IEEE Conference on Communications and Network Security

25 - 28 September 2022 // Austin, TX (Hybrid)

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**
- **Biometric authentication and identity management**
- **Security and privacy of blockchain and its applications**
- **Censorship countermeasures and privacy**
- **Combating cyber-crime (anti-spam, anti-phishing anti-fraud techniques, etc.)**
- **Computer and network forensics**
- **Cyber deterrence strategies**
- **Data and application security**
- **Data protection and integrity**
- **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, authentication, and access control**
- **Malware detection, prevention, and mitigation**
- **Security metrics and models**
- **Physical-layer and cross-layer security technologies**
- **Security and privacy for big data and machine learning**
- **Security and privacy for data and network outsourcing**
- **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 (CPS)**
- **Security and privacy in Internet of Things (IoT)**
- **Security and privacy in emerging wireless technologies and applications (dynamic spectrum sharing, cognitive radio networks, millimeter wave communications, MIMO systems, RFID, 5G/6G networks, etc.)**
- **Security and privacy in peer-to-peer and overlay networks**
- **Security and privacy in WiFi, ad hoc, mesh, sensor, body-area, and disruption/delay tolerant systems**
- **Security and privacy in smart cities, smart and connected health, and other smart systems/buildings/offices**
- **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 and privacy in connected/autonomous vehicles, UAVs/UAS, drones, etc.**
- **Security and privacy of social networks, metaverse/ virtual/augmented reality-based networks/systems**
- **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**

Due to the COVID-19 situation, the conference organizers kept in mind the safety of all participants and have decided to hold the conference in a hybrid mode. Accepted and presented technical papers will be published in the 2022 IEEE CNS Proceedings and submitted to IEEE Xplore(R) 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.

IMPORTANT DATES

Full Paper Submission Deadline:
20 May 2022
Notification of Acceptance:
15 July 2022
Final Paper Submission:
5 Aug 2022

GENERAL CO-CHAIRs

Haining Wang
(Virginia Tech)
Sencun Zhu
(Pennsylvania State University)

PROGRAM CO-CHAIRS

Selcuk Uluagac
(Florida International University)
Ming Li
(University of Arizona)

For more information, visit http://cns2022.ieee-cns.org/