Communication and Information System Security Symposium

SYMPOSIUM CHAIRS AND CO-CHAIRS

- Bin Xiao, Hong Kong Polytechnic University, Hong Kong. <b.xiao@polyu.edu.hk>
- Cheng Huang, Fudan University, China. <chuang@fudan.edu.cn>
- Nadjib AITSAADI, UVSQ Paris-Saclay University, France. <nadjib.aitsaadi@uvsq.fr>

SCOPE AND MOTIVATION

Continuous advances in computation and communication technologies have led to a rapidly expanding cyber-threat landscape. In today's world, communication and information systems have become increasingly indispensable to society. The growing reliance on communication infrastructure and information systems has been recognized and exploited by cyber attackers. As the scope of content, devices, and users connected to the public internet expands to encompass almost every aspect of day-to-day living, security has become more critical and challenging. This trend will inevitably continue in the future.

Motivated by the challenging cyber threat landscape and the prevalence of cyberattacks, this symposium welcomes top-notch contributions 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 are solicited, as well as those devising efficient security and privacy solutions leveraging futuristic technologies. Top quality papers focusing on applications of communications theory, as well as neighboring fields, in security and privacy from both industry and academia are encouraged.

TOPICS OF INTEREST

Topics of interests for the Communication & Information System Security (CISS) Symposium include, but are not limited to, the following areas:

- Adversarial machine learning
- Artificial intelligence and machine learning for security and privacy
- Security and privacy for artificial intelligence and machine learning
- Attack prediction, detection, response, and prevention
- Authentication protocols and key management
- Anonymous communications
- Biometric secrecy systems and physical unclonable functions (PUFs)
- Blockchain security

- Code constructions for information security and privacy
- Information theoretic security
- Cyber Physical System (CPS) security and privacy
- Formal trust models, security modeling, and the design of secure protocols
- Malware detection and damage recovery
- Physical layer security
- Programmable network security
- Internet-of-Things (IoT) security and privacy
- Cloud, data center and distributed systems security
- Connected and autonomous vehicle security
- Security and privacy for 5G and beyond
- Security and privacy for vehicular networks
- Security for metaverse
- Security in healthcare systems
- Security in smart grid communications
- Security for wireless medical devices
- Security for software defined network (SDN)-based IoT networks
- Security and privacy methods for communication and information systems
- Trust management in networks through emerging technologies
- Emerging technologies and methods for information, cyber, and network security

IMPORTANT DATES

Deadline for paper submission: 1 April 2024

Date for notification: 1 August 2024

Deadline for final paper submission: 1 September 2024

SUBMISSION INSTRUCTIONS

All papers for technical symposia should be submitted via EDAS through the following link:

https://edas.info/N31420.