Journal of Hardware and Systems Security (2019) 3:199
https://doi.org/10.1007/s41635-019-00077-7

Guest Editorial: Special Issue on Hardware Solutions for Cyber Security

Michael Vai[1] · Yunsi Fei[2] · Roger Khazan[1]

Published online: 22 August 2019

Welcome to this "Special Issue on Hardware Solutions for Cyber Security" in the *Journal of Hardware and Systems Security*.

A cyber system could be viewed as an architecture consisting of application software, system software, and system hardware. The hardware layer, being at the foundation of the overall architecture, must be secure itself and also provide effective security features to the software layers. In order to seamlessly integrate security hardware into a system with minimal performance compromises, designers must develop and understand tangible security specifications and metrics to trade between security, performance, and cost for an optimal solution. Hardware security components, libraries, and reference architecture are increasingly important in system design and security. This special issue includes four exciting manuscripts on several aspects of developing hardware-oriented security for systems.

Using formal methods for hardware security has become desirable despite challenges. With suitable formal modeling and property specification, provable system security can be achieved. In their paper "SRASA: A Generalized Theoretical Framework for Security and Reliability Analysis in Computing Systems," the authors have described a unified security and reliability analysis framework and illustrated its application with use cases.

In order to integrate security hardware into a system, strong physically unclonable functions (PUFs) are essential. The authors of "Design of Robust, High-Entropy Strong PUFs via Weightless Neural Network" have presented their development and assessment of novel and effective PUFs.

While hardware features can enhance system security, they broaden the attack surface and should be included in vulnerability analyses. Hardware vulnerabilities to physical attacks and tampers should thus be evaluated and mitigated. In "Survey of Microarchitectural Side and Covert Channels, Attacks, and Defenses," the author has extracted the key features of a processor's microarchitectural functional units that could be leveraged for side channel attacks, presented an analysis and categorization of the variety of microarchitectural side and covert channels others have presented in literature, and surveyed existing defense proposals.

Supply chain management must be established to ensure the security of hardware components from design and manufacturing to deployment. Reverse engineering, while commonly considered a physical attack, is also a last resort approach for integrity verification and counterfeit identification. In the fourth paper, "Practical Partial Hardware Reverse Engineering Analysis: For Local Fault Injection and Authenticity Verification," its author has explained a low-cost alternative to full-scale reverse engineering.

Over the last decade, there has been much research and practical applications in the abovementioned areas. We hope that we have assembled a valuable resource for our community for setting and pursuing with more clarity further advances in the field of cyber security.

✉ Michael Vai
mvai@ll.mit.edu

Yunsi Fei
yfei@ece.neu.edu

Roger Khazan
rkh@ll.mit.edu

[1] Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusetts, USA

[2] Northeastern University, Boston, USA