ELECTRICAL AND COMPUTER ENGINEERING SEMINAR

Nader Sehatbakhsh
Georgia Institute of Technologies

Designing Secure Computer Systems

Thursday, January 30th
138 ISEC
11:45 am

Abstract:

This decade has already seen a significant surge in the number of cyber-attacks. With the exponential growth of computers in numbers, due to the rise of cyber-physical systems (CPS) and internet-of-things (IoT) devices, and their ever-increasing importance in controlling critical tasks, it is expected that cybersecurity and data privacy become even more serious problems in the next decade.

To this end, I will present our methods and findings in designing secure computing systems using two main themes: 1) by discovering, modeling, and mitigating side-channels, and 2) by leveraging side-channels for useful purposes such as debugging and security monitoring. Specifically, in this talk, I will first present our novel method on debugging and securing resource-limited devices such as embedded systems, CPSs, and IoTs by externally monitoring these devices using analog side-channels (e.g., electromagnetic emanations, power fluctuations, etc.) that are unintentionally created by these devices. I will describe how analog sidechannel signals can be also leveraged for profiling, intrusion detection, and establishing a trusted execution environment (TEE) on resource-constrained devices without incurring any overhead or requiring any hardware-support on the monitored device and/or any intrusion to its functionality. In the second part of the talk, I will demonstrate how we can mitigate information leakage vulnerabilities by accurately modeling analog side-channels. I will discuss our approach in designing an open-source microarchitectural simulator which can accurately simulate analog side-channel signals (electromagnetic and power side-channels) in a variety of low-end processors. I will conclude my talk by describing future directions toward secure, private, and remote computing systems.

Bio:

Nader Sehatbakhsh is a Ph.D. Candidate in the School of Computer Science, Georgia Institute of Technology. His research interest is on the broad area of Security and Privacy and Computer Architecture with emphasis on hardware security, side-channels, hardware-support for security and privacy, and embedded system security. His work has been published in top venues such as MICRO, ISCA, and HPCA, and has been recognized with several awards and honors including the MICRO-49 Best Paper Award and Micro Top-Picks Honorable Mention.