Journal of Computer Virology and Hacking Techniques (2022) 18:69–70
https://doi.org/10.1007/s11416-021-00403-0

EDITORIAL

Editorial

Special Issue: Iranian Research in Information and System Security

Babak Sadeghiyan[1] · Salman Niksefat[2]

Published online: 7 January 2022

Guest Editors: Babak Sadeghiyan and Salman Niksefat

This special issue of the *Journal of Computer Virology and Hacking Techniques* includes some works of Iranian researchers on both fundamental and applied problems in information and computer system security.

The aim of this special issue is to promote the Iranian research in the field within the international scientific community. The scope of the special issue was announced to cover all aspects of Information and System Security, dealing with operational as well as formal and theoretical aspects of information security systems. Moreover, all technical elements for cyber security, as well as security issues in emerging technologies, were announced to be of interest.

Upon the announcement of the special issue in late April 2020, 15 manuscripts were submitted.

For the first round of reviewing process, 85 reviews were solicited on the manuscripts, while 46 reviews were invited from international scientific community and 39 reviews were invited from Iranian domestic academic community. As the first decisions results, 5 Manuscripts were Rejected, 5 were required Major Revisions and 5 were Accepted with Minor Revisions.

This special issue includes 10 papers on different topics of the announced scope.

The subject field of the accepted papers can roughly be categorized into 4 groups. Three papers on Malware, two papers on Vulnerability, two papers in Cryptology, and three papers on different security issues of computer systems. The research objective of the accepted papers can be categorized into: no papers as hypothesis making/verification, 5 papers as analysis/investigating the factors, no papers as comparison, and 5 papers as designing.

It can be concluded that the accepted papers are either on Design or on Analysis related issues.

The article titled "*Android Malware Classification Using Convolutional Neural Network and LSTM* " presents a classification process for Android malware by analyzing both the source codes and the applications using Call-Graph and generating call-graphs for both classes.dex and lib.so files. The proposed method of classification is CNN-LSTM, where a sequential neural network is designed for malware detection. Then, the proposed method is compared with several other classification methods such as CNN, SVM, Naive Bayes, Random Forest, etc. The obtained experimental results show its more effectiveness, efficiency, and reliability. (Malware, Design)

The article titled "*A Novel Method for Malware Detection Based on Hardware Events Using Deep Neural Networks*" presents a dynamic malware detection method which utilizes hardware events during file execution as features of the classification model. Then, two Deep Neural Network (DNN) based algorithms are used to construct the machine learning model. A voting network is used between the outputs of CNNs and the LSTM network to determine the label of the suspicious sample. The experimental results show that the design can be effective in detecting new malware. (Malware, Design)

The article titled "*MARKHOR: Malware Detection Using Fuzzy Similarity of System Call Dependency Sequences*" presents a dynamic and behavior-based malware detection approach, which is called Markhor. It uses system call data dependency and system call control dependency sequences to create a weighted list of malicious patterns. The list is then used to determine the malicious processes. The similarity of a file system call sequences to a malicious pattern is extracted with a fuzzy algorithm. The efficiency of Markhor is exper-

✉ Babak Sadeghiyan
basadegh@aut.ac.ir

Salman Niksefat
niksefat@aut.ac.ir

[1] The Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

[2] APA Research Center, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

imentally evaluated in terms of its accuracy, precision, and F-Measure. (Malware, Design)

The article titled "*A Generalized Framework for Accelerating Exhaustive Search Utilizing Deterministic Related-key Differential Characteristics*" describes a framework for utilizing several deterministic related-key differential distinguishers. The connection between some deterministic related-key properties and the security of cryptographic primitives in the single-key model is described. It presents a unified methodology to evaluate the security of several well-known cipher constructions. (Cryptology, Analysis)

The article titled "*Zipf's Law Analysis on the Leaked Iranian Users' Passwords*" deals with the analysis of five datasets of the leaked passwords of Iranian users, and examines the existence of Zipf's law on them using three different approaches. It investigates their differences from the passwords of English speaking users, in terms of their length and the combination of characters. The robustness of the leaked Iranians' passwords to statistical guessing attacks has also been measured. (Computer Security, Analysis)

The article titled "*Covert Timing Channels: Analyzing WEB Traffic*" studies the effect of using different features (or levels) of HTTP protocol on identifying a covert timing channel. An entropy-based method for analyzing covert timing channel is used, and the sensitivity of various parameters affecting invisibility is examined. The impact of analyzer's level and the effect of increased intentional noise on channel invisibility have been shown experimentally. A new parameter called the relative position of covert channel and analyzer is considered. It is concluded that an analyzer must investigate the traffic at all possible levels. (Computer Security, Analysis)

The article titled "*On Delegatability of MDVS Schemes*" studies all multi-designated verifier signature (MDVS) schemes proposed up to now and shows that all of them are delegatable with proposing delegatability attacks on all MDVS schemes. The paper addresses a new open problem that is proposing MDVS schemes which satisfy the non-delegatability as well as the basic security requirements. (Cryptology, Analysis)

The article titled "*Understanding Linux Kernel Vulnerabilities*" reports on the analysis of 1,858 Linux kernel vulnerabilities covering a period of Jan 2010-Jan 2020. The vulnerabilities are classified from the attacker's view using various criteria such as the attacker's objective, the targeted subsystems of the kernel, the location from which vulnerabilities can be exploited (i.e., locally or remotely), the impact of the attack on confidentiality, system integrity and availability, and the complexity level associated with exploiting vulnerabilities. The analysis indicates the presence of a large number of low-complexity vulnerabilities. The paper concludes that most of the vulnerabilities can be exploited from a local system, leading to attacks that can severely compromise the kernel quality of service, and allow attackers to gain privileged access. (Vulnerability, Analysis)

The article titled "*Cross-VM Cache Attacks on Camellia*" demonstrates that the Camellia implementations of OpenSSL 1.1.0 running inside the victim VM are vulnerable to the Flush+Reload attacks. Flush+Reload is a powerful cache-based side-channel attack in which the attacker takes advantage of a security weakness in the X86 processor architecture to ascertain whether specific cache lines are accessed by the victim or not. The flush+Reload attack can be performed in a cross-core setting under the assumption that the last level cache is shared between the cores. (Vulnerability, Design)

The article titled "*Anomaly Detection in Business Processes logs Using Social Network Analysis*" presents an approach to detect anomalies in process-aware information systems. This approach is based on process mining and uses social network analysis metrics to detect anomalous behavior. The main idea is to prove that applying the organizational perspective using social network analysis metrics can detect anomalies that follow a normal flow but are executed by unauthorized users. The proposed approach has been evaluated using artificial event logs and the cross-validation method. The paper concludes that the F-measure evaluation results show that this approach is even effective in the worst case, i.e., the highest anomaly rate. (Computer Security, Design)

All articles presented above were thoroughly peer-reviewed by independent anonymous experts. The final decisions on articles were first proposed by Guest Editors to the Editor-in-Chief, and then the final decisions were approved by the Editor-in-Chief.

We wish this special issue helps indicate the valuable efforts and contributions of Iranian researchers of the field to the science, and to help promote the aim of the special issue.

We are glad to have accepted the invitation of the French Journal of Computer Virology and Hacking Techniques to help publish Iranian information and system security studies.

The Editorial Team would like to express its sincere gratitude to all the esteemed authors who answered our call for paper and submitted their scientific work for this special issue of the journal, to all the esteemed authors of accepted articles for all the efforts they made to finalize their work, to all the esteemed reviewers who accepted our invitation for their time and their thorough review of the article materials, to Springer team, especially Mr. Shanthakumar Kulasekar and Mr. Adam Rajah, for their prompt technical support.

Our appreciation and special thanks also extends to the Editor-in-Chief, Professor Eric Filiol, for providing the opportunity to present some works of Iranian researchers as a special issue of the esteemed *Journal of Computer and Virology Techniques*.