Proposal Defense

Doctor of Philosophy in Computer Science

“Secure I/O on Trusted Platforms with Lightweight Kernels” by Nicholas Gordon

Date: May 8, 2023
Time: 3:00PM – 4:30PM
Place: Board room 6329, Sennott Square, 210 Bouquet St, Pittsburgh, PA, 15260

Committee:
- John Lange, Associate Professor, Computer Science, University of Pittsburgh
- Amy Babay, Assistant Professor, DINS & Computer Science, University of Pittsburgh
- Adam Lee, Professor, Computer Science, University of Pittsburgh
- Devesh Tiwari, Associate Professor, Electrical and Computer Engineering, Northeastern University

Abstract:
Trusted computing has become widespread and the complexity of trusted applications has increased substantially, such as in real-time patient vitals data processing or employee-free stores that continuously monitor customers. These applications differ from existing trusted computing usage in that they are directly acquiring and processing sensitive information via sensors like cameras and microphones, while application complexity demands a rich, general-purpose OS environment. Current trusted OSes fail to provide this environment because they are designed to only provide trusted services to untrusted applications, and full-weight kernels like Linux cannot be used due to security concerns. We aim to solve this problem by using lightweight kernels (LWK) to strike the correct balance between security and usability and fully exploit hardware to provide secure device I/O.

Lightweight kernels present a familiar programming environment to Linux both in userspace and in the kernel, allowing many applications to run without modification, as well as ease porting for existing device drivers. Further, hardware is more directly exposed to programmers—that is, with fewer hardware abstraction layers—enabling easy leveraging of platform hardware and peripherals. To demonstrate these design advantages we will develop a LWK trusted OS for the ARM TrustZone environment on a typical IoT or edge computing hardware platform. Specifically, we will extend the Kitten LWK to be TrustZone-aware, develop an I/O stack to demonstrate a viable camera driver in one of these IoT systems, and then build a framework to re-use by paravirtualizing existing Linux drivers securely by using recent TrustZone hardware.