Journal of Computer Virology and Hacking Techniques (2020) 16:1–2
https://doi.org/10.1007/s11416-020-00350-2

EDITORIAL

Editorial

Antonella Santone[1]

Published online: 25 February 2020

This issue of *Journal of Computer Virology and Hacking Techniques* contains a collection of five extended papers from the ForSE 2018 & 2019 workshops.

ForSE is an annual workshop on FORmal methods for Security Engineering in conjunction with ICISSP, the International Conference on Information Systems Security and Privacy. ForSE has established itself as a solid community aiming to address essential security problems and foster the development of verifiable secure and malware resistant systems using formal methods, which represent an excellent means to model software systems mathematically and verify their security properties to improve their resilience against malicious code.

The 2018 edition of ForSE was held in Funchal, Portugal, while the 2019 edition was held in Prague, Czech Republic. Both editions attracted a total of 26 regular paper submissions coming from 7 different countries around the world (Austria, France, Germany, Italy, USA, Brasil, United Kingdom). The conference program committee selected 17 regular papers to be presented at the conference and published in the conference proceedings.

Authors of excellent papers were invited to extend their submission for publication in this special edition, based on relevance to the journal and the reviews of the conference version of the papers. The authors were asked to revise the conference paper for journal publication, and, in accordance with customary practice, to add 30% new material. The articles were reviewed by at least two blind reviewers as per the norms of the *Journal of Computer Virology and Hacking Techniques*. On the basis of reviewers' comments the articles were revised by the authors, and then the revised papers were re-submitted. The revised papers were re-examined by the reviewers and by the Guest Editor and then the final publication decision on the paper was made. In this process five research articles have finally been selected for publication in this special issue. We appreciate the willingness of the authors to help in organizing this special issue.

The five extended papers in this special issue range from network security to cyber-physical systems security.

The authors of the paper "Statistical and combinatorial analysis of the TOR routing protocol: structural weaknesses identified in the TOR network" present the results of a deep TOR routing protocol analysis from a statistical and combinatorial point of view. They have proved that the probability for a circuit to be selected (or built) was not ruled by the uniform law but but by a power law. As a major consequence, it means that most of the TOR network traffic goes through a very limited number of nodes. Targeting these nodes would inevitably maximize a number of attacks they have described, while involving limited resources and efforts. Their study tends to prove that the security of the Tor network is not optimal.

The authors of the paper "PenQuest: a gamified attacker/defender meta model for cyber security assessment and education" introduce PenQuest, the design of a gamified meta model that can be used to train personnel, assess risk mitigation strategies, and compute new attack/defender scenarios in abstracted infrastructures.

The authors of the paper "Formalization and co-simulation of attacks on cyber-physical systems" present a methodology for the formal modelling of security attacks on cyber-physical systems, and the analysis of their effects on the system using logic theories. They consider attacks on sensors and actuators. The theorem prover of PVS has been used for deriving formal proofs of invariants of the system under attack.

The authors of the paper "Multifamily Malware Models" propose a comparison between different machine learning techniques. They conduct experiments based on byte *n*-gram features to quantify the relationship between the generality of the training dataset and the accuracy of the corresponding machine learning models, all within the context of the malware detection problem. They find that neighbourhood-based algorithms generalize surprisingly well, far outperforming the other machine learning techniques considered.

✉ Antonella Santone
antonella.santone@unimol.it

[1] Campobasso, Italy

The authors of the paper "Analytical Modelling of Cyber-Physical Systems Applying Kinetic Gas Theory to Anomaly Detection in Networks" present a novel model for cyber physical systems (CPS) that exploits the kinetic gas theory. The main goal is to use this theory to detect anomaly in a network made of CPS. This way of modelling the normal behaviour of a cyber-physical system has the advantage over machine learning methods mainly used for this purpose, in that it is not based on the effective operation of the system during a training phase, but rather on the specification of the system and its intended use.

On behalf of the organizing committee of ForSE2018 & 2019, I would like to express my sincere thanks to the authors for submitting an extended version of their articles into this special issue. I express my sincere gratitude to the reviewers for revising the articles. I appreciate the effort of the Editor-in-Chief, Prof. Eric Filiol, for providing me the opportunity to publish the extended and revised version of some deserving papers of ForSE 2018 & 2019 in the *Journal of Computer Virology and Hacking Techniques*.

I hope this special issue conveys valuable research information to the readers.