL, ODTÜ

Osman Nihat ŞEN

Serhat ÖZEREN

Cabir BİLİRGİN

Doç. Dr. Ferah ONAT

BTK TİB Başkan V.

UDHB İnternet Gel. Kur. Başkanı

UDHB Bakan Danışmanı

Yaşar Üniversitesi

16:00-18:00

OTURUM 1/SESSION 1

SALON A/HALL A

BULUT BİLİŞİM/CLOUD COMPUTING

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Prof. Dr. Ersan AKYILDIZ

Prof. Dr. Hayri SEVER

A Decision Framework for Combat Cloud Computing Strategy

Kerim Göztepe, Kara Harp Akademisi; İsmet Çehreli, Kara Harp Akademisi; S. Eyüp Şensoy, Kara Harp Akademisi

Halk ve Özel Bulut Yapılarında Karşılaştırmalı Performans Ölçümleri

Hakan Aydın, Başkent Üniversitesi; Oumout Chouseinoglou, Başkent Üniversitesi

Attack Types and Intrusion Detection Systems in Cloud Computing

Ucman Oktay, Hava Harp Okulu; Özgür Koray Şahingöz, Hava Harp Okulu

Mobile Cloud Authentication and Secure Communication

Redi Gokaj, İstanbul Üniversitesi; M. Ali Aydın, İstanbul Üniversitesi; R. Selami Özbey, TÜBİTAK BİLGEM

Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukukî Sorunlar

M. Mürsel Başgöl, Başkent Üniversitesi; Oumout Chouseinoglou, Başkent Üniversitesi

16:00-18:00

OTURUM 2/SESSION 2

SALON B/HALL B

SİBER GÜVENLİK/CYBER SECURITY

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Prof. Dr. Mustafa ALKAN

Dr. Mehmet Sabir KİRAZ

A Data Security System Design for Hybrid (Cloud & Volunteer) Global Computing

Emrah Dönmez, İstanbul Teknik Üniversitesi; Akif Kutlu,
Süleyman Demirel Üniversitesi

DNS Güçlendirme Saldırısı Risk Analizi

Devrim Seral, Uluslararası Kıbrıs Üniversitesi

Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Üçlü Boyut Yaklaşımı

İnan Semiz, Kara Harp Akademisi; Kerim Göztepe, Kara Harp Akademisi; Recep Kılıç, Kara Harp Akademisi

BOME'lerin Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Kullanımının Etkinleştirilmesi

Melih Durak, Kara Harp Akademisi; İnan Semiz, Kara Harp Akademisi; Selçuk Sönmez, Kara Harp Akademisi

Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala (Capture The Flag)

Osman Akın, Hacettepe Üniversitesi; Işıl Çınar, Gazi Üniversitesi; Muhammed Kahraman, Siber GÜv. Uzmanı; Fatih Bilekyiğit, Siber GÜv. Uzmanı

16:00-18:00

OTURUM 3 /SESSION 3

SALON C /HALL C

BİLGİ GÜVENLİĞİ/INFORMATION SECURITY

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Yrd. Doç. Dr. Sedat AKLEYLEK

Dr. Hamdi Murat YILDIRIM

24 Bit Renkli Dokümanların Farklı Biyometri Teknoloji Kullanılarak Güvenliğinin Sağlanması

Mehmet Kıvılcım Keleş, İstanbul Aydın Üniversitesi; Ali Güneş, İstanbul Aydın Üniversitesi

Genetik Algoritma ve Tekil Değer Ayrışımı Tabanlı Yeni Bir Kırılgan Resim Damgalama

Veysel Aslantaş, Erciyes Üniversitesi; Mevlüt Doğru, Milli Emlak Genel Müdürlüğü

Güvenli ve Kişisel Aşı Bilgi Sistemi

Okan Bursa, Ege Üniversitesi; Emine Sezer, Ege Üniversitesi; Özgü Can, Ege Üniversitesi; Murat Osman Ünalır, Ege Üniversitesi

A Hypergame Model for Information Security

Yadigar Imamverdiyev, Institute of Information Technology of Azerbaijan National Academy of Sciences

16:00-18:00

OTURUM 4/SESSION 4
SALON D/HALL D
SİBER GÜVENLİK/CYBER SECURITY

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Doç. Dr. Ali Doğan AKSOY

Yrd. Doç. Dr. Kerim GÖZTEPE

Siber Güvenliğin Taarruzi Boyutu ve Uluslararası Hukuk Kurallarının Uygulanabilirliği

Hakan Şentürk, Kara Harp Okulu; C. Zaim Çil, Çankaya Üniversitesi; Şeref Sağıroğlu, Gazi Üniversitesi

A Novel Concept for Cybersecurity: Institutional Cybersecurity

İbrahim Şişaneci, Gebze Yüksek Teknoloji Enst.; Osman Akın, Hacettepe Üniversitesi ;
Muammer Kahraman, Siber GÜv. Uzmanı; Mehmet Sağlam, VirginiaTech

Data and Endpoint Security in Mobile Computing

Sait Murat Giray, ODTÜ

Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri

Seda YILMAZ, Gazi Üniversitesi; Şeref Sağıroğlu, Gazi Üniversitesi

Kurumsal Elektronik Posta İletiminde Siber Güvenlik

Dr. Önder Şahinaslan, Maltepe Üniversitesi; Dr. Ender Şahinaslan, Bank Asya

16:00-18:00

OTURUM 5/SESSION 5
SALON E/HALL E
**BİLGİ ve BİLGİSAYAR GÜVENLİĞİ/INFORMATION
AND COMPUTER SECURITY**

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Prof. Dr. Ali YAZICI

Doç. Dr. Cüneyt BAZLAMAÇCI

Secure Database in Cloud Computing: CryptDB Revisited

Ziynet Nesibe Dayıoğlu, TÜBİTAK, BİLGEM; Mehmet Sabir Kiraz,
TÜBİTAK BİLGEM; Fatih Birinci, TÜBİTAK BİLGEM; İhsan Haluk Akın, Fatih Üniversitesi

Donanımsal Truva Atı Tespiti Etkinlik Analizi

Muhammet Şahinoğlu, TÜBİTAK BİLGEM; Muhammet Öztemür, TÜBİTAK BİLGEM;
Betül Soysal, TÜBİTAK BİLGEM

ICT Usage Characteristics and Web Security

Atıla Bostan, Atılım Üniversitesi; İbrahim Akman, Atılım Üniversitesi

Virmon: A Virtualization-Based Automated Dynamic Malware Analysis System

Hüseyin Tirli, TÜBİTAK BİLGEM; Abdurrahman Pektaş, TÜBİTAK BİLGEM; Yliés Falcone,
University of Grenoble; Nadia Erdoğan, İstanbul Teknik Üniversitesi

Zararlı Yazılım Tespit, Takip ve Analiz Yöntemleri Geliştirilmesi

Mustafa Alkan, Gazi Üniversitesi; Burak Çifter BOA Bilgi Teknolojileri ve Güvenliği; Elif Tuba Kılıç, Kara Kuvvetleri MEBS Okulu ve Eğitim Merkezi Komutanlığı

2.GÜN/SECOND DAY

21 EYLÜL/SEPTEMBER 2013 CUMARTESİ/SATURDAY

09:00-09:30

ÇAY-KAHVE ARASI/TEA-COFFEE BREAK

09:30-12:30

EĞİTİM/TUTORIAL

ANA SALON/MAIN HALL: KEMAL KURDAŞ

SİBER GÜVENLİK EĞİTİMİ/CYBER SECURITY
TRAINING COURSE

Koordinator/Coordinator: Uraz YAVANOĞLU, Gazi Üniversitesi

Eğitim Programı/Training Course Programme

09:00-09:20

Siber Güvenlik ve Savunma

Konuşmacı:

Uraz YAVANOĞLU, Gazi Üniversitesi

09:20-09:40

Bilgi Güvenliği ve Kriptoloji Uygulamaları

Konuşmacı:

Yrd. Doç. Dr. Sedat AKLEYLEK,
Ondokuz Mayıs Üniversitesi

09:40-09:50

Konuşmacılar:

Bilgi Güvenliği

Anıl UTKU, BGD

Burak ÖZÇAKMAK, BGD Genç Başkanı

09:50-10:10

Konuşmacı:

Güvenli Yazılım Geliştirme

Özgür YÜREKTEN, BGD

10:10-10:30

Konuşmacı:

Casus ve Kötücül Yazılım

Adem TEKEREK, BGD

10:30-10:50

Konuşmacı:

Adli Bilişim

Mehmet KARAMAN, GUTIC

10:50-11:10

Konuşmacılar:

Sosyal Ağlarda Adli Takip

Sedef GÜNDÜZ, GUTIC

Büşra ÇAĞLAR, BGD-Genç

Semra ÇAKIR, BGD-Genç

11:10-11:30
Konuşmacı:

Bulut ve Web Güvenliği
Duygu SİNANÇ, GUTIC

11:30-11:50
Konuşmacı:

Mobil Güvenlik
Eyüp Burak CEYHAN, GUTIC

11:50-12:10
Konuşmacılar:

Endüstriyel Güvenlik
Dr. Alper ÖZBİLEN, BGD
Hacer ATLI, BGD-Genç
Gizem TANIŞ, BGD-Genç

12:10-12:20
Konuşmacı:

Bilgi Güvenliği Standardı
Medine ÇOLAK, GUTIC

12:20-12:30

Soru-Cevap

12:30

Sertifika Dağıtım Töreni

10:00-12:00

OTURUM 6/SESSION 6
SALON A/HALL A
AÇIK ANAHTARLI ŞİFRELEME VE PROTOKOLLERİ
PUBLIC KEY CRYPTOGRAPHY AND PROTOCOLS

OTURUMBAŞKANLARI/SESSION CHAIRMEN

Doç. Dr. Hasan Ş. BİLGE

Y. Doç. Dr. Ömer KÜÇÜKSAKALLI

Storage Free Basis Conversion over Composite Finite Fields of odd Characteristics

Riaz Sial, ODTÜ; Ersan Akyıldız, ODTÜ

Recent Attacks against HFE/Multi-HFE MQ Cryptosystems and Connection with Ore's p-Polynomial Decomposition

Bilal Alam, ODTÜ; Oğuz Yayla, ODTÜ

Test Suite Study for Security Analysis of Digital Signature Applications

Tamer Ergun, TÜBİTAK; Ferruh Özbudak, ODTÜ; Ferda Topcan, TÜBİTAK

RSA Kriptosistemi Parametreleri için Güvenlik Testi Yazılımı

Ersan Akyıldız, ODTÜ; Çağdaş Çalık, ODTÜ; Mert Özarar, TÜRKTRUST Bilgi, İletişim ve Bilgi Güvenliği Hizmetleri A.Ş.; Zaliha Tok, ODTÜ; Oğuz Yayla, ODTÜ

A Secure Internet Voting Protocol Based On Homomorphic Encryption

Ahmet Sinak, ODTÜ; Mehmet Sabir Kiraz, TÜBİTAK BİLGEM; Seçil Özkan, ODTÜ; Hakan Yıldırım, ODTÜ

10:00-12:00

OTURUM 7/SESSION 7

SALON B/HALL B

BİLGİ ve BİLGİSAYAR GÜVENLİĞİ/INFORMATION
AND COMPUTER SECURITY

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Doç. Dr. Ali Aydın SELÇUK

Dr. Orhun KARA

Kamu Kurumlarında Elektronik İmza Hakkında Karşılaştırmalı Bir Çalışma

Çiğdem Selçukcan Erol, İstanbul Üniversitesi; Fatma Önay Koçoğlu, İstanbul Üniversitesi; Zeki Özen, İstanbul Üniversitesi; Elif Kartal, İstanbul Üniversitesi

Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler

Uğur Akyazı, Hava Kuvvetleri Komutanlığı

Yazılım Güvenliği Üzerine Bir İnceleme

Seda Yılmaz, Gazi Üniversitesi; Şeref Sağıroğlu, Gazi Üniversitesi

Solution of a Conjecture: On 2-PCD RFID Distance Bounding Protocols

Eren Kocaağa, İstanbul Teknik Üniversitesi; Bünyamin Tanıl, İstanbul Teknik Üniversitesi; Muhammed Ali Bingöl, TÜBİTAK BİLGEM; Süleyman Kardaş, TÜBİTAK BİLGEM

Yazılım Güvenlik Açıklıklarının Analizi ile Olası Zafiyet Öngörüsü

Oğuz Bozoklu, Kara Harp Okulu; Celal Zaim Çil, Çankaya Üniversitesi; Şeref Sağıroğlu, Gazi Üniversitesi

10:00-12:00

OTURUM 8/SESSION 8

SALON C/HALL C

KRİPTOGRAFİ/CRYPTOGRAPHY

OTURUM BAŞKANLARI/SESSION CHAIRMEN

Yrd. Doç. Dr. Zülfikar SAYGI

Dr. Barış KIRLAR

Some Observations on Distribution of Cross Correlation of Two Nonbinary Sequences

Ernist Tilenbaev, TOBB Ekonomi ve Teknoloji Üniversitesi; Hasan Dilek, TOBB Ekonomi ve Teknoloji Üniversitesi; Zülfükar Saygı, TOBB Ekonomi ve Teknoloji Üniversitesi; Çetin Ürtiş, TOBB Ekonomi ve Teknoloji Üniversitesi

Some Results On Three-Valued Walsh Transforms from Decimations of Hellesteth-Gong Sequences

Hasan Dilek, TOBB Ekonomi ve Teknoloji Üniversitesi; Ernest Tilenbaev, TOBB Ekonomi ve Teknoloji Üniversitesi; Zülfükar Saygı, TOBB Ekonomi ve Teknoloji Üniversitesi; Çetin Ürtiş, TOBB Ekonomi ve Teknoloji Üniversitesi

Distribution of Boolean Functions of 6 Variables According to the Frequency of Walsh Coefficients

Erdener Uyan, ODTÜ; Ali Doğanaksoy, ODTÜ

Period Analysis of Pseudorandom Vector Sequences With Dynamical Polynomial Systems

Pınar Balıkçioğlu, ODTÜ; Melek D. Yücel, ODTÜ

Off-The-Record Communication with Location Hiding

Halil Kemal Taşkın, ODTÜ; Murat Demircioğlu, ODTÜ

10:00-12:00

FİRMA SUNUMU – STM

SALON D/HALL D

“Savunma Sanayiinde Proje Geliştirme Ortamlarında Tek Noktadan Farklı Güvenlik Seviyeli Etki Alanlarına Güvenli Erişim”

09:00-12:30

POSTER SUNUMLARI/ POSTER SESSION

FUAYE/FOYER

Identity Management Based Security Architecture of Cloud Computing on Multi-Agent Systems

Rasim Alguliyev, Institute of Information Technology of ANAS Farqana Abdullayeva, Institute of Information Technology of ANAS

Disaster Readiness of Hospital Information Systems: A Case Study from a Turkish University Hospital

Elif Çalık, Karabuk University, Health School; Hilal Kaya, Ministry of National Education; Abdullah Çavuşoğlu, Yıldırım Beyazıt University, Faculty of Engineering and Natural Sciences; Selami Akkuş, Yıldırım Beyazıt University, School of Medicine; Baha Şen, Yıldırım Beyazıt University, Faculty of Engineering and Natural Sciences

Siber Güvenlik Konusunda Kurumsal Farkındalık ve Entegre Çözüm Altyapısı

İbrahim Dinçer, BİTES

Askerî Alandaki Bulut Sistemi Kullanımına Güvenlik Yaklaşımları

İsmail Aydın, Harp Akademileri Komutanlığı; Recep Kılıç, Harp Akademileri Komutanlığı; Ahmet Zeki Gerehan, Harp Akademileri Komutanlığı

Siber Tehdit Ortamında Muharebe Sahasının Sayısallaştırılması

Selçuk Dal, KHA; Eşref Fırat, KHA; Serbülent Eken, KHA

Cyber Attack Timing

Ferhat Çalışkan, Kara Harp Akademisi; Yavuz İduğ, Kara Harp Akademisi

Metin için Yapay Sinir Ağı Tabanlı Hash Fonksiyonu

Yakup Kutlu, Mustafa Kemal Üniversitesi; Apdullah Yayık, TSK

Bulut Bilişimde Bilgi Güvenliği ve Standardizasyon Çalışmaları

Gökhan Şengül, Atılım Üniversitesi; Atıla Bostan, Atılım Üniversitesi

Bulut Ortamında Adli Bilişim

Onur Sevlı, Suleyman Demirel University; Ecir Uğur Küçüksille, Süleyman Demirel Üniversitesi

Irregular Warfare with Cyber Means

Hilmi Kendircioğlu, War Colleges Command; Tuncay Kaymazlı, War Colleges Command; A. Alper Eker, War Colleges Command

Martin C. Libicki'nin "Siber Caydırıcılık" Kavramının Nükleer Caydırıcılık Olgusu ile Karşılaştırılmalı Analizi

Uğur Ermiş, Uludağ University; Barış Özdağ, Uludağ University

Güvenli Yazılım Geliştirme Yaşam Süreci ve Statik Kod Analizi

Güncel Sarıman, Muğla Sıtkı Koçman Üniversitesi; Ecir Uğur Küçüksille, Süleyman Demirel Üniversitesi

Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti

Yavuz Iduğ, Kara Harp Akademisi; Ferhat Çalışkan, Kara Harp Akademisi; Talip Güler, Kara Harp Akademisi

Son İşlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki Etkisinin İncelenmesi

Erdinç Avaroğlu, İnönü Üniversitesi; Mustafa Türk, Fırat Üniversitesi

Hücrel Otomata ve Kaos Tabanlı Bir Şifreleme Algoritmasının Güvenlik Analizi

Fatih Özkaynak, Fırat Üniversitesi; Ahmet Bedri Özer, Fırat Üniversitesi; Sırma Yavuz, Yıldız Teknik Üniversitesi

Hava-Hava ve Hava-Yer Taktik Data Link Sistemi için Kriptografi Donanımı

Muhammet Hamdi Yavuz, Gate Elektronik A.Ş.; Osman Buğra Sarıca, Gate Elektronik A.Ş.; Mehmet Haluk Canberi, Gate Elektronik A.Ş.; Alper Kılıç, Gate Elektronik A.Ş.

Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri

M.Zekeriya Gündüz, Bingöl Üniversitesi; Resul Daş, Fırat Üniversitesi;

Bukalemun: Bilişim Güvenliğinde Yeni Bir Sızma Test Platformu

Emrah Ayyüzlü, Kuveyt Türk Katılım Bankası; Emre Özer, Kuveyt Türk Katılım Bankası

Uygulamalarda Şifre Güvenliği İçin Yeni Bir Yaklaşım

Yasin Sönmez, Batman Üniversitesi; Murat Karabatak, Fırat Üniversitesi; Engin Avcı, Fırat Üniversitesi

Security Challengers in Grid Operating Systems

Farhad Soleimanian Gharehchopogh, Islamic Azad University; Neda Jabbari, Islamic Azad University; Nima Hojjati, Islamic Azad University

Siber Saldırı Hedefleri ve Türkiye’de Siber Güvenlik Stratejisi

Seda Yılmaz, Gazi Üniversitesi; Şeref Sağıroğlu, Gazi Üniversitesi

Özgün Bir Şifreleme Algoritması Kullanan Güvenli E-Posta Uygulaması

Muhammet Çınar, Hacettepe Üniversitesi; Işıl Çınar, Gazi Üniversitesi; Hasan Şakir Bilge, Gazi Üniversitesi

A Secure System Development Framework for SaaS Applications in Cloud Computing

Eren Tatar, METU; Emrah Tomur, METU

Ulusal Siber Güvenliğin Sağlanmasında NATO’nun Olumlu Etkilerinin Artırılması İçin Yaklaşım Modeli

Ümit Bayık, Kara Harp Akademisi; İnan Semiz, Harp Akademisi; Selçuk Sönmez, Kara Harp Akademisi; Melih Durak, Kara Harp Akademisi

AES Blok Şifresinin Anahtar Genişletme Rutininin Geliştirilmesi ve Bir Blok Şifreden Bağımsız Anahtar Genişletme Rutininin Tasarımı

Fatma Büyüksaraçoğlu Sakallı, Trakya Üniversitesi; Ercan Buluş, Namık Kemal Üniversitesi; Muharrem Tolga Sakallı, Trakya Üniversitesi; Hüseyin Vural, Trakya Üniversitesi

Eşler Arası Ağlarda Teşvik Modelleri

Serkan Çakmak, Hacettepe Üniversitesi; Ahmet Burak Can, Hacettepe Üniversitesi

12:30-12:45

KONFERANS DEĞERLENDİRME TOPLANTISI
CONFERENCE EVALUATION MEETING

12:45-13:00

KAPANIŞ/CLOSING CEREMONY