CALL FOR POSTERS

Third IEEE Conference on Communications and Network Security (CNS 2016) Philadelphia, USA, October 17-19, 2016
http://www.ieee-cns.org

IMPORTANT DATES

- 2-page Abstract Due by (extended): ~~**July 15, 2016 11:59pm**~~ **July 22, 2016 11:59pm**
- Notification of Acceptance: **August 1st, 2016**
- Final Abstract Due: **August 12, 2016**

SCOPE

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

Building on the success of the past three years' conferences, IEEE CNS 2016 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. Abstracts will be evaluated by the Posters Session Committee based on the novelty and the potential to stimulate discussions and promote collaborations. Poster abstracts should be submitted via EDAS at http://edas.info/N22693. Please follow the same template for regular conference papers available on http://www.ieee-cns.org. Sample topics of interest include but are not limited to:

- Anonymization and privacy in communication systems
- Biometric authentication and identity management
- Computer and network forensics
- Data and application security
- Data protection and integrity
- Availability of communications, survivability of networks in the presence of attacks
- Key management and PKI for networks
- Information-theoretic security
- Intrusion detection and prevention
- Location privacy
- Mobile security
- Outsourcing of network and data communication services
- Physical layer security methods, cross-layer methods for enhancing security
- Secure routing, network management
- Security for critical infrastructures
- Security metrics and performance evaluation
- Security and privacy for big data
- Security and privacy in body area networks
- Security and privacy in content delivery network
- Security and privacy in cloud computing and federated cloud
- Security and privacy in crowdsourcing
- Security and privacy in the Internet of Things

- Security and privacy in multi-hop wireless networks: ad hoc, mesh, sensor, vehicular and RFID networks
- Security and privacy in peer-to-peer networks and overlay networks
- Security and privacy in single-hop wireless networks: Wi-Fi, Wi-Max
- Security and privacy in smart grid, cognitive radio networks, and disruption/delay tolerant networks
- Security and privacy in social networks
- Security and privacy in pervasive and ubiquitous computing
- Social, economic, and policy issues of trust, security, and privacy
- Traffic analysis
- Usable security for networked computer systems
- Vulnerability, exploitation tools, malware, botnet, DDoS attacks
- 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 proceedings 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.