EAI Endorsed Transactions
on Security and Safety

Editorial **EAI.EU**

Vulnerability Analysis, Intrusion Detection and Privacy Preservation of Modern Communication Systems

Dr. Sencun Zhu[1], Dr. Kevin Jones[2] and Dr. Leandros A. Maglaras[3]

[1]The Pennsylvania State University
[2]Airbus Group
[3]De Montfort University

Received on 27 December 2017, published on 28 December 2017

doi: 10.4108/eai.28-12-2017.153514

1. Editorial

The second issue of the fourth volume of the EAI transactions on Security and Safety provides an insight to methods and techniques that improve security, safety and privacy of modern systems, such as Software-Defined Systems (SDNs), Cognitive radio networks (CRNs) or 802.11wireless networks. The articles that constitute this issue can be divided into two main classes. The first one consists of novel methods that can strengthen either intrusion detection or encryption capabilities of the system under consideration, while the second one is based on the analysis of collected data from different wireless access points in order to reveal vulnerabilities and security level of the providers. In particular, in the area of novel security and privacy methods the issue presents (i) a deep learning based DDoS detection system for multi-vector attack detection in an SDN environment, (ii) an adaptive parameter and component selection mechanism for online anomaly detection problem in CRNs (iii) a compact homomorphic symmetric encryption scheme based on learning with errors (LWE) principle. In the area of the data collection and analysis study, the issue presents an overview of the security level of wireless networks in Romania.

In article A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN) by Quamar Niyaz, Weiqing Sun and Ahmad Y. Javaid, authors try to address the Distributed Denial of Service (DDoS) attack, which is one of the most prevalent attacks that an organizational network infrastructure faces nowadays. The article focuses on SDNs, where attacks can occur either on the data plane or control plane. For that reason authors implement a DDoS detection system as a network application in SDN to handle attacks for both cases. The proposed system is evaluated using collected network traffic from a real network and a private network testbed. It identifies individual DDoS attack class with an accuracy of 95.65% and can be used as a basis for a NIDS system that can cope with different kinds of attacks.

In article Exploration of Singular Spectrum Analysis for Online Anomaly Detection in CRNs, by Qi Dong, Zekun Yang, Yu Chen, Xiaohua Li and Kai Zeng, authors try to deal with attacks that happen in CRNs, which due to being unregulated wireless network environments, are susceptible to various malicious entities. In CRNs, an “anomaly situation” can be caused by various malicious activities as well as by versatile unpredictable (licensed/primary) PU activities, both of which can cause degradation on link quality of CRNs and the detection of which must happen without imposing too much overhead to cognitive entities. The current article introduces an adaptive parameter and component selection mechanism based on the SSA method, upon which it built up a sliding window online anomaly detector in CRNs. The proposed online method is evaluated against two anomalies, namely the primary user emulation (PUE) attack and the PU abnormality but it can be used for many other anomaly detections, such as spectrum sensing data falsification (SSDF) and jamming, since those anomaly activities inevitably deteriorate communication condition of CRNs.

In article Compact lossy and all-but-one trapdoor functions from lattice by Leixiao Cheng, Quanshui Wu and Yunlei Zhao, authors deal with lossy trapdoor functions (LTDF) and all-but-one trapdoor functions (ABO-TDF). Based on recent advances on in quantum computing, authors state that it is desirable to develop new and improved lattice-based LTDF and ABO-TDF. The current article provides improved and more compact constructions of LTDF and ABO-TDF based on the LWE problem that can be used for black-box constructions of many primitives and cryptosystems.

Finally in article Overview of Romania 802.11Wireless Security & Statistics, by Cristian Liviu Leca, author collected statistically significant data from representative areas of Romania in order to have an objective overview of the wireless security situation in Romania. Based on the analysis of more than 100000 unique wireless networks gathered in Bucharest, major urban areas and the surrounding rural areas author tries to answer several questions regarding the current level of security of wireless networks that exist in Romania and the existence known vulnerabilities in public and private wireless networks in Romania. Two basic conclusions from this study are (1) wireless security situation has improved in Romania consequently being now at level with world statistics and (2) security situation of provider wireless networks is shown to be significantly better than that of private networks.

The topics treated in the aforementioned articles come to confirm that the area of security and privacy of systems and networks is an ever evolving field of research and study. New attacks that try to exploit vulnerabilities of novel systems and architectures, e.g. SDNs or CRNs, demand the implementation of novel methods that must be both efficient, fast and impose low overhead in system’s performance. Moreover modern IDSs need to be combined with other detection methods in order to be more efficient, use ensemble-based approaches in order to be able to detect various kinds of attacks and be accompanied by deep learning methods in order to catch attacks that pass undetected from traditional network flow analysis techniques.