Thesis Defense

Computer Science Master's Program

"Machine-Checked Proofs for Correctness Guarantees in Containment Architectures"

By **Sophie Russ**

Abstract:

Modern computing systems are increasingly susceptible to attacks at the hardware and software levels. Formal methods offer promising guarantees as to the correctness and security of systems. However, these methods tend to scale poorly and are thus insufficient to protect complex systems. Leveraging minimal amounts of trusted hardware and software to ensure the security of whole systems is a promising approach to gain the benefits of formal methods without having to overcome the scaling problem. TrustGuard realizes this approach: a containment architecture model that requires all outgoing communication from the host computer be validated by a small, external hardware module called the Sentry. In essence, the trusted Sentry ensures that only correct behavior of the host computer system is visible outside of the system. The nature of TrustGuard requires precise coordination and synchronization of the host and the Sentry. Previous work has provided a paper-based proof of the correctness of this host-Sentry relationship. However, proofs done on paper are inherently susceptible to human error and may contain subtle gaps. This thesis provides the first step towards a formally verified TrustGuard system. Leveraging Agda, an automated theorem prover, we present a mechanically-checked proof of the host-Sentry relationship. Additionally, we implement a framework to verify arbitrary programs within this system.

Date: Tuesday, June 10th, 2025
Time: 3:10 PM – 5:00 PM
Location: 14-232b
Committee: Dr. Beard, Dr. Clements, Dr. Keen, and Dr. Jones