In Hardware We Trust?: Gains and Pains of Hardware-assisted Security

ABSTRACT

After years of research in hardware security, we are still missing adequate solutions to protect modern computing platforms. Deployed hardware solutions like Physical unclonable functions (PUFs), Trusted Platform Modules (TPMs), and Trusted Execution Environments (TEEs) are lacking widespread usage, or have been successfully attacked. Additionally, we are witnessing a paradigm shift towards cross-layer attacks, hardware vulnerabilities from software, making hardware vulnerabilities remotely exploitable. Recent attacks like CLKS crew, Meltdown, and Spectre, have demonstrate that even systems with advanced defenses such as Control Flow Integrity (CFI) are affected by this new class of attacks.

In this talk we will discuss the impact of deployed hardware-assisted security solutions, their strengths and shortcomings, as well as new research directions on enhancing trust in hardware through new security architectures in particular based on Open Source Hardware such as RISC-V.

BIOGRAPHY

Ahmad-Reza Sadeghi is a full professor of Computer Science at the TU Darmstadt, Germany. He is the head of the Systems Security Lab at the Cybersecurity Research Center of TU Darmstadt. He is also the director of the Intel Research Institute for Collaborative Autonomous Resilient Systems (ICRI-CARS) at TU Darmstadt. He holds a Ph.D. in Computer Science from the University of Saarland, Germany. Prior to academia, he worked in R&D of Telecommunications enterprises, amongst others Ericsson Telecommunications. He has been continuously contributing to security and privacy research.

Prof. Sadeghi was Editor-in-Chief of IEEE Security and Privacy Magazine, served 5 years on the editorial board of the ACM Transactions on Information and System Security (TISSEC), and is currently on the editorial boards of ACM Books, ACM TODAES, ACM TIOT and ACM DTRAP.

For his influential research on Trusted and Trustworthy Computing he received the renowned German “Karl Heinz Beckurts” award. This award honors excellent scientific achievements with high impact on industrial innovations in Germany. In 2018 Prof. Sadeghi received the ACM SIGSAC Outstanding Contributions Award for dedicated research, education, and management leadership in the security community and for pioneering contributions in content protection, mobile security and hardware-assisted security. SIGSAC is ACM’s Special Interest Group on Security, Audit and Control.

All are welcome!

In case of questions, please contact Dr Cong Wang at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/.