Special Issue on
Security in a Completely Interconnected World
Security and Communication Networks Journal

Scope

The convergence of multiple paradigms, visions, and technologies – Internet of Things (IoT), People (IoP) and Services (IoS); Ambient Intelligence (AmI); Machine-to-Machine (M2M); and many others – is giving birth to a completely interconnected world. In this world, every entity (be it a machine, a daily object, a person, or anything) can have a globally locatable, addressable, and readable virtual counterpart, which can collaborate with each other in the provisioning of various services. This concept is slowly becoming a reality: specific standards are being developed, new research results are being obtained, and novel services are being provided by both newborn start-ups and experienced companies in various areas (e.g., SCADA systems, smart grids, smart cities). However, several significant obstacles hinder the full implementation of this concept, and among them are the security issues. In fact, as there is already a parallel economy exploiting the foundational weaknesses of the Internet, this new environment will surely be targeted by original and ingenious malicious models. The challenge here is to prevent the growth of such models or at least to mitigate and limit their impact. Therefore, it is necessary to provide strong foundations to those paradigms that require it (such as IoT), and develop various robust and resilient security mechanisms that allow the secure interaction between entities even in restrictive contexts. Precisely, the goal of this special issue is to publish cutting-edge research results and innovation case studies that will help to set the security foundations of this new interconnected world.

Topics of Interest

In terms of security challenges, topics of interest include but are not limited to:

- Novel security problems and challenges.
- Privacy risks and data management problems.
- Identifying, authenticating, and authorizing entities.
- Development of trust frameworks for secure collaboration.
- Cryptographic primitives and algorithms for constrained devices.
- Secure connection of heterogeneous ecosystems and technologies.
- Legal challenges and governance issues.
- Fault tolerance and resilience to external and internal attacks.
- Context-Aware security.
- Security of cloud-based M2M/IoT platforms.
- Distributed policy enforcement and rights management.
- Usability of security and privacy technologies.
- Security in social interactions between virtual entities.

Submission

Papers must represent high-quality and previously unpublished works. Original research papers are solicited in all relevant areas (IoT, M2M, etc) on the topic of security for the completely interconnected world. All submissions will be peer reviewed by at least three experts working in the areas. The guidelines for prospective

authors can be found at http://www.interscience.wiley.com/journal/security). Prospective authors should submit their papers online at http://mc.manuscriptcentral.com/scn. When submitting the papers, the authors should make sure to choose the Manuscript type as 'Special Issue', enter the 'Running Head' as 'SCN-SI-049', and the 'Special Issue title' as and '**Security in a Completely Interconnected World**', respectively. Failure to do so may be subject to rejection without review.

Guest Editors

Jim Clarke
Waterford Institute of Technology, Ireland
E-mail: jclarke@tssg.org

Stefanos Gritzalis
University of the Aegean, Greece
E-mail: sgritz@aegean.gr

Rodrigo Roman
Institute for Infocomm Research, Singapore
E-mail: rroman@i2r.a-star.edu.sg

Jianying Zhou
Institute for Infocomm Research, Singapore
E-mail: jyzhou@i2r.a-star.edu.sg

Important Dates

Manuscript due	15th October 2012 (extended)
First Review Phase Results	January 2013
Final Acceptance Notification	March 2013
Camera Ready Manuscript due	April 2013
Publication	The 2nd half of 2013 (Tentative)