NJIT

Department of Computer Science

Securing embedded systems using compartmentalization

Arslan Khan
Purdue University

Hosted by Ioannis Koutis

Date: Tuesday, January 23, 2024

Coffee: 2:15 PM – 2:30 PM

Time: 2:30 PM – 3:30 PM

Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: https://njit-edu.zoom.us/j/97592288472?pwd=WVZMNjhmV2tvczJwL1RqdG1tVXI4QT09

Abstract:

Embedded systems are low-power resource-constrained devices implementing specialized tasks, unlike general-purpose computers. Embedded systems find applications in various domains, from the Internet of Things (IoT) to general purpose Personal Computers (PC). Unfortunately, due to the resource constraints of embedded systems, developers often sacrifice security in favor of performance, leaving a huge attack surface for attackers.

In this talk, I will talk about the challenges of securing embedded systems. I will introduce software compartmentalization and will show how we can utilize compartmentalization to secure embedded systems. Next, I will talk about my research on automatic compartmentalization frameworks that can work within the constraints of embedded systems. We will discuss Compartmentalized Real-Time C (CRT-C), a low-cost compile-time compartmentalization mechanism to achieve privilege separation using specialized programming language dialects and static analyses for user threads and device drivers. CRT-C extends the C language type system to protect the kernel space from user threads and device drivers. CRT-C can enforce isolation 178x faster than state-of-the-art solutions. I will also talk about, Embedded Compartmentalizer (EC), an auto-compartmentalization tool that can achieve compartmentalization in the kernel space. EC uses EC-Kernel (ECK), a formally verified microkernel that uses a novel operating system architecture, to provide privilege separation without hardware context switching in the kernel space. EC can enforce isolation 1.2x faster than state-of-the-art solutions. Lastly, I will briefly talk about my future research directions.

Bio:

Arslan Khan is a Post-Doctorate researcher in Computer Science at Purdue University, where he also finished his doctorate under the supervision of Dr. Dongyan Xu and Dr. Dave (Jing) Tian. His research lies at the intersection of system security, software engineering, and programming languages, with a focus on securing embedded systems. His research has received the Best Presentation Award in UEMCON and has been adopted by both academia and industry. He was part of the Secure Software Group (SSG) when he interned at Qualcomm, enhancing their Secure Execution Environment (QSEE) and Trust Management Engine (TME). Before his doctorate, he worked at Siemens and contributed to the Nucleus RTOS and hypervisor.