Important Dates

Deadline for poster submission: **~~March 5, 2018~~; March 16, 2018**
Notification to authors: **March 26, 2018**
Camera-ready version: **April 2, 2018**

Scope

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.

Building on the success of the past years' conferences, IEEE CNS 2018 welcomes poster submissions to be presented during the conference. A poster submission should be a 2-page abstract, which summarizes the key merits of proposed ideas, presents initial results, and identifies challenges to develop a complete solution. Poster submissions will be evaluated by the Posters Session Committee based on the novelty and the potential to stimulate discussions and promote collaborations. Posters should be submitted via EDAS at https://edas.info/N24385. Please follow the same template for regular conference papers available on http://cns2018.ieee-cns.org/submission-instructions.

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

- Anonymity and privacy technologies
- Biometric authentication and identity management
- 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, and authentication
- Location privacy
- Malware detection and mitigation
- Physical-layer and cross-layer security technologies
- Security metrics and models
- 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
- Security and privacy in crowdsourcing
- Security and privacy in emerging wireless technologies (dynamic spectrum sharing, cognitive radio networks, millimeter wave communications, MIMO systems, 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
- 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

The conference will arrange the poster session in a room where the posters can be displayed. An accepted poster must be presented by an author in the poster session to interested attendees. The abstract of the accepted posters will appear in the conference proceeding and be submitted to IEEE Xplore. Each accepted poster requires an author to register for the conference at the appropriate rate based on the membership level. Each author registration can cover up to three posters or papers of the conference, but each poster must have a dedicated presenter at the session.

A Best Poster Award will be given based on the poster's novelty and potentials in research. The quality of presentation and the interaction during the session will also be important criteria. The award will be announced in a plenary session of the main conference.

Poster Chairs

- **Sara Foresti**, Università degli Studi di Milano, Italy
- **Chunyi Peng**, Purdue University, USA