COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Lauren Biernacki

Achieving Security and Privacy via Encrypted Architectures

Monday, June 12, 2023
1:00pm – 3:00pm
3725 Beyster
Hybrid – Zoom
Passcode: encrypt

ABSTRACT: There are increasing incidences of high-profile data breaches and clever new attacks that exploit weaknesses throughout the software stack, with recent attacks moving into the hardware layer. Yet, the security landscape consists not only of these novel exploits but also of exploits we have known about for decades that leverage vulnerabilities equally as pervasive. Despite the prevalence of these known vulnerabilities and significant efforts to defend against them, exploits remain widespread.

Understanding the landscape of security attacks can aid in the design of more durable defenses. Security attacks take on a similar structure, despite their diverse forms. Attackers leverage one or more vulnerabilities and system information assets to synthesize their exploit. Ultimately, classes of information assets that are instrumental for attacks (e.g., pointers, data layout, cache organization) are lesser in number than classes of vulnerabilities. Thus, by applying protections to a few critical pieces of information, defenses can potentially achieve broad coverage against security exploits. Further, hardware provides an advantageous place to situate protections as it can isolate critical information assets from higher-level layers of the stack, enabling vulnerability-tolerant systems.

Based on these insights, this dissertation explores how encrypted architectures—processors that encrypt information domains directly in hardware—can provide comprehensive security and privacy guarantees. Our research has evolved from using encryption minimally in an ensemble of moving target defenses to comprehensively applying encryption with small but powerful architectural extensions. The first half of this dissertation studies the protection of code and pointers to thwart control-flow attacks following the evolution of the Morpheus secure architecture. The second half of this dissertation discusses how encrypted architectures can comprehensively protect sensitive data. Vulnerability-tolerant design undercuts all our proposed defenses, as we aim to protect systems in the presence of pervasive software vulnerabilities. Our work demonstrates that architectural approaches can emerge as dynamic, expressive, and performant security and privacy solutions.

CHAIR: Prof. Todd Austin