

PREFACE

The 7th International Conference on Information Security and Cryptology (ISCTurkey 2013) organized by the Information Security Association of Turkey, Information Technologies and Communications Authority (BTK), Gazi University, Istanbul Technical University and Middle East Technical University (METU) was held in Istanbul, Turkey, on September, 17-18, 2014. "Information Security and Cryptology Conference" is an event in which related scientific and sectoral studies done in Turkey and around the world are shared, university-government-industry cooperation is developed, the public is informed and trained, and all scientists, researchers and industry practitioners exchange their knowledge and experiences among themselves. The goals of this conference are to help adaptation of society members to the information security and cryptology concepts, to contribute to increase the accumulation of scientific knowledge in this field, and to enhance cooperation among scientists, institutions and industries.

The main theme of this year's "International Conference on Information Security and Cryptology" is "Siber Security and Defence". As living in the age of information and technology, public and private sector institutions and organizations begin to place their own data in electronic medium with an increasing demand; hence, protecting the electronic data is more important than ever in today's cyber environment in which the new spyware is developed every half second, and an average of 15-25 new attacks is occurring every day. Therefore, especially, the solutions to prevent, defence and/or resist against cyber attacks which are occurred increasingly recently towards the military, economic, technological, and critical infrastructure of the countries, and other topics were discussed by experts in the conference.

The submitted papers were evaluated by the members of program committee. Accepted papers, reviewed by at two or least three referees, were published in the conference proceedings. We are happy to declare the acceptance rate of 52/75. The proceedings of ISCTurkey 2014 include 33 regular papers and 19 posters. The papers cover cryptographic hardware implementations, mathematical aspects of efficient cryptographic applications, cryptanalysis techniques, methods in data privacy, steganography, cyber security and defence, military aspects of cyber security and solutions to security problems in networks and cloud computing security.

In addition to that; four invited speakers have been invited, Two panels are organised. One training course for security awareness is prepared and 2 company presentations are included to the conference program.

This conference would not be possible without the involvement of many participants, in particular the members of organizing committee and program committee who reviewed all the submitted manuscripts. We would like to thank to the members, participants, invited speakers, panelists and the sponsors. Last but not least, we also would like to thank all the authors who have submitted their papers and greatly contributed to the success of ISCTurkey 2014.

Hoping and wishing that the outputs of the conference would help to develop more secure environments and platforms for people, sectors, institutions and countries.

Best wishes.

ISCTurkey 2014 Organising Committee

ÖNSÖZ

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın (ISCTURKEY'14), Bilgi Güvenliği Derneği'nin Bilgi Teknolojileri ve İletişim Kurumu, Gazi Üniversitesi, İstanbul Teknik Üniversitesi (İTÜ) ve Orta Doğu Teknik Üniversitesi (ODTÜ) işbirliği ile bu sene altıncısı 17-18 Ekim 2014 tarihleri arasında İstanbul'da düzenlenmektedir.

Bilgi Güvenliği ve Kriptoloji Konferansı düzenlendiği ilk yıldan beri Türkiye'nin bu alanlardaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı Türkiye'deki bu alandaki en önemli etkinliktir. Her ülke için önemli olan bilgi güvenliği ve kriptoloji kavramlarının, toplumun bireyleri tarafından özümsemesine yardımcı olmak, ülkemizde bu alanda bilimsel bilgi birikiminin artırılmasına katkılar sağlamak, kurumlar ve sektör arasındaki işbirliğini arttırmak bu konferansın temel hedefleri arasındadır.

Bilgi Güvenliği ve Kriptoloji Konferansı'nın hedefleri doğrultusunda, bu seneki ana tema "Siber Güvenlik ve Savunma" olarak belirlenmiştir. Bilgi ve teknoloji çağı olarak adlandırılan günümüzde, kamu ve özel sektör kurum ve kuruluşlarının bilgi varlıkları her geçen gün daha fazla elektronik ortamlarda yer almaya ve bu veriler artık bulutlarda tutulmaya başlamıştır. Bu verilerin korunması ise her yarım saniyede yeni bir casus yazılımın geliştirildiği ve hemen hemen her saatte yeni bir siber saldırının bulunduğu günümüzde her zamankinden daha önemli hale gelmiştir. Bu bağlamda, ülkelerin askeri, ekonomik, teknolojik ve kritik altyapılarına karşı son zamanlarda büyük artış gösteren siber saldırılara karşı koyabilecek ve/veya engel olabilecek çözüm önerileri diğer konularla beraber özellikle konferans çerçevesinde konunun uzmanları tarafından değerlendirilmiştir.

Konferansın bildiriler kitabında yayınlanması için akademisyenler ve uygulayıcılar tarafından eşbaşkanlara iletilen bildiriler, alanında uzman en az iki veya üç hakem tarafından yapılan raporlar göz önüne alınarak değerlendirilmiştir. Hakem raporlarınca uygun bulunan bildiriler sözlü veya poster sunumu için seçilerek bildiriler kitabında basılmıştır. Toplam 75 bildiri başvurusundan 52 tanesi bildiriler kitabında basılmıştır. Bunların 33'ü sözlü sunum ve 19'u ise poster sunumudur. Sözlü sunum için seçilen bildiriler, konferansta üç ayrı salonda yazarlar tarafından sunulacaktır. Poster sunumları ise katılımcıların görebileceği bir salonda poster halinde sunulacaktır. Kabul edilen bildiriler, gizli paylaşım senaryo önerileri, sonlu cisim aritmetiği, simetrik sistemlerde protokol analizleri, bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, siber güvenlik ve savunma, bulut bilişim güvenliği ve akıllı kartlarda kullanılan kriptografik protokoller ve bunların uygulamalarına yönelik çalışmaları kapsamaktadır. Konferans süresince ana tema "Siber güvenlik ve Savunma" konusu çerçevesinde sözlü ve poster sunumların yanında iki panel organize edilmiş, 4 davetli konuşmacı konferansa davet edilmiş, güvenlik farkındalık eğitim programı hazırlanmış ve iki kurumun sunum yapması için programa eklenmiştir.

Bu konferansın gerçekleştirilmesinde emeği geçen Düzenleme Kurulu ve Danışma Kurulu üyelerine, bildirilerini konferansta sunan katılımcılara ve bu bildirilerin bilimsel kalitesinin yüksek olması için katkıda bulunan tüm hakemlerimize, ve konferansa destek olan sponsorlarımıza teşekkür ederiz.

Bu yıl yedincisi düzenlenen bu konferansın, kullanıcılara, kurumlara, sektöre ve ülkelere faydalı olacak çıktılar üretmesini ve daha güvenli ortamlar oluşturulmasına katkılar sağlamasını dileriz.

Saygılarımızla.
ISCTurkey 2014 Düzenleme Kurulu