Thesis Defense

Computer Science Master's Program

"Bulk Memory Verification Unit For Trusted Program Verification System"

By **Richard Rios**

Abstract:

Today, all modern computing systems are undoubtedly vulnerable to numerous types of attacks that could be targeted toward any layer of the system from dedicated hardware to highly abstracted software. Unfortunately, many devices and systems naturally contain inadequately protected components or software modules that undermine their security as a whole. Additionally, security is heavily variable system to system, and has a huge dependence on adequate implementation and ongoing support from device and software manufacturers. To address these various security issues in a very general way, TrustGuard, a containment security system utilizing an external device called the Sentry that would verify the activity of the host machine and control all incoming/outgoing communication accordingly, was created. To do this, TrustGuard uses cryptographic memory protection schemes, a small trusted hardware and software base, and recomputation and checking of application behavior running on the host machine at an instruction-by-instruction granularity before allowing external communication to occur. Currently, however, the TrustGuard system only allows for one 8-byte chunk to be sent or received externally at one time, limiting overall throughput, and heavily polluting the main system caches in the case of large data transfers. To combat this limitation, This thesis proposes a system to allow for efficient communication of large batches of data at once. In particular, it does so by using a small dedicated cache and efficient tree traversal techniques to asynchronously verify large chunks of program memory in stream-like fashion. This thesis primarily serves to provide a design, proof-of-concept, and collection of important information that will help future students implement such a system using FPGAs.

Date: Thursday, December 12th, 2024
Time: 1:00 PM – 3:00 PM
Location: 14-232b
Committee: Dr. Beard, Dr. Oliver, and Dr. Bellardo