Hindawi
Security and Communication Networks
Volume 2018, Article ID 9672523, 1 page
https://doi.org/10.1155/2018/9672523

Editorial

Emerging and Unconventional: New Attacks and Innovative Detection Techniques

Luca Caviglione,[1] **Wojciech Mazurczyk**,[2] **Steffen Wendzel**,[3] **and Sebastian Zander**[4]

[1] *National Research Council of Italy, Genoa, Italy*
[2] *Warsaw University of Technology, Warsaw, Poland*
[3] *Worms University of Applied Sciences, Worms, Germany*
[4] *Murdoch University, Perth, WA, Australia*

Correspondence should be addressed to Luca Caviglione; luca.caviglione@ge.issia.cnr.it

Received 21 March 2018; Accepted 22 March 2018; Published 26 April 2018

Nowadays, security must face new and challenging scenarios, for instance, those exploiting cloud and fog computing, the Internet of Things (IoT), or complex frameworks for orchestrating botnets. Therefore, new attacks and innovative countermeasures should be investigated and this special issue focuses on how advancements provided by information and communication technologies influence modern cyberinfrastructures.

We received several high-quality submissions containing novel original research results. After a thorough review process, we accepted six articles that can be grouped into three different areas, each one offering insights on emerging and unconventional threats and detection techniques.

The first area deals with information hiding and covert channels, which are important aspects as many modern threats exploit a variety of methods to increase their stealthiness for remaining unnoticed for long periods or for limiting the efficiency of digital forensics techniques and detection tools. In this perspective, the article entitled "Leveraging KVM Events to Detect Cache-Based Side Channel Attacks in a Virtualization Environment" focuses on securing a virtualization environment by introducing a novel approach to detect covert communication attempts. Besides, the article entitled "Detecting Web-Based Botnets Using Bot Communication Traffic Features" introduces two metrics for the detection of command and control servers orchestrating botnets by means of HTTP commands and Webpages.

Detection is the second area. Novel forms of detection are mandatory to counteract sophisticated malware or to perform traffic analysis in emerging and complex scenarios. In this case, the article entitled "Leverage Website Favicon to Detect Phishing Websites" proposes a way to exploit favicon to reveal the identity of a Website and mitigate phishing attacks. Moreover, the article "Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders" discusses how to approach the problem of automatically and efficiently extracting features from large amounts of unlabeled raw network traffic data using deep learning approaches.

The last area covered by this special issue deals with IoT and modern, interconnected, and smart systems. The article entitled "Remotely Exploiting AT Command Attacks on ZigBee Networks" addresses an IoT scenario and showcases how to remotely exploit AT commands to attack sensors. Lastly, the article entitled "Predictive Abuse Detection for a PLC Smart Lighting Network Based on Automatically Created Models of Exponential Smoothing" investigates statistical models to detect attacks targeting smart lighting infrastructures.

Summing up, we think that this special issue will improve the understanding of how modern communication and computing frameworks can be exploited and how they can be secured.

Acknowledgments

We would like to thank all the reviewers for reviewing the articles submitted to the special issue.

Luca Caviglione
Wojciech Mazurczyk
Steffen Wendzel
Sebastian Zander