USC Viterbi School of Engineering
Ming Hsieh Department of Electrical and Computer Engineering

Seminar

Architectures for Verifiable Confidentiality, Integrity, and Availability in Resource-Constrained Embedded Devices

Ivan de Oliveira Nunes
Assistant Professor
Department of Computing Security
Rochester Institute of Technology (RIT)

Wednesday, March 22, 2023
10:00am – 11:00am
EEB248
Zoom Link: https://usc.zoom.us/j/93387896454?pwd=MVdwL2NHS1hqSXFlaFhPaE91WHVGUT09

Abstract: Embedded devices are increasingly ubiquitous and their importance is hard to overestimate. While they often support safety-critical functions (e.g., in medical devices, industrial control systems, and sensor-alarm combinations), these devices are usually implemented under strict cost and energy budgets, using low-end microcontroller units (MCUs) that lack sophisticated security mechanisms. On the lower end of the scale, these devices are small, cheap, and specialized. They tend to host small CPUs, have very limited memory, and run simple software. Nonetheless, if such devices are left unprotected, consequences of forged sensor readings or ignored actuation commands can be catastrophic, particularly, in safety-critical settings. This prompts the following three questions: (1) how to trust data produced, or verify that commands were correctly performed, by a simple remote embedded device? (2) how to actively prevent malware that infects embedded devices from exfiltrating private sensor data? and (3) how to guarantee that safety-critical tasks are always performed in a timely manner, irrespective of malware infections?

Motivated by these questions, this talk will overview a set of architectures based on hardware/software (HW/SW) co-designs to provide provable guarantees about data confidentiality, software integrity, and availability in (potentially compromised) embedded devices. In particular, I will discuss three formally verified HW/SW co-designs, each realizing one of the aforementioned goals (namely APEX [SEC'20], GAROTA [SEC'22], and VERSA [S&P'22]) and how they have been securely implemented atop the popular TI MSP430 micro-controller at a relatively low-cost.

Bio: Ivan De Oliveira Nunes is an Assistant Professor of Computing Security at the Rochester Institute of Technology (RIT). Before RIT, he received his Ph.D. degree in 2021 from the University of California Irvine (UCI). Ivan also holds a Bachelor's degree in Computer Engineering from the Federal University of Espirito Santo (UFES), Brazil, and a Master's degree in Computer Science from the Federal University of Minas Gerais (UFMG), Brazil. In recent years, he has worked on several topics, including IoT Security, Hardware-assisted security, HW/SW Co-design, Network Security, and Applied Cryptography. His research interests span the fields of security and privacy, computing systems, computer networking, applied cryptography, and especially their intersection.

Hosts: Dr Bhaskar Krishnamachari, bkrishna@usc.edu