TOPICS

Topics of Interest include, but are not limited to:

Main Topic: Cyber Security and Defence

- Cryptographic Protocols for Cloud Security
- Energy/Cost/Efficiency of Security in Clouds
- Secure Data Management Outsourcing (e.g., database as a service)
- Secure Computation Outsourcing
- Trusted Computing Technology and Clouds
- Trust and Policy Management in Clouds
- Security Risk Models and Clouds
- Spying
- Social Networks
- Critical Infrastructures
- Cloud Computing
- Threats
- Practices and Solutions
- Strategies and Policies
- Laws
- Standards
- International Collaboration

Data Privacy

- Privacy Foundations
- Privacy Enhancing Technologies
- Privacy-Preserving Computing
- Privacy Policies and Laws
- Electronic Healthcare Privacy
- Economics of Privacy
- Privacy Theory and Engineering
- Natural Disasters and Emergencies, and Terrorism Protection
- Risk Analysis, Modeling, and Management
- Trust Formalization and Modeling
- Trustworthy Computing
- Trust Management
- Trust Evaluation
- Security Foundations

E-Governance Security

- E-Government Security
- E-Archive
- E-Bid
- E-Commerce
- E-Health
- E-Id
- E-Invoice
- E-Justice

- E-Notary
- E-Passport
- E-Voting
- Critical Information Infrastructure Protection
- Virtual Wars and Countermeasures
- Information Systems and Crime Analysis
- Risk Evaluation and Security Certification

Public Key Infrastructure

- Digital Signature
- Certified Electronic Mail
- Certificates and Certificate Management
- Standards
- Protocols
- Trust Models
- Key and Identity Management
- Hardware/Software Applications
- Digital Signature Policies and Law
- Validity of Digital Signature in Government, Finance, and Commerce
- Effects of Digital Signature on Digital Signature Law
- Responsibilities for Opponents to ESSP in Law in Digital Signature
- Discrepancy between Digital Signatures
- Judgments related to Digital Signatures
- Digital Signature Law in Other Countries

Cryptology

- Boolean Functions
- Block Ciphers
- Stream Ciphers
- Public Key Cryptography
- Quantum Cryptography
- Elliptic Curve Cryptography
- Algebraic Curves in Cryptography
- Homomorphic Encryption
- Cryptographic Protocols
- Zero Knowledge
- Secret Sharing
- Cryptanalysis
- Hash Functions
- Applications of Coding Theory in Cryptography
- Cryptographic Hardware and Embedded Systems
- Special Purpose Hardware for Attacking Cryptographic Systems
- Efficient Software and Hardware Implementations
- Side Channel Analysis and Countermeasures
- Pairing Based Cryptography
- Key and Identity Management

Information Security

- Steganography
- Secure Multiparty Computation
- Biometric Approaches
- Computer Security
- Mobile Communications Security
- Operating System Security
- Trusted Computing
- Network Security
- Wireless Security
- Ad Hoc and Sensor Network Security
- Peer to Peer Network Security
- Web Security
- E-mail Security
- Database Security
- IPTV Security
- E-commerce Protocols
- Content filtering and tracing
- Copyright protection
- Distributed System Security
- Security Weaknesses on Information Technologies
- Secure Code Development
- Penetration Tests
- Intrusion Detection Systems
- Malicious Codes
- Viruses, Spyware, Spamware, Scam
- Smart Card Applications and Security
- RFID Security

Information Forensics and Security

- Digital Forensics
- Signal processing in the encrypted domain
- Forensics for Future Generation Communication (FGC)
- Digital Forensics tools in FGC
- Digital Evidence Analytics and Management in FGC
- Digital Forensics Surveillance Technology and Procedures in FGC
- Digital evidence visualisation and communication for FGC
- Digital evidence storage and preservation in FGC
- Incident response and investigation in FGC
- Forensic procedures in FGC
- Portable electronic device forensics for FGC
- Network forensics in FGC
- Data hiding and recovery in FGC
- Network traffic analysis, traceback and attribution in FGC
- Legal, ethical and policy issues related to digital forensics in FGC
- Integrity of digital evidence and live investigations

- Multimedia analysis in FGC
- Trends and Challenges for FGC
- Evidence Protection in FGC
- Forensics case studies in FGC

Sectoral Applications

- E-government Applications
- M-government Applications
- Applications of Electronic Signature Certificate Providers
- Applications for Banks and
- Finance Institutions
- GSM Operators

Senior Design Projects

- Projects dealing with information security and cryptology

MSc. and PhD. Thesis

- Thesis dealing with information security and cryptology

KONU BAŞLIKLARI

Ana Tema: Siber Güvenlik ve Savunma

- Casusluk
- Sosyal Ağlar
- Terör
- Tehditler ve Tehlikeler
- Ulusal/Uluslararası Hukuk
- Tatbikatlar
- Metodolojiler/Çözümler
- Strateji/Politikalar
- Standartlar
- Uluslararası İşbirlikleri

Kişisel Verilerin Korunması

- Gizlilik Temelleri
- Gizlilik Geliştirme Teknolojileri
- Gizlilik-Koruma Programlama
- Gizlilik Politika ve Yasaları
- Elektronik Sağlık Gizliliği
- Gizlilik Ekonomisi
- Gizlilik Teorisi ve Mühendisliği
- Doğal Felaketler ve Acil Servisler ve Terörizm Koruması
- Risk Analizi, Modelleme ve Yönetimi
- Güven Biçimlendirme ve Modelleme
- Güvenli Programlama
- Güven Yönetimi
- Güven Değerlendirmesi
- Güvenlik Temelleri

E-Yönetim Güvenliği

- E-Devlet Güvenliği
- E-Arşiv
- E-İhale
- E-Ticaret
- E-Denetim
- E-Sağlık
- E-Kimlik
- E-Fatura
- E-Adalet
- E-Noter
- E-Pasaport
- E-Oylama
- Kritik Bilgi Altyapısı Koruma
- Sanal Savaşlar ve Karşı Tedbirler
- Bilgi Sistemleri ve Suç Analizi
- Risk Değerlendirmesi ve Güvenlik Belgelendirmesi

Açık Anahtar Altyapısı

- Elektronik İmza
- Kayıtlı Elektronik Posta
- Sertifikalar ve Sertifika Yönetimi
- Standartlar
- Protokoller

- Güven Modelleri
- Anahtar ve Kimlik Yönetimi
- Donanımsal ve Yazılımsal Uygulamalar
- Elektronik İmza Politikaları ve Yasalar
- Elektronik İmzanın Kamusal İşlemlerde, Bankacılık İşlemlerinde ve Diğer Ticari İşlemlerde Hukuki Geçerliliği
- Elektronik İmzanın Elektronik İmza Mevzuatına Getirebileceği Değişiklikler
- Elektronik İmza Uygulamasında Yer Alan Tarafların ESHS'ye Karşı Hukuki
- Sorumluluk Halleri
- Elektronik İmza İle İlgili Çekişmeli Olaylar
- Elektronik İmza İle İlgili Yargı Kararları
- Diğer Ülkelerdeki Elektronik İmza Yasaları

Kriptoloji

- Boole Fonksiyonlar
- Blok Şifreler
- Akan Şifreler
- Açık Anahtarlı Kriptografi
- Kuantum Kriptografisi
- Eliptik Eğri Kriptografisi
- Kriptografide Cebirsel Eğriler
- Protokoller
- Sıfır Bilgi Yaklaşımı
- Sır Paylaşımı
- Kriptoanaliz
- Özet Fonksiyonlar
- Kriptografide Kodlama Teorisi Uygulamaları
- Akıllı Kart Uygulamaları ve Güvenliği
- RFID Güvenliği
- Kriptografik Donanım ve Gömülü Sistemler
- Kriptografik Sistemlerin Kriptoanalizi için Özel Amaçlı Donanım
- Verimli Yazılım ve Donanım Uygulamaları
- Yan Kanal Analizi ve Karşı Önlemler
- Eşleme Tabanlı Kriptografi
- Anahtar ve Kimlik Yönetimi

Bilgi Güvenliği

- AJAX/Web 2.0/Javascript Güvenliği
- Sömürme Taktikleri
- Java & .NET Güvenliği
- Mobil Cihaz Güvenliği
- Kaynak Kod Denetim ve Revizyonu
- Steganografi ve Steganaliz
- Güvenli Çoklu Hesaplama
- Biometrik Yaklaşımlar
- Bilgisayar Güvenliği
- Mobil İletişim Güvenliği
- İşletim Sistemi Güvenliği
- Güvenilir Hesaplama
- Ağ Güvenliği
- Kablosuz Güvenlik
- Özel Amaca Yönelik ve Algılayıcı Ağ Güvenliği
- Uçtan Uca Ağ Güvenliği
- Web Güvenliği
- E-posta Güvenliği

- Veritabanı Güvenliği
- IPTV Güvenliği
- E-ticaret Protokollerinde Güvenlik
- İçerik Filtreleme ve Takibi
- Yayınım Güvenliği
- Telif Hakkı Koruması
- Dağıtık Sistem Güvenliği
- Bilgi Teknolojilerinde Güvenlik Zaafiyetleri ve Açıkları
- Güvenli Kod Geliştirme
- Sızma Testleri
- Saldırı Tespit Sistemleri
- Kötücül ve Casus Yazılımlar
- IPv6 Güvenliği
- Çevrimiçi Dolandırıcılık

Adli Bilişim ve Güvenlik

- Adli Bilişim
- Şifrelenmiş Alanda Sinyal İşleme
- Yeni Nesil İletişim(YNİ)'de Adli Bilişim ve Güvenlik
- YNİ'de Adli Bilişim ve Hukuk
- YNİ'de Adli Bilişim Araçları
- YNİ'de Elektronik Kanıt Yönetimi
- YNİ'de Elektronik Kanıt Tahlili
- YNİ'de Adli Bilişim Denetim Teknolojileri ve Prosedürleri
- YNİ için Elektronik Kanıt Görüntüleme ve İletişim
- YNİ'de Elektronik Kanıt Saklama ve Koruma
- YNİ'de Kaza Müdahalesi ve İncelemesi
- YNİ'de Adli Prosedürler
- YNİ'de Taşınabilir Elektronik Cihazların Adli Takibi
- YNİ'de Ağ Hukuku
- YNİ'de Veri Saklama ve Kurtarma
- YNİ'de Ağ Trafik Analizi, Takibi ve Niteliklendirme
- YNİ'de Adli Bilişimle İlgili Yasal, Etik ve Politika Konuları
- Elektronik Kanıt ve Soruşturma Bütünlüğü
- GNİ'de Çoklu Ortam Analizi
- GNİ'de Yönelimler ve Zorluklar
- GNİ'de Kanıt Koruma
- GNİ'de Adli Durum Çalışmaları

Sektörel Uygulamalar

- E-Devlet Uygulamaları
- M-Devlet Uygulamaları
- Elektronik Sertifika Hizmet Sağlayıcı Uygulamaları
- Bankacılık ve Finansal Uygulamalar
- GSM Operatörleri

Bitirme Projeleri

- Bilgi Güvenliği ve Kriptoloji alanında yapılmış Bitirme Projeleri

Yüksek Lisans ve Doktora Tezleri

- Bilgi Güvenliği ve Kriptoloji alanında yapılmış tez çalışmaları

LANGUAGE

The working languages of the ISCTurkey 2014 conference are English and Turkish

KONFERANS DİLİ

Konferans dili İngilizce ve Türkçe'dir.