Thesis Defense

Computer Science Master's Program

"SENTRY V3: EXTENDING CONTEXT SWITCHES ON A TRUSTED SECURE COPROCESSOR"

By **Mark Kong**

Abstract:

Software correctness and integrity is only ensured through trust in the underlying hardware. However, modern computer systems are complex to design and secure. Thus, given the choice between performance and security, companies will often prioritize performance, resulting in vulnerable systems. This creates exploitable systems that must be patched retroactively because security was an afterthought.

One approach to this issue is to separate the root of security from the rest of the system to create a minimal trusted computing base. Trustguard is one instance of this. Trustguard implements a Containment Architecture with Verified Output (CAVO) model which shows how a simple, pluggable co-processor, called the Sentry, can secure commodity systems. The Sentry monitors committed instructions from trusted software to enforce containment and software integrity.

The Sentry is currently implemented as a proof-of-concept single-context coprocessor for unicore systems with no concurrency features. This thesis aims to extend the work of the Sentry by leveraging its correctness guarantees and present a design capable of managing multiple single-threaded programs. It discusses the problems and solutions when managing multiple independent Merkle trees to ensure program integrity and isolation for processes on a time-sharing processor. To this end, this thesis proposes a new Sentry hardware architecture, runtime algorithms, and bootstrapping procedures to support context switching.

Date: Monday, June 9th, 2025
Time: 11:00 AM – 1:00 PM
Location: 14-238b
Zoom: https://calpoly.zoom.us/j/81391636939
Committee: Dr. Beard, Dr. Bellardo, and Dr. Peterson