IEEE International Conference on Communications
IEEE ICC 2014
Communications: The Centrepoint of the Digital Economy
10 - 14 June 2014, Sydney, Australia

Communications and Information Systems Security Symposium (CISS)

Symposium Co-Chairs

Peter Mueller, IBM Zurich Research, Switzerland, pmu@zurich.ibm.com
Shui Yu, Deakin University, Australia, syu@deakin.edu.au
Thorsten Strufe, TU Darmstadt, Germany, strufe@cs.tu-darmstadt.de

The 2014 IEEE International Conference on Communications (ICC) will be held in the beautiful city of Sydney, Australia between 10 and 14 June 2014. The theme of this flagship conference of IEEE Communications Society for 2014 is "*Communications: The Centrepoint of the Digital Economy*." The conference will feature a comprehensive technical program including twelve Symposia and a number of Tutorials and Workshops. IEEE ICC 2014 will also include an attractive expo program including keynote speakers, and Industry Forum & Exhibitions (IF&E). 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 2014 Conference Proceedings and in IEEE Xplore®. Full details of submission procedures are available at http://www.ieee-icc.org/2014.

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 puts a stronger emphasis on network oriented security and privacy, such as security related topics of cloud computing, networking related security in Big Data, IoT, and so on.

To ensure complete coverage of the advances in communication and information systems security, the topics of interest of the CISS include, but are not limited to, the following areas:

- Anonymity, anonymous communication, metrics and their performance analysis
- Authentication protocols and message authentication
- Authorization and access control
- Availability and survivability of secure services and systems
- Big Data security and privacy
- Biometric security

- Botnet detection, prevention, and defense
- Cloud and distributed application security
- Computer and network forensics
- Cryptography and evaluation
- Data center security
- Firewall technologies; intrusion detection, localization, and avoidance
- Formal trust models, security modeling and protocol design
- Key distribution and management
- Lightweight security
- Location-based services and their security and privacy aspects
- Mobile and Wireless network security
- Mobile App security and privacy
- Multi-mode surveillance and homeland security
- Network public opinion analysis and monitoring
- Network security metrics and their performance evaluation
- Operating systems and application security and analysis tools
- Online Social Networks and their security aspects
- Physical security and hardware/software security
- Privacy and privacy enhancing technologies
- 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 15 September 2013 for publication in the IEEE ICC 2014 Conference Proceedings and for oral or poster presentation(s). All submissions should be written in English with a maximum paper length of six (6) printed pages (10-point font) including figures without incurring additional page charges (a maximum of one additional page will be accepted, subject to over-length charge).

Standard IEEE Transactions templates for Microsoft Word or LaTeX formats found at
http://www.ieee.org/portal/pages/pubs/transactions/stylesheets.html
Alternatively you can follow the sample instructions in template.pdf at

http://www.comsoc.org/confs/globecom/2008/downloads/template.pdf

Only PDF files will be accepted for the review process and all submissions must be done through EDAS at

http://edas.info/

Short biography of co-chairs

Peter Mueller joined IBM Research as a Research Staff Member in 1988. He is also the Chair of the IEEE Communications and Information Systems Security Technical Committee (CIS-TC).

His research expertise covers broad areas of human-machine interfaces, distributed computing systems architecture, communications and interconnects technology, device physics, nanoscience, and computer modeling.

Focusing on communications, his main experience is in the fields of complex systems architecture, including resource allocation and re-allocation, synchronization, and real-time behavior; cross layer reliability issues; channel coding techniques; and error control and correction methods. His current field of research is in the area of data center storage security and reliability.

He is member of the Electrochemical Society (ECS), the Swiss Physical Society (SPS), and IEEE. He also served as government counsel and as program chair for many international conferences and workshops, such as ICNC 2013, CIS symposium of Gobecom 2012.

Shui Yu is currently a Senior Lecturer of the School of Information Technology, Deakin University, Australia. Dr Yu is active in research services in various roles. He is a guest editor for a special issue on Security, Privacy and Forensics for P2P Networks for the Journal of Peer-to-Peer Networking and Applications. He services the editor boards of three International journals, such as the International Journal of Internet Services and Information Sciences. He is a reviewer for a number of prestigious journals, such as IEEE TPDS, IEEE TOC, IEEE ToWC, IEEE TSMC (Part B), The Computer Journal, The Journal of Parallel and Distributed Computing. Dr Yu is also involved in organizing international conferences, such as TPC Co-chairs of security symposium ICC2014, ICNC 2013; publicity co-chairs for ICNC 2012, UbiSafe 2011. He services as TPC member for international conferences, such as INFOCOM 2013, 2012, AINA2012, DASC2011, MobiWac2011, FCST2011, and iCAST2011.

Dr Yu's current research interests include network security, privacy and forensics, networking theory, and mathematical modeling. He targets on narrowing the gap between theory and applications using mathematical tools. He has been publishing papers in high quality journals, such as IEEE Transactions on Information Forensics and Security, IEEE Transactions of Parallel and Distributed Systems, IEEE Transaction on System, Man, and Cybernetics, Part B, and IEEE Transactions on Mobile Computing. He is a Senior Member of the IEEE.

Thorsten Strufe is professor for peer-to-peer networks at Technische Universität Darmstadt. His research interests lie in the areas of large scale distributed systems and social networking services, with an emphasis on privacy and resilience. Recently, he has focused on studying user behavior and security in online social networks and possibilities to provide privacy-preserving and secure social networking services through P2P technologies.

He was appointed visiting professor for Dependable Distributed Systems at University of Mannheim, Germany, throughout 2011. Previously, he took a post as senior researcher at EURECOM and at TU Ilmenau, working on analysis and the security of online social networks, as well as resilient networking.

He received his PhD degree from TU Ilmenau in 2007. His PhD thesis deals with the construction of network-efficient overlay topologies for live multimedia streaming, and means to making them especially resilient towards both the failure of nodes and DoS attacks.