Journal of Computer Virology and Hacking Techniques (2021) 17:165–166
https://doi.org/10.1007/s11416-021-00394-y

EDITORIAL

Editorial

Antonella Santone[1]

Published online: 2 August 2021

This issue of Journal in Computer Virology and Hacking Techniques contains a collection of five extended papers from the ForSE2020 with the addition of an invited paper.

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 is establishing itself as a strong community aiming to address essential security issues and promote the development of secure systems using Formal Methods. Formal Methods are techniques based on a solid mathematical basis for the specification, development and verification of software and hardware systems. The adoption of Formal Methods in various areas has greatly improved the quality of computer systems and can also provide a similar improvement to the computer systems' security.

Currently, Formal Methods are in a period of rapid development and significant expansion in practical applications. In fact, while Formal Methods have long been associated with the verification of software systems, today the new techniques developed are becoming crucial also for security goals. Formal security methods will have a huge effect in the coming years thanks to recent technological advances, while previously they were not usable due to scalability problem. In fact, many techniques to reduce the state explosion problem have been defined and developed.

Without extensive use of Formal Methods, security would always remain fragile. The resulting security improvements will stimulate new investments in formal tools and techniques. This interaction will produce a virtuous circle of capital investment in methods and it could increase both the quality of secure systems and the productivity of security-conscious developers.

Formal Methods can be used as complementary techniques to the well-known Artificial Intelligence ones for security issues. They are definitely a reliable way to achieve security and privacy in computer science and, applying scientific methods and rigorous foundations, they are central to providing a secure process of science. In fact, despite the advantageous potential demonstrated by Artificial Intelligence, recently it was observed that it was necessary to carefully evaluate any problems that may arise with the use of automatic decision-making processes. The typical weaknesses of systems based on automatic learning are:

- large data sets are needed to achieve good performance;
- robustness, because a minimal deviation from the learned behaviour of the model is sufficient to perform an incorrect classification on cases never seen before.

Moreover, it is also known that many Artificial Intelligence algorithms generate non-interpretable models, so called "black boxes", i.e., models that do not provide understandable information to a human being on the decision-making process that determined the result. The transformation, therefore, from "black" to "white" boxes represents a recent but unavoidable challenge, especially in the cyber security field where, in addition to identify threats and prevent unauthorized intrusions, it is very important to provide an understandable explanation of the model's decision. The explanation is addressed to have, on the one hand, a better understanding of the decision-making process and, on the other, an increase in confidence in the functioning of the same. Therefore, the main criticism of the methods currently used at the state of the art for the realization of intelligent systems, is the total lack of explainability. For this reason, we believe that Formal Methods may support explainability and interpretability in decision support systems in cyber security and they can be used by integrating them with Artificial Intelligence techniques.

The 2020 edition of ForSE went online due to Covid-19 restrictions. The edition attracted a total of 10 regular paper submissions coming from 4 different countries around the world (Republic of Malta, France, Netherlands, Italy, Belgium). The conference program committee

✉ Antonella Santone
antonella.santone@unimol.it

[1] University of Molise, Campobasso, Italy

selected 7 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 the relevance of 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 materials. The articles were reviewed by at least two blind reviewers as per the norms of the Journal in 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. In addition to the five selected papers, this special issue presents also the invited paper "Learning Metamorphic Malware Signatures from Samples". The authors consider the problem of automatically extracting metamorphic signatures from the analysis of metamorphic malware variants. They define a metamorphic signature as an abstract program representation that ideally captures all the possible code variants that might be generated during the execution of a metamorphic program. For this purpose, they develop a tool that takes as input a collection of metamorphic code variants and produces, as output, a set of transformation rules that could have been used to generate the considered metamorphic variants.

The five extended papers from ForSE2020 range from network security to cyber-physical systems security. In particular, the authors of the paper "Detection of Crawler Traps: Formalization and Implementation—Defeating Protection on Internet and on the TOR Network" define a new distance to compare two objects (from a family to a single sample) and applied it to the case of crawler trap detection. They can decide with accuracy if a web page belongs to which family (crawler trap or not) with better results compared to existing information distances.

The authors of the paper "The Blockchain potential in computer virology. Leveraging combinatorial techniques of k-ary codes" delve into the state of the art of computer virology formalisation and then tackle the development of a new malware algorithm. They detail how the work leveraged Blockchain to create an undetectable malware depicting two versions of the new malware, starting from a first naive version to achieve an advanced armoured undetectable k-ary malware that leverages decentralized storage namely IPFS. The detection of the new malware algorithm has been proven NP-complete.

The authors of the paper "A Framework for Formal Analysis and Simulative Evaluation of Security Attacks in Wireless Sensor Networks" present ongoing work on a security-aware design approach for Wireless Sensor Network (WSN) applications and protocols. Such an approach exploits the integration between Formal Methods and network simulators enhanced for reproducing security attacks. This enables WSN designers to gather valuable insights on the realistic behaviour of the abstract model since design time, thus helping them to recognize design flaws and security-related issues, and then select and validate appropriate countermeasures. As a proof of concept, the authors have built a framework that integrates the model checker UPPAAL with the network and attack simulator.

The authors of the paper "RV-TEE: Secure Cryptographic Protocol Execution based on Runtime Verification" present an RV-centric TEE targeting various levels of security threats to a protocol implementation ranging from high-level to hardware and promising to improve the robustness of the implementation with minimal additional hardware and/or runtime overheads. A feasibility study of the approach has been carried out on a real-world third party code-base, which implements a state-of-the-practice key establishment protocol.

The author of the paper "A Framework for Supporting Ransomware Detection and Prevention based on Hybrid Analysis" discusses a hybrid framework, combining static and dynamic analysis, exploiting APIs to prevent and mitigate ransomware threats. The evaluation demonstrates that the hybrid API calls-based detection can be proved to be a promising direction in ransomware prevention and mitigation.

I believe that the above selected papers will contribute towards research progress in security promoting the integration between the communities of formal methods and security.

On behalf of the organizing committee of ForSE2020, I would like to express my sincere thanks to the authors for submitting an extended version of their articles into this special issue and for submitting the invited paper. 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 ForSE2020in the Journal in Computer Virology and Hacking Techniques.

Hope this special issue will convey valuable research information to the readers.

Guest Editor

Antonella Santone