



IEEE Global Communications Conference

7-11 December 2021 • Madrid, Spain

Connecting Cultures around the Globe

COMMUNICATION AND INFORMATION SYSTEMS SECURITY SYMPOSIUM

SYMPOSIUM CHAIRS AND CO-CHAIRS

Francesco Chiti, University of Florence, francesco.chiti@unifi.it

Abbas Bradai, University of Poitiers, abbas.bradai@univ-poitiers.fr

Chunxiao Jiang, Tsinghua University, jchx@tsinghua.edu.cn

SCOPE AND MOTIVATION

Recent global events pointed out the way communications and information systems are widely involved in our experiences, since contents, users, and devices are interconnected among them through the Internet, so that security is becoming more critical and challenging.

The Communication and Information Systems Security Symposium (CISS) welcomes manuscripts on all aspects of the modeling, design, implementation, deployment, and management of security algorithms, protocols, architectures, and systems. In addition to this, 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 for emerging areas, from physical-layer technology to the application layer, are solicited.

TOPICS OF INTEREST

To ensure complete coverage of the security advances in communication and information systems, this Communication and Information Systems Security (CISS) 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
- Attacks detection and prevention
- Authentication protocols and key management
- Autonomous vehicle security
- Availability and survivability of secure services and systems
- Biometric security: technologies, risks, vulnerabilities, bio-cryptography
- Blockchain, cryptocurrencies, markets and finance
- Cloud, data center and distributed systems security

- Computer and network forensics
- Cryptography for network security
- Crypto economics, incentives and gamification
- Digital rights management
- Edge computing security and privacy
- Firewall technologies
- Formal trust models, security modelling, and design of secure protocols
- Healthcare systems security and privacy
- Internet of Things security and privacy
- Malware detection and damage recovery
- Mobile and wireless network security
- Operating system and virtual machine security
- Secure applications and testbeds
- Security tools for communication and information systems

IMPORTANT DATES

Deadline for paper submission: 15 April 2021

Date for notification: 25 July 2021

Deadline for final paper submission: 1 September 2021

SUBMISSION INSTRUCTIONS

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

<https://edas.info/newPaper.php?c=27482&track=102684>