Call for Articles for Computer Communications, Elsevier (IF: 1.079)

http://www.journals.elsevier.com/computer-communications/

COMCOM seeks submissions for a special issue on

Security and Privacy in Unified Communications: Challenges and Solutions

Unified Communications (UC) merge different communication technologies, types of products, and services, from various manufacturers, operators, and countries, following diverse policies and standards. Specifically, in the context of UC, a range of communication tools are integrated in a way that both corporations and individuals are able to manage all their communications in one entity instead of doing it disjointly. It is therefore said that UC bridges the opening between the various computer related communication technologies and Voice over IP (VoIP). However, this high level of heterogeneity expands the risks related to security and privacy that stakeholders should deal with. To eliminate or even prevent the increasing threats to end-users and operators, it is important to explore this growing and timely research topic.

This feature topic will benefit the research community towards identifying challenges and disseminating the latest methodologies and solutions to UC security and privacy issues. Its objective is to publish high-quality articles presenting open issues, algorithms, protocols, policies, frameworks, standards, and solutions for UC related to security and privacy. Only technical papers describing previously unpublished, original, state-of-the-art research, and not currently under review by a conference or a journal will be considered. Reviews and case studies which address state-of-art research and state-of-practice industry experiences are also welcomed. We solicit papers in a variety of topics related to unified communications security and privacy, including, but not limited to:

- Authorization and access control for UC services
- Denial of service prevention schemes for UC
- Reliability and availability issues on UC
- Penetration testing, intrusion detection and prevention
- End-to-end security solutions
- Cryptographic protocols for UC
- Voice security
- Signaling security and privacy
- Multimedia application security and privacy analysis
- Multimedia communication platforms vulnerabilities and attacks
- Security and privacy in mobile communication services
- Smartphone multimedia apps security and privacy
- Social networking security and privacy
- Testbed and case studies for secure and private UC services
- Trust establishment in UC
- IP Multimedia Subsystem (IMS) security
- Privacy and identity management
- Privacy enhancing technologies for UC
- Privacy models for UC
- Security and privacy assessment for UC
- Security policies
- Auditing, verification, and validation of UC services
- Risk analysis and management
- Cyber-security issues affecting UC
- Protection of UC as a Critical Information Infrastructure
- VoIP peering security issues

All received submissions will be sent out for peer review by at least two experts in the field and evaluated with respect to relevance to the special issue, level of innovation, depth of contributions, and quality of presentation. The guest editors will make an initial determination of the suitability and scope of all submissions. Papers that either lack originality, clarity in presentation or fall outside the scope of the special issue will not be sent for review and the authors will be promptly informed in such cases. Submitted papers must not be under consideration by any other journal or publication.

Schedule

Manuscript Due: **October 31, 2014**
Pre-notification (first round): January 30, 2015
Final-notification (second round): April 3, 2015
Publication of special issue: 2015 (tentative)

Submission Procedure

Authors should follow the instructions available at http://ees.elsevier.com/comcom - kindly click the "Guide for Authors" link in the top box on the right side. When submitting the article, select "UC Security and Privacy" in the "Select an Article Type" box in the submission process.

Guest Editors

Georgios Karopoulos (corresponding guest editor)
Critical Infrastructure Protection Unit, European Commission's Joint Research Centre (JRC)
Ispra, Italy, email: georgios.karopoulos@jrc.ec.europa.eu

Georgios Portokalidis
Computer Science Dept., Stevens Institute of Technology
New Jersey, USA, email: gportoka@stevens.edu

Josep Domingo-Ferrer
Dept. of Computer Engineering and Maths, Universitat Rovira i Virgili
Tarragona, Catalonia, email: josep.domingo@urv.cat

Ying-Dar Lin
Dept. of Computer Science, National Chiao Tung University (NCTU)
Hsinchu,Taiwan, email: ydlin@cs.nctu.edu.tw

Dimitris Geneiatakis
Digital Citizen Security Unit, European Commission's Joint Research Centre (JRC)
Ispra, Italy, email: dimitrios.geneiatakis@jrc.ec.europa.eu4

Georgios Kambourakis
Dept. of Information and Communication Systems Engineering, University of the Aegean
Samos, Greece, email: gkamb@aegean.gr