Dissertation Defense
Doctor of Philosophy in Computer Science

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

Date: August 8, 2024
Time: 11:00 a.m. – 1:00 p.m.
Place: 6106 Sennott Square, 210 S Bouquet St, Pittsburgh PA 15260
https://pitt.co1.qualtrics.com/jfe/form/SV_5w1EHWlglg06yFw

Committee:
- John Lange, Associate Professor, University of Pittsburgh
- Amy Babay, Assistant Professor, University of Pittsburgh
- Adam Lee, Professor, University of Pittsburgh
- Devesh Tiwari, Associate Professor, 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 directly acquire and process sensitive information from sensors like cameras and microphones. Simultaneously, application demands are expanding to include a rich, general-purpose OS environment to provide network, filesystems, and multicomputing capabilities. An application runtime of similar capability approaches an OS in terms of complexity and would require extensive interfacing with the underlying untrusted OS anyway, so we claim that a full-stack trusted OS provides similar capabilities with a smaller, less complex trust profile. Further, current trusted OSes fail to provide this environment because they are designed to provide trusted \textit{services} to untrusted applications, and the use of full-weight kernels (FWKs) like Linux is ruled out due to security concerns. We aim to solve this problem by using lightweight kernels (LWK), which strike the correct balance between security and usability and can fully exploit hardware to provide secure device I/O.

Lightweight kernels are an OS design approach that presents 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 of 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 the viability of a camera driver, and then build a framework for securely paravirtualizing existing Linux drivers by using recent, modern TrustZone hardware.