Thesis Defense

Computer Science Master's Program

"Hardware Control Unit for Trusted Program Verification System"

By **Jake Alt**

Abstract:

Trust in the underlying hardware is the foundational step towards trusting the correctness and integrity of a software application. However, verifying that today's extremely complex processors work exactly as intended has not been feasible, as evidenced by several recent hardware bugs. Trustworthy, formally verified processors currently forego intricate performance enhancements such as out-of-order execution, hampering them substantially versus their less secure counterparts.

The Containment Architecture with Verified Output (CAVO) system solves this problem by isolating the host system and requiring the result of each instruction to be double-checked by a small, trusted hardware module called the Sentry. Any transmissions to the outside world must be performed through the Sentry, which ensures all prior instructions have been computed correctly. The first version of CAVO was centered around a customized host CPU with hardware modifications to manage the Sentry with minimal overhead, while the second used compiler tooling and a software version of the Sentry controller, incurring a significant performance penalty on checked programs. This paper proposes a novel hardware-based Sentry control system that serves as a first step toward fast checking of native programs while greatly reducing modifications to the host, all without expanding the root of trust. We implement a proof-of-concept hardware design and verify its correctness using SPECINT2006 benchmarks, demonstrating steady-state performance of 1 instruction per clock and an average overhead of 45 clocks per cache miss.

Date: Wednesday, September 25th, 2024
Time: 8:00 AM – 10:00 AM
Location: 14-232b
Zoom: https://calpoly.zoom.us/j/6834792650
Committee: Dr. Beard, Dr. Pantoja, Dr. Danowitz