Security and Communication Networks

Special Issue on

Emerging and Unconventional: New Attacks and Innovative Detection Techniques

CALL FOR PAPERS

In the last years, advancements of the information and communication technologies have spawned a variety of innovative paradigms, such as cloud and fog computing, the Internet of Things (IoT), or complex vehicle-to-vehicle frameworks. As a consequence, the cybersecurity panorama is now getting populated with complex, emerging, and unconventional attacks, which require deep investigation and proper understanding. For example, the diffusion of online social networks brought social engineering to the next level, while IoT led to a completely new set of hazards also endangering the user at a physical level. Modern threats also exploit a variety of advanced methods to increase their stealthiness in order to remain unnoticed for long periods, as well as reduce the effectiveness of many digital forensics techniques and detection tools.

Therefore, new and emerging technologies changed the modern cybersecurity landscape, which nowadays is populated by novel attacks and also requires innovative detection and prevention methods. In this perspective, the special issue aims at investigating the most advanced and innovative forms of attacks and scenarios, for instance, considering automotive or building automation settings. To complete the picture, a relevant attention will be given to works dealing with innovative forms of detection and forensics analysis, which are mandatory to counteract sophisticated malware able to hide or take advantage of unconventional and complex scenarios. This issue accepts high quality papers containing novel original research results and review articles of exceptional merit covering the most cutting-edge cybersecurity threats and countermeasures.

Potential topics include but are not limited to the following:

- Novel advanced and persistent threats aiming at automotive and smart buildings/cities
- Security issues and profiling hazards in smart buildings/cities
- IoT and device specific attacks, for example, battery drain attacks or attacks on IoT routing protocols
- Hazards taking advantage from social media, for example, social bots and new social engineering attacks
- Information hiding threats to counteract forensics tools and analysis
- Network steganography for data exfiltration and new information-hiding-capable threats
- Energy-based detection of slow and hidden attacks, including low-attention rising threats for mobile and handheld devices
- Scalable countermeasures for preventing steganography in big-data-like sources
- Novel threats targeting vehicles and cloud and software defined networking technologies
- Bioinspired attacks and detection mechanisms
- Ransomware: novel trends, characteristics, and detection
- Moving Target Defense (MTD) solutions against infections

Authors can submit their manuscripts through the Manuscript Tracking System at http://mts.hindawi.com/submit/journals/scn/emun/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Luca Caviglione, National Research Council of Italy (CNR), Genoa, Italy
luca.caviglione@ge.issia.cnr.it

Guest Editors
Wojciech Mazurczyk, Warsaw University of Technology, Warsaw, Poland
wmazurczyk@cygnus.tele.pw.edu.pl

Steffen Wendzel, Worms University of Applied Sciences, Worms, Germany
wendzel@hs-worms.de

Sebastian Zander, Murdoch University, Perth, Australia
s.zander@murdoch.edu.au

Submission Deadline
Friday, 27 October 2017

Publication Date
March 2018