The 1st IEEE International Workshop on

Security in Computers, Networking and Communications (SCNC)

In conjunction with IEEE INFOCOM 2011
April 10-15, 2011, Shanghai, China

Web site: http://bbcr.uwaterloo.ca/~rxlu/scnc/

IMPORTANT DATES:

Paper submission:	Jan. 3, 2011
Author notification:	Feb. 15, 2011
Camera ready:	Mar. 15, 2011

IEEE

IEEE COMMUNICATIONS SOCIETY

CALL FOR PAPERS

The IEEE International Workshop on Security in Computers, Networking and Communications (SCNC) is an international forum for researchers, developers, and practitioners to demonstrate new ideas, techniques, and tools on secure and usable computer and communications systems and user privacy, new threats to confidentiality, integrity, and usability of computer and communications systems and user privacy, for users to exchange their experience in new tools and techniques that lead to improvement of security, integrity, and usability of computer and communication systems. The workshop welcomes academia, government, industry, and contributing individuals to submit unpublished papers in theoretical and practical aspects of computer and communications security. Original, unpublished contributions are solicited in ALL security aspects of computers, networking and communications. Possible topics of interest include, but are not limited to:

- Accountability, non-repudiation, privacy, and anonymity
- Usability and security
- Computer systems security
- Software security
- Network security
- Security in networked sensing and control systems
- Attacks and counter measures
- Computer and network forensics
- Attacks, security mechanisms, and security services
- Authentication
- Access control
- Multicast security
- Security specification techniques
- Encryption and decryption
- Secure routing protocols
- Formal analyses
- Security group communications
- Intrusion detection
- Key management
- Trust establishment
- Revocation of malicious parties
- Security policies
- Fraudulent usage
- Dependability and reliability
- Prevention of traffic analysis
- Secure PHY/MAC/routing protocols
- Secure location determination
- Denial of service
- Network security performance evaluation
- Tradeoff analysis between performance and security
- Design or analysis of security protocols
- Mobile and Wireless network security, including ad hoc networks, P2P networks, sensor networks, mesh networks, and social networks
- Trust and reputation in ubiquitous environments
- Web, eBusiness, eCommerce, eGovernment security
- Security standards

Papers must not exceed 6 single-spaced and two-column pages using at least 10 point size type on 8.5 x 11 inches pages, and must be formatted in strict accordance with the IEEE Communications Society author guidelines. Submissions are being considered with the understanding that they describe original research, neither published nor under review elsewhere. Accepted papers will be published in the IEEE Digital Library after the conference and included in INFOCOM 2012 proceedings. **Selected best papers will be invited to a journal special issue.**

For further information, please refer to the site **http://bbcr.uwaterloo.ca/~rxlu/stnc/**, or contact the program co-chairs.