Annals of Telecommunications (2019) 74:123–124
https://doi.org/10.1007/s12243-019-00706-w

EDITORIAL

Cybersecurity in networking

Rida Khatoun[1] · Diogo Menezes Ferrazani Mattos[2] · Otto Carlos Muniz Bandeira Duarte[3]

Published online: 11 March 2019

Today, the pervasive use of the communication technologies in various systems and domains such as the Intelligent Transportation System (ITS), the Industrial Supervisory and Control Systems (SCADA), social networks, financial networks, and connected objects continues to improve the quality of human life. However, the strong dependency of these infrastructures on information and communication technologies, as well as their connectivity to the Internet, makes them increasingly vulnerable to sorts of threats that can fatally impact on economic and societal dimensions. Besides, traditional cybersecurity platforms, protocols, and measures are not efficient enough especially in virtualized, heterogeneous, and critical environments. The primary objective of this special issue is to address various research issues related to the cybersecurity and protection of smart infrastructures. This special issue discusses some of these challenges. The papers of this issue cover a wide range of topics from new security threats to cloud computing until new approaches for applying addictive homomorphic cryptography.

After a thorough reviewing process where at least two experts have evaluated every paper, seven papers have been accepted for this special issue. Reviewers' comments were constructive first to select the most significant contributions as well as to improve the content, quality, and presentation of the accepted papers. Hereafter, we provide a summary of each paper in this special issue.

The first one from André Nasserala and his colleagues is entitled "Cache nFace: a Simple Countermeasure for the Producer-Consumer Collusion Attack in Named Data Networking." In the paper, the authors address the collusion attacks in the new network architecture of Named Data Networking (NDN). Their proposal focuses on mitigating the effect of collusion attacks that generate high rates of content requests, which creates fake content popularity on the network. The key idea is to divide the cache on each node into subcaches for each interface of the node. The results show that the proposal reduces up to 50% the effectiveness of the attack.

The second paper from Martin Andreoni and his colleagues is proposing an "A Fast Unsupervised Preprocessing Method for Network Monitoring." The authors identify network administrators usually neglect zero-days threats until a large number of attacks occurs. The authors claim that countermeasures have to be applied as soon as possible to reduce the impacts of networking attacks. Thus, network protection mechanisms should fast processes flow. The paper proposes a fast preprocessing method to prepare network flows to classification algorithms. The key idea is to use zero previous knowledge about the flows to select which are the best features to be processed to a machine learning classification algorithm. The authors show that the proposal enhances up to 11% of the classification accuracy and implies a 100-fold reduction of the processing time.

The following from Katarzyna Kapusta and her colleagues is entitled "Additively Homomorphic Encryption and Fragmentation Scheme for Data Aggregation inside Unattended Wireless Sensor Networks." In this paper, the authors address the confidentiality and the availability of Unattended Wireless Sensor Network through the application of additively homomorphic encryption and fragmentation scheme. Their proposal, when compared with the state-of-art techniques on homomorphic encryption, reduces at a half part the volume of stored data in sensors. Storing low amount of data in sensors, the proposal supports the adoption of lower transmission costs and allows sensors to save battery.

The fourth paper from Renato S. Silva and Luís F. M. de Moraes proposes "A Cooperative Approach with Improved Performance for a Global Intrusion Detection Systems for Internet Service Providers." The authors claim that Internet Service Providers may be induced to take incorrect countermeasures to protect their subscribers against attacks due to classification errors of their perimeter-based Intrusion Detection Systems. Therefore, the paper proposes a global

✉ Rida Khatoun
rida.khatoun@telecom-paristech.fr

[1] Telecom ParisTech, Paris, France

[2] UFF, Niterói, Brazil

[3] UFRJ, Rio de Janeiro, Brazil

intrusion detection system based on a cooperative federation of distributed autonomous intrusion detection elements. Each element propagates alarms of potential threats through BGP messages. The results show that the proposal enhances the whole system accuracy to detect attacks.

The next paper from Mohit Gupta and Narendra S. Chaudhari is dealing with "Anonymous roaming authentication protocol for wireless network with backward unlinkability and natural revocation." The authors decouple identification and authentication and, thus, they propose that a mobile device authenticates in a foreign server using a two-party authentication protocol based on group signature. Their proposal introduces backward unlinkability to natural user revocation without periodic updates. The paper proves that the proposed protocol is secure under a random oracle model.

The sixth paper from Romain Laborde and his colleagues presents "A situation-driven framework for dynamic security management." The key idea of this paper is to represent security policies according to situations since situation-based policies express dynamic security measures that would be complex or even impossible to convey with access control lists or role-based access controls. The authors develop a modular framework and present two real experiments.

The last paper from Mohammad-Mahdi Bazm and his colleagues is entitled "Isolation in Cloud Computing Infrastructures: New Security Challenges." The authors review the threats on cloud computing, and they identify that isolation is the core security challenge, since sharing physical resources is subject to side-channel attacks. Moreover, the paper conceptualizes the problem of distributed side-channel attacks, discusses how these attacks threaten cloud computing infrastructures, and summarizes a set of countermeasures to be applied to these infrastructures.

Acknowledgments The guest editors would like to express their deep appreciation to the editor-in-chief, Prof. Guy Pujolle, for giving them the opportunity to publish this special issue. The guest editors also thank the managing editor, Alexia Kappelmann as well as the journal editorial staff for their continuous support during the process of this publication. Last, the guest editors would like to express their thanks to all the authors for submitting quality articles and the reviewers for helping in the selection of papers and improving the accepted papers.