Securing IoT Devices: Challenges and Countermeasures

Farimah Farahmandi
University of Florida

Wednesday, March 7, 2018
10:00 am – 11:00 am
HUB Room 3

Abstract:

Our daily life is intertwined in the fabric of Internet-of-Things (IoT), a fabric in which the number of connected smart computing devices exceeds the human population. Security and trust are paramount considerations while designing these systems. Unlike microcontroller based designs in the past, even resource constrained IoT devices nowadays incorporate one or more complex System-on-Chips (SoCs). It is a major challenge to verify the security requirements of SoCs in IoT devices, primarily due to the fact that SoCs are designed using hardware Intellectual Property (IP) blocks to reduce cost while meeting aggressive time-to-market constraints. Growing reliance on these pre-verified hardware IPs, often gathered from untrusted third-party vendors, severely affects the security and trustworthiness of SoC computing platforms. These IPs may come with deliberate malicious implants, undocumented test and debug interface working as a hidden backdoor, or other integrity issues. In the absence of comprehensive SoC security and trust verification, vulnerable IoT devices can lead to unintended consequences including damages to critical infrastructure, violating personal privacy, or undermining the credibility of a business. In this talk, I will present novel hardware security and trust validation techniques. First, I will outline various SoC security and trust vulnerabilities. Next, I will highlight why existing verification techniques are not suitable for security and trust validation. The core part of my talk will cover a trustworthy SoC design framework consisting of formal verification, statistical test generation as well as side channel analysis. Finally, I will describe the future IoT security challenges and potential countermeasures while considering the trade-off between security, energy, connectivity, and intelligence.

Short Bio:

Farimah Farahmandi is a Ph.D. candidate in the Department of Computer and Information Science and Engineering at the University of Florida. She received her B.S. and M.S. from the Department of Electrical and Computer Engineering at the University of Tehran, Iran in 2010 and 2013, respectively. Her research is focused on developing analytical models and computational methods for design and verification of secure, trustworthy and energy-efficient systems. Her research has resulted in one book, six book chapters, and thirteen publications in premier ACM/IEEE journals and conferences including Design Automation Conference (DAC) and Design, Automation and Test in Europe (DATE). Her research has been recognized by several awards including IEEE System Validation and Debug Technology Committee Student Research Award, Gartner Group Info-Tech Scholarship, nomination for Best Paper Award in ASPDAC 2017, and DAC Richard Newton Young Student Fellowship. She was a research intern in advanced security research group at Cisco in summer 2016. She has actively collaborated with various research groups (IBM, NXP, Intel, and Cisco) that led to several joint publications.