Annals of Telecommunications (2023) 78:133–134
https://doi.org/10.1007/s12243-023-00956-9

EDITORIAL

Cybersecurity in networking: adaptations, investigation, attacks, and countermeasures

Ahmad Samer Wazan[1] · **Frédéric Cuppens**[2]

Published online: 14 March 2023

Networks and IT systems play a vital role in our daily life. We use these systems for unlimited number of activities such as social networks and business management or for conducting our research activities. However, the usage of these services can come with a cost: the security of our information which is defined by the security offered by these systems. Attackers are constantly finding and exploiting vulnerabilities in these systems which are becoming increasingly complex. This complexity poses significant challenges to the defenders who need to make tremendous efforts to identify the vulnerabilities of these systems and to close them on time.

To address some of these challenges, our special issue featured a set of research works that handle different topics in cybersecurity, including forensic and investigation, attacks and countermeasures, and the adaptation of blockchains consensus protocols for mobile ad hoc networks (MANETs). We received 11 submissions, from which we accepted 5 papers that address important challenges in their respective areas and propose relevant solutions. Each paper underwent at least two reviews and passed through multiple rounds of reviews.

Three of the accepted papers in our special issue handle topics related to AI and blockchain. It should not be surprising because AI and blockchain have reshaped many aspects of the Internet. Blockchains, with their decentralized ledger, provide a unique business model without intermediaries, while AI, particularly with the large language models (LLM), causes fundamental changes in many sectors, including cybersecurity.

The first accepted paper, titled "Mitigation of a poisoning attack in federated learning by using historical distance detection" falls in the area of AI and handles a critical topic related to machine learning methods. Specifically, the paper discusses the method of federating learning that allows training AI models while respecting users' privacy. The authors show that while this learning method is appealing because users can train models using their local data on their own devices, malicious clients can cause integrity and availability threats by interfering with the global model. The authors have illustrated their idea through a scenario in which multiple clients can launch a poisoning attack against a central server. Inspired by the evolutionary clustering method, the authors have developed a defense mechanism to mitigate the integrity and availability threats. Their scheme has also been experimented with different other scenarios.

The second accepted paper, titled "Multipath neural networks for anomaly detection in cyber-physical systems" also falls in the area of AI. The objective of this paper is to enhance the security of model-based Intrusion Detection Systems (IDSs). The authors focus on the authenticity of the anomaly detection model. They use a new type of neural network called multipath neural network to define a confidence measure. They also use the Wilcoxon-Mann–Whitney (WMW) test to detect any unusual change in the distribution of this measure, which allows them to feature the authentic aspect of the detection model.

The paper titled "A performance evaluation of C4M consensus algorithm" proposes adapting the consensus protocols used in blockchains to the mobile ad hoc networks (MANETs) to handle the network partition problem. The challenges raised in this paper are the adaptation of consensus protocols of blockchains MANETs where nodes are communicating in an unreliable way in contrast to blockchains that are designed to work on a reliable and fully connected network. The authors propose a new consensus algorithm called Consensus for Mesh (C4M) that can be used for MANETs. The simulation results obtained from NS-3 show encouraging results obtained from C4M algorithms. The authors outline the need to test their algorithm

✉ Ahmad Samer Wazan
ahmad.wazan@zu.ac.ae

[1] CTI College, Zayed University, Abu Dhabi, United Arab Emirates

[2] Polytechnique Montréal, Montréal, Canada

with other mobility scenarios different from the one used in the simulation.

The fourth accepted paper in this special issue covers the area of forensic and investigation. The paper handles the relevant topic related to the security of videoconferencing applications that became very popular during the COVID-19 pandemic. The authors provide a detailed analysis of the Cisco WebEx Application by extracting a set of artifacts collected from the Cisco WebEX desktop client, web, and Android application. For example, the authors could extract user credentials, emails, user IDs, chat messages, and other confidential information such as meeting passwords or AES keys.

Finally, the last accepted paper handles the security of embedded devices. The authors propose a novel approach that can allow an attacker to get information about the firmware instructions by sniffing unencrypted incremental updates. The authors analyze two types of incremental code updates. They demonstrate that attacks can happen with both types of updates, such as return-oriented programming (ROP) attacks. The authors discussed also different countermeasures that need to be evaluated and enhanced in the future.

Our special issue covers various topics in the cybersecurity area. We hope that the knowledge provided in this special issue will give valuable insights for the cybersecurity community that can help improve human life and society.

Finally, we would like to thank all the authors who submitted their work to this special issue. We also express our gratitude to the volunteer reviewers who carefully read and analyzed the various submissions. Without their help and commitment, this special issue would not have been possible. We appreciate their expertise and dedication to advance research in the field of cybersecurity.