IEEE Conference on Communications and Network Security
June 10 – 12, 2019//Washington, DC

Call for Papers

The IEEE Conference on Communications and Network Security (CNS) is a premier forum for cyber security researchers, practitioners, policy makers, and users to exchange ideas, techniques and tools, raise awareness, and share experiences related to all practical and theoretical aspects of communications and network security.

The conference seeks submissions from academia, government, and industry presenting novel research results in communications and network security.

Particular topics of interest include, but are not limited to:

- Anonymity and privacy technologies
- Censorship countermeasures and privacy
- Combating cyber-crime (anti-spam, anti-phishing, anti-fraud techniques, etc.)
- Computer and network forensics
- Cyber deterrence strategies
- Game-theoretic security technologies
- Implementation and evaluation of networked security systems
- Information-theoretic security
- Intrusion detection, prevention, and response
- Key management, public key infrastructures, certification, revocation, and authentication
- Malware detection and mitigation
- Security metrics and models
- Physical-layer and cross-layer security technologies
- Security and privacy for big data
- Security and privacy for data and network outsourcing services
- Security and privacy for mobile and wearable devices
- Security and privacy in cellular networks
- Security and privacy in cloud and edge computing
- Internet Security: protocols, standards, measurements
- Security and privacy in crowdsourcing
- Security and privacy in cyber-physical systems
- Security and privacy in emerging wireless technologies and applications (dynamic spectrum sharing, cognitive radio networks, millimeter wave communications, MIMO systems, smart/connected vehicles, UAS, etc.)
- Security and privacy in peer-to-peer and overlay networks
- Security and privacy in WiFi, ad hoc, mesh, sensor, vehicular, body-area, disruption/delay tolerant, and social networks.
- Security and privacy in smart cities, smart and connected health, IoT, and RFID systems
- Security for critical infrastructures (smart grids, transportation systems, etc.)
- Security for future Internet architectures and designs
- Security for software-defined and data center networks
- Security in machine learning
- Social, economic, and policy issues of trust, security, and privacy
- Traffic analysis
- Usable security and privacy
- Web, e-commerce, m-commerce, and e-mail security

Important Dates:

Paper Submission Deadline: December 21, 2018
Notification of Acceptance: February 28, 2019
Final Paper Submission: March 21, 2019

Organizing Committee:

General Chair:
T. Charles Clancy, Virginia Tech, USA

Program Co-Chairs:
Jerry Park, Virginia Tech, USA
Amir Herzberg, University of Connecticut, USA

Accepted and presented technical papers will be published in the 2019 IEEE CNS Proceedings and submitted to IEEE Xplore® as well as other Abstracting and Indexing (A&I) databases. See the website for detailed instructions and submission rules and regulations and for author requirements for accepted papers.