



## **Call for Papers for *Communication and Information System Security Symposium***

### **Scope and Motivation:**

With the advent of the Internet of Things and the ubiquitous sharing of and access to networked content, computer and network security has become a primary concern for individuals, industry and governments. For example, sensitive information can potentially be copied, altered or injected for malicious purposes, e.g. taking advantage of sensitive information or stealing/abusing digital identities. There is also a growing risk that computer and network attacks will be deployed to disturb or even severely impact important infrastructure components like communication systems, power grids, or traffic control systems in order to cause significant economic damages. In addition to this, there is a growing awareness of privacy concerns, regarding individual users as well as corporate and/or governmental organizations. Therefore, new approaches to information security, availability protection and privacy management are required to be tightly integrated into IT- and communication systems.

The CISS Symposium will address all aspects of modeling, design, implementation, deployment, and management of computer/network security algorithms, protocols, services, architectures, and systems. Envisaged contributions to CISS symposium target all security aspects of wired networks (electrical/optical) as well as wireless networks: 3G/ 4G, Satellite, WLAN, WiMAX, Ad hoc, Vehicular, Sensor and RFID networks, considering all layers from the physical to the application layer (including middleware and peer-to-peer systems). Furthermore, contributions devoted to the evaluation, optimization, or enhancement of security mechanisms for current technologies as well as novel security and data privacy solutions for emerging technologies are solicited.

Papers should represent high-quality and previously unpublished work, and may not be submitted in parallel to other conferences or publications.

## Topics of Interest

The Communication and Information System Security (CISS) Symposium seeks original contributions in, but not limited to, the following topical areas:

- Access control
- Accounting and auditing
- Anomaly detection
- Botnets identification and mitigation
- Anonymization and privacy in communication networks
- Applied cryptography
- Authentication
- Computer and network forensics
- Critical infrastructure security
- Cloud computing for/with security
- Cross-layer methods for enhancing security
- Deep packet inspection
- Distributed Denial-Of-Service (DDOS) attacks and countermeasures
- Distributed systems security
- Fingerprinting of devices and services
- Flow-based security analysis
- Information hiding and watermarking
- Internet security
- Intrusion detection, localization, and avoidance
- IPv6 and transition security
- Key distribution and managementMalware analysis
- Network Risk Management
- Network forensics
- Network security metrics and performance evaluation
- Peer-to-peer system security
- Privacy-preserving techniques
- Security and privacy in social networks
- Security modeling and protocol design
- Security and privacy policies
- Security of Cyber-physical systems
- Security for RFID
- Security for SCADA Systems
- Self-healing networks
- Sensor network security
- Smart cards and secure hardware
- Social networks security/privacy
- Trust models and trust management
- Vulnerability, exploitation tools, and virus/worm analysis
- Web, e-commerce, m-commerce, and e-mail security
- Wi-Fi, WiMAX security
- Wireless and Mobile networking security