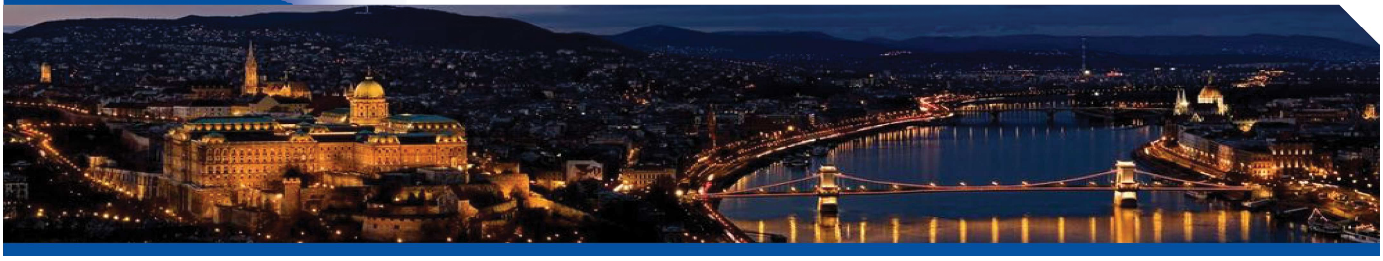
IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS

IEEE International Conference on Communications 2013

Bridging the Broadband Divide
9-13 June • Budapest, Hungary

IEEE
IEEE COMMUNICATIONS SOCIETY

WWW.IEEE-ICC.ORG/2013



Communications and Information Systems Security Symposium (CISS)

Symposium Co-Chairs

Tansu Alpcan, The University of Melbourne, Australia

Email: tansu.alpcan@unimelb.edu.au

Mark Felegyhazi, Budapest University of Technology and Economics, Hungary

Email: mfelegyhazi@crysys.hu

Kejie Lu, University of Puerto Rico at Mayagüez

Email: kejie.lu@upr.edu

The 2013 IEEE International Conference on Communications (ICC) will be held in the vibrant city of Budapest, Hungary from 9 – 13 June 2013. This flagship conference of IEEE Communications Society aims at addressing an essential theme on "Bridging the Broadband Divide." The conference will feature a comprehensive technical program including several Symposia and a number of Tutorials and Workshops. IEEE ICC 2013 will also include an attractive expo program including keynote speakers, various Business, Technology and Industry forum, and vendor exhibits. We invite you to submit your original technical papers, industry forum, workshop, and tutorial proposals to this event. Accepted and presented papers will be published in the IEEE ICC 2013 Conference Proceedings and in IEEE Xplore®. Full details of submission procedures are available at http://www.ieee-icc.org/2013.

Scope and Topics of Interest

The Communications and Information Systems Security Symposium (CISS) will focus on all aspects of security, privacy, trust, and risk management, which pose a serious challenge to today's globally connected society. The symposium welcomes novel contributions on evaluation, modeling, analysis, and design of communication and information systems security solutions, from the physical layer to the application layer. In addition, this year's CISS emphasizes security risk management of information systems where quantitative models are utilized to balance available resources against security risks.

To ensure complete coverage of the advances in communication and information systems security, the CISS presents original contributions in, but not limited to, the following topical areas:

- Anonymity, anonymous communication, measures and performance analysis
- Authentication protocols and message authentication
- Authorization and access control
- Availability and survivability of secure services and systems
- Biometric security: technologies, risks, vulnerabilities, bio-cryptography, anonymity and privacy
- Botnet prevention, detection and defense
- Cloud and distributed application security
- Computer and network forensics

- Cyber security
- Datacenter security
- DDOS attacks, DNS spoofing, intrusion, localization and countermeasures
- Digital rights management: information hiding, watermarking, and fingerprinting
- Firewall technologies; intrusion detection, localization, and avoidance
- Formal trust models, security modeling and protocol design
- Identity management
- Information systems security and security management
- Integrity
- IPv6 and future Internet security
- Key distribution and management
- Lightweight security
- Mobile and Wireless network security, including ad hoc networks, P2P networks, 3G, 4G, sensor networks, Bluetooth, 802.11 family and WiMAX
- Multi-mode surveillance and homeland security
- Multimedia security including VoIP, IPTV, DAB
- Network public opinion analysis and monitoring
- Network security metrics and performance evaluation
- Operating systems and application security and analysis tools
- Physical security and hardware/software security
- Privacy and privacy enhancing technologies
- Public-key, symmetric-key, applied crypto, coding-based applied cryptography
- Quantum cryptography and communication applications
- Resource allocation, incentives, and game-theoretic approaches
- Security in virtual machine environments
- Security in wired systems and optical networks
- Security of Cyber-physical systems
- Security risk management
- Trust models, management and certificate handling
- Virtual private networks and group security
- Vulnerability, exploitation tools and virus analysis
- Web, e-commerce, and m-commerce security

Submission Guidelines

Prospective authors are invited to submit original technical papers by the deadline 16 September 2012 for publication in the IEEE ICC 2013 Conference Proceedings and for oral or poster presentation(s).

All submissions should be written in English with a maximum paper length of Five (5) printed pages (10- point font) including figures without incurring additional page charges (maximum 1 additional page with over length page charge if accepted).

It is strongly recommended to use the standard IEEE templates for preparing your manuscripts.

Standard IEEE templates for Microsoft Word or LaTeX formats can be found at http://www.ieee.org/conferences_events/conferences/publishing/templates.html.

Only PDF files will be accepted for the review process and all submissions must be done through EDAS at http://edas.info/N12645.

Short biography of co-chairs

Tansu Alpcan is a Senior Lecturer at the University of Melbourne, Australia. His research involves applications of distributed decision-making, game theory, and control to various security and resource allocation problems in complex and networked systems. He has received multiple research achievement and best paper awards, including one in 2010 IEEE ICC, CISS. He has played an active role in the organization of various IEEE conferences and chaired GameSec, GameComm, RawNet conferences/workshops. He is the (co-)author of more than 100 journal and conference articles as well as the book "Network Security: A Decision and Game Theoretic Approach" published by Cambridge University Press in 2011.

Mark Felegyhazi Mark is an assistant professor in the Laboratory of Cryptography and Systems Security (CrySyS Lab) at Budapest University of Technology and Economics (BME), Hungary, and the deputy head of the lab. He received the M.Sc. degree from BME, Hungary in 2001, and earned the Ph.D. degree from EPFL (Swiss Federal Institute of Technology -- Lausanne), Switzerland in 2007. From 2008 to 2010, he was a postdoctoral researcher at UC Berkeley and in the International Computer Science Institute (ICSI) in Berkeley. Mark's research interest covers incentive problems in risk management and computer security. He has been a member of high-profile projects featured in mainstream media: Click Trajectories (on spam underground economy), Duqu and Flame (on targeted attacks against critical infrastructure).

Dr. Kejie Lu received the B.S. and M.S. degrees in Telecommunications Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1994 and 1997, respectively. He received the Ph.D. degree in Electrical Engineering from the University of Texas at Dallas in 2003. Since July 2005, he has been a faculty member in the Department of Electrical and Computer Engineering, University of Puerto Rico at Mayaguez. Dr. Kejie Lu’s research interests include architecture and protocols design for computer and communication networks, performance analysis, network security, and wireless communications. Dr. Kejie Lu has many experience managing reviews and publications. He is an Editor of IEEE Communications Society Survey & Tutorial, an Associate Editor of Wiley Security and Communication Networks (SCN), and an Associate Editor of Wiley International Journal of Communication Systems (IJCS). His experience also includes TPC co-chair of ISWPC 2007, Track chair of the Information Assurance and Security (IAS) track at both IEEE MILCOM 2007 and IEEE MILCOM 2008, Track co-chair of Mobile / Wireless Applications and Services track at IEEE VTC2008-Spring, Symposium co-chair of the Wireless Communications Symposium in ICCCAS 2009, Symposium co-chair of the Communication and Information System Security (CISS) symposium in IEEE Globecom 2010. Dr. Kejie Lu is a senior member of IEEE.