Journal of Computer Security 30 (2022) 753–755
DOI 10.3233/JCS-220951
IOS Press

Guest Editorial

Special issue ESORICS 2021

Following the tradition of the European Symposium European Symposium on Research in Computer Security (ESORICS), this special issue includes selected papers from the 2021 edition of ESORICS. This edition was held (virtually) in Darmstadt (Germany) on October 4–8, 2021.

ESORICS 2021 introduced for the first time in the ESORICS series two review cycles: a winter cycle and a spring cycle. Multiple submission cycles are today common in top conferences; they are not only more convenient for the authors but also allow revision and resubmission of papers. In response to the call for papers, 351 papers were submitted to ESORICS 2021. The papers were peer reviewed and discussed based on their novelty, quality, and contribution by the members of the Program Committee. Based on the reviews and discussions 71 high quality papers were selected for presentation at the conference. As a result, ESORICS had an interesting program covering timely and interesting security and privacy topics in theory, systems, networks, and applications.

Because of the high quality of the papers accepted for presentation at ESORICS 2021, selecting the papers to invite for the special issue was challenging. To select the papers, we analyzed the top ranked papers and also asked for inputs by the PC members, and finally identified and invited six papers. Out of those six papers, one was not submitted owning to some resource issues by the authors. The remaining five papers went through the customary review cycles and were all accepted. These papers cover a broad set of topics, ranging from zero-knowledge proof protocols and privacy-preserving neural network inferences to privacy-preserving searching techniques, malware sandbox evasion and password strength estimation. Overall the selected papers address timely and crucial topics and provide novel solutions. We now briefly describe the main contributions of these papers.

The paper titled “Scriptable and Composable SNARKs in the Trusted Hardware Model”, by Z. Zhou, B. Zhang, Y. Chen, J. Li, Y. Zhou, Y. Lu, and K. Ren (Zhejiang University), and P. Thai, H.S. Zhou (Virginia Commonwealth University), focuses on non-interactive zero knowledge proof protocol (NIZK) systems. Such systems are a critical security building block and have been widely investigated. This paper proposes an important extension to SNARK – one of the most well-known NIZK systems. The extension allows the parties involved in the protocols to specify, via a script, the function to be proved. As part of such an extension, the authors also provide a generic implementation solution based on trusted hardware. The extension is then instantiated on SGX and Trustzone. Experimental results reported in the paper show that the proposed extension is much more efficient than all known SNARK systems. The paper discusses the requirements driving the design of the extension and provides formal proofs and implementation details. This paper definitely provides an important contribution enabling the practical applications of NIZK systems.

The paper titled “Deep Learning-Based Medical Diagnostic Services: A Secure, Lightweight and Accurate Realization”, by X. Liu and Xun Yi (RMIT University), Y. Zheng (Harbin Institute of Technology), and X. Yuan (Monash University), focuses on the challenging problem of enabling accurate, lightweight and privacy-preserving medical diagnostics via neural network inferences. To achieve privacy, the paper proposes the CryptMed system, which is based on carrying out neural network inferences in the encrypted domain. CryptMed is lightweight in that it uses secret sharing techniques, which do not require expensive cryptographic computations nor transmission of large cyphertexts. CryptMed relies on an interesting hybrid approach, by which most computations are carried out during a preprocessing phase (executed before records become available). Therefore, the online phase, which does the actual inference on the records, is very efficient. The paper provides interesting details about the design of CryptMed, including how it addresses the main challenge, that is, how to accurately and efficiently evaluate smooth activation functions, such sigmoid and tanh, in the secure domain. The paper also includes experimental results on accuracy and overhead. This paper makes an important step forward with respect to efficient and privacy-preserving deep learning.

The paper titled "Range Search on Encrypted Spatial Data with Dynamic Updates", by S. K. Kermanshahi and Xun Yi (RMIT University), R. Dowsley, R. Steinfeld, A. Sakzad, J. Liu and S. Lai (Monash University), and S. Nepal (CSIRO), focuses on privacy-preserving searches on spatial data, hosted on the cloud. The paper specifically addresses the problem of defining a searchable symmetric encryption (SSE) protocol supporting geometric range queries without leaking access patterns and in the presence of dynamic updates to the data. Previous approaches only work for static data, and therefore do not support changes to the data. The paper proposes two approaches addressing dynamic data changes; both approaches leverage the R+-tree indexing structure for spatial data and use secret sharing techniques. The paper includes extensive experimental results on the round-trip times between client and server, and computational and storage overhead at the client side. This paper provides an effective solution toward addressing a critical requirement for the deployment of privacy-preserving search on spatial data.

The paper titled "SCRAMBLESUIT: An Effective Timing Side-Channels Framework for Malware Sandbox Evasion", by A. Nappa, A. Ubeda-Portugues, and J. Tapiador (University Carlos III de Madrid), P. Papadopoulos (Telefonica Research), M. Varvello (Nokia Bell Labs), and A. Lanzi (University of Milan)", focuses on the techniques used by malware to detect whether it is running inside a sandbox; sandboxes are typically used by security analysts and researchers to monitor and analyze the behavior of malware. Conventional techniques adopted by malware to detect sandboxes are based on the use of fine-grained timing instructions provided by the operating system; however, access to these instructions has been recently restricted for protection against side-channel attacks, such as Spectre and Meltdown. This paper thus proposes a different detection approach based on proof of work (PoW) techniques. The approach uses PoW to generate a statistical model for identifying the class of hardware machines where the algorithm is running. Such a model can then be used to distinguish between physical and virtualized architectures, like those used by malware sandboxes. The paper provides experimental results on the evaluation of the proposed detection technique on several different hardware architectures, malware families, and sandboxes. The results are very interesting and show that the proposed technique reduces the existing malware detection rate by a factor of 10. The paper is interesting not only because of the detection technique but also because the design of countermeasures against this technique is very challenging. The authors argue that the only plausible one is running malware analysis tools on bare metal, which is obvious not a practical option. It will be interesting to see if future research will be able to devise some effective countermeasures.

The paper titled "PESrank: An Explainable Online Password Strength Estimator", by Liron David and Avishai Wool (Tel Aviv University), focuses on the well-known password mechanism. Passwords still remain the most used form of authentication, used alone or in combination with other authentication factors. Their strength against password cracking tools is thus critical. This paper proposes a novel password strength estimator that has several advantages; it accurately models the behavior of powerful password cracker and is very fast, as it can estimate the password rank with respect to strength in fractions of a second. It is also explainable. The proposed estimator is based on the clever idea of casting the question of estimating the rank of passwords in a probabilistic framework used for side-channel cryptanalysis. The paper includes results on the evaluation of the proposed method on a corpus of 1.4 billion of leaked pairs of usernames and passwords and also a comparison with other approaches. This paper definitely provides an effective tool to strengthen authentication based on passwords.

To conclude, we would like to thank the ESORICS 2021 Program Committee members that reviewed those papers and provided many valuable suggestions for improvements. We also thank the EiCs and the Editorial Assistant of Journal of Computer Security for their guidance in the organization of the special issue.

Enjoy the papers!!

Elisa Bertino and Haya Shulman (ESORICS 2021 Program Committee Chairs)
Michael Waidner (ESORICS 2021 General Chair)