



Call for Papers for *Communication and Information Systems Security Symposium*

SYMPOSIUM CO-CHAIRS:

Xiaodong Lin, University of Guelph, Canada, email: xlin08@uoguelph.ca

Hongwei Li, University of Electronic Science and Technology of China, email: hongweili@uestc.edu.cn

Liang Xiao, Xiamen University, China, email: lxiao@xmu.edu.cn

SCOPE AND MOTIVATION:

Owing to the unprecedented advancements in computation and communication technologies, the cyber-threat landscape has also drastically expanded. On the other hand, the inception of futuristic technologies such as the Internet of Everything, where the low-cost resource-constrained devices are connected through the Internet, is a luring playground for cyberattacks. In today's world, communication and information systems are becoming more indispensable to society and because of that security has become more critical and challenging when many contents, devices, and users get connected to the public Internet. This trend will inevitably continue in the future.

In the wake of such cyber threat landscape and cyberattacks, this symposium welcomes manuscripts on all aspects of the modeling, design, implementation, deployment, and management of security algorithms, protocols, architectures, and systems. Furthermore, contributions devoted to the evaluation, optimization, or enhancement of security and privacy mechanisms for current technologies, as well as devising efficient security and privacy solutions by leveraging futuristic technologies, are solicited. High quality papers reporting on applications of communications theory from both industry and academia are encouraged.

TOPICS OF INTEREST:

The Communication & Information System Security Symposium seeks original contributions in the following topical areas, plus others that are not explicitly listed but are closely related:

- Anonymous communications, metrics, and performance
- Applied cryptography for cyber, information, and network security
- Attack detection and prevention
- Authentication protocols and key management
- Blockchain, cryptocurrencies, markets and finance

- Cellular network security and privacy (5G and beyond)
- Cloud, data center and distributed systems security
- Cyber forensics and threat intelligence
- Edge computing security and privacy
- Emerging technologies and methods for information, cyber, and network security
- Formal trust models, security modeling, and design of secure protocols
- Security and privacy in future Internet
- Firewall technologies
- Operating system and virtual machine security
- Internet of Things security and privacy
- Malware detection and damage recovery
- Security for mobile and wireless networks
- Security and privacy in healthcare systems
- Security in smart grid communications
- Security tools for communication and information systems
- Trust management in networks
- Vehicular cloud and vehicular network security
- Secure applications and testbeds

IMPORTANT DATES:

Deadline for paper submission: 11 October 2021

Date for notification: 18 January 2022

Deadline for final paper submission: 15 February 2022