

# CALL FOR PAPERS

## CHINACOM 2008

August 25 - 27 2008, Hangzhou, Zhejiang, China.

### Network and Information Security Symposium

#### *Symposium Co-Chairs*

**Fei Hu**, Rochester Institute of Technology, USA ([fxheec@rit.edu](mailto:fxheec@rit.edu))

**Cheng Li**, Memorial University of Newfoundland, Canada ([licheng@enr.mun.ca](mailto:licheng@enr.mun.ca))

**Wade Trappe**, Rutgers University, USA ([trappe@winlab.rutgers.edu](mailto:trappe@winlab.rutgers.edu))

#### *Brief Description*

With the advent of pervasive computer applications and due to the proliferation of heterogeneous wired and wireless networks, computer and network security has become paramount. The ChinaCom2008 Network and Information Security Symposium will address all aspects of the modeling, design, implementation, deployment, and management of computer/network security algorithms, protocols, architectures, and systems. Furthermore, contributions to the evaluation, optimization, and/or enhancement of security mechanisms for current technologies as well as the achievements in devising efficient security and privacy solutions for emerging technologies are solicited. High-quality and original research papers are solicited in all areas of computer and network security systems. The symposium solicits original papers on all aspects of network and information security.

#### *Topics of interest include, but are not limited to:*

- 3G and 4G security
- 802.11 security and 802.11i
- Application/network penetration testing
- Authentication protocols
- Biometric security: technologies, risks and vulnerabilities
- Bluetooth security
- Computer and network forensics
- Critical infrastructure security
- Data and system integrity
- Deployment and management of computer/network security policies
- Distributed Denial-Of-Service (DDOS) attacks and countermeasures
- Distributed systems security
- DNS spoofing and security
- Encryption standards
- Financial cryptosystems
- Firewalls
- Formal trust models
- Information hiding and watermarking

- Intrusion avoidance
- IPv6 security and IPSec
- Key distribution and management
- Light-weight cryptography
- Message authentication
- Intrusion detection
- Countermeasures
- Quantum Cryptography and Quantum Key Distribution
- Mobile code security
- Network security metrics and performance evaluation
- Operating System(OS) security and log analysis tools
- Peer-to-peer system security
- Public-key cryptography
- Revocation of malicious parties
- Robust Security Network (RSN)
- Secure naming
- Secure Socket Layer (SSL)
- Security modeling and protocol design
- Security specification techniques
- Self-healing networks
- Sensor network security
- Single- and multi-source intrusion detection and response (automation)
- Smart cards and secure hardware
- Symmetric key cryptography
- Transport Layer Security (TLS)
- Trust establishment
- Upper-layer authentication
- Virtual Private Networks (VPNs) security
- Vulnerability, exploitation tools, and virus/worm analysis
- Web, e-commerce, m-commerce, and e-mail security
- Wi-Fi Protected Access (WPA)
- Power-reliability-security trade-offs in wireless networks
- Cross-layer approaches to security
- Mobile network security
- Location aware security in mobile networks
- Throughput-Security trade-offs in wireless networks
- Secure group multimedia communications
- Secure PHY/MAC/routing protocols
- Distributed security systems
- Secure cooperation in wireless networks
- Jamming and counter measures
- Attacks on security and vulnerability analysis
- Application layer encryption
- Digital watermarking and biometrics for secure information access

- Capacity and security analysis of covert channels
- Security Engineering
- Security in large-scale environments
- Security protocols
- Security of ad-hoc/sensor networks