Annals of Telecommunications (2023) 78:383
https://doi.org/10.1007/s12243-023-00988-1

EDITORIAL

Foreword of the special issue on « FPS 2021» symposium

Esma Aïmeur[1] · Maryline Laurent[2] · Reda Yaich[3] · Benoît Dupont[1] · Frédéric Cuppens[4]

Published online: 29 August 2023

The Foundations and Practice of Security (FPS) international symposium series is rooted in the desire to strengthen relations between the scientific communities in security of Canada and France. The founding event was the Canada-France Meeting on Security held at the Simon Fraser University, Vancouver, on December 06–08, 2007. Since 2008, the FPS symposium has been held annually, alternating Canadian and French locations, Grenoble, then Toronto, Paris, Montréal, La Rochelle, Montréal, Clermont-Ferrand, Quebec City, Nancy, Montréal, Toulouse, Montréal, and one symposium that was exceptionally organized as a virtual event in 2020 due to COVID-19.

The spirit of FPS is to gather doctorate students, post-doctorate, young researchers, and senior scientists to discuss and exchange theoretical and practical ideas that address privacy and security issues in inter-connected systems. It aims to establish links, scientific collaborations, joint research programs, and student exchanges between institutions involved in this important and fast-moving research field. Since 2008, the conference's topics have evolved to integrate the latest advanced cybersecurity-related topics, including privacy, Internet of Things security, malwares, digital identity, fake news, data brokers, and all the topics that revolutionize the practices and theories related to digital security.

The 14th International Symposium on Foundations and Practice of Security took place in Paris from 8 to 10 December 2021, in a fully hybrid mode. From the 62 papers submitted to the symposium, the program committee selected 18 regular papers and ten short papers for presentation. As the guest editors of the special issue, we proposed to the authors of six high-scored regular papers to significantly extend their papers for publication in the special issue, of which only four finally achieved publication.

The four published papers address very diverse issues ranging from the human selection of weak passwords compromising the user account security to malware in IoT environments increasing system vulnerabilities, to data processing history that might be corrupted, and corrective enforcement actions that might not be optimized in a system. The paper by Murray et al. introduces a specific methodology based on several password lists and a probability function whose optimum must be found, with the objective of improving the password guessing attack. What is also shown is that choosing passwords highly depends on the spoken language and nationality of the user, with two users sharing the same spoken language and nationality being more likely to choose the same password. The paper by Vitorino et al. provides a comparative analysis to compare the capacity of supervised, unsupervised, and reinforcement learning techniques to detect malwares. The experiment is performed on 9 malwares captured in the IoT environment and included in the IoT-23 data set. The paper by Paulin et al. presents a solution combining Ethereum blockchain technology and secure hardware to provide stakeholders with a reliable and timestamped record of the entire data processing history to which they can refer in case of stakeholder disagreement. Beyond the implemented security measures, the advantage is that the performances reached allow to consider an integration in an industrial context. The paper by Taleb et al. proposes a new model of runtime enforcement monitor that supports selecting one of several corrective enforcement actions, based on an objective user-defined gradation. The experiment demonstrates the ability of the model to automatize the selection of enforcement actions at runtime.

We want to thank the volunteer reviewers who carefully read and provided valuable feedback to improve the quality of the papers and the authors for taking the time to enhance and extend their scientific contribution originally published in FPS 2021 proceedings.

✉ Maryline Laurent
Maryline.Laurent@telecom-sudparis.eu

[1] Université de Montréal, Montreal, Quebec, Canada

[2] Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France

[3] IRT Systemx, Palaiseau, France

[4] Polytechnique Montréal, Montréal, Quebec, Canada