Security policies stipulate restrictions on the behaviors of systems to prevent them from behaving in harmful ways. One way to ensure that systems satisfy the constraints of a security policy is through the use of security enforcement mechanisms. To understand the fundamental limitations of such mechanisms, formal methods are employed to prove properties and reason about their behaviors. The particular formalism employed, however, typically depends on the time at which a mechanism operates. Mechanisms operating before a program's execution are static mechanisms, and mechanisms operating during a program's execution are dynamic mechanisms. Static mechanisms are fundamentally limited in the types of policies that they can enforce, due to the lack of runtime information. However, the class of policies enforceable by particular types of dynamic mechanisms depends on the capabilities of the mechanism. An open, foundational question in computer security is whether additional sorts of security mechanisms exist. This dissertation takes a step towards answering this question by presenting a unifying theory of security mechanisms that casts existing mechanisms into a single framework based on the granularity of program code that they monitor. Classifying mechanisms in this way provides a unified view of security mechanisms and shows that all security mechanisms can be encoded as dynamic mechanisms that operate at one or more levels of program code granularity. This unified view has allowed us to identify new types of security mechanisms capable of enforcing security policies at various levels of code granularity. This dissertation also demonstrates the practicality of the theory through a prototype implementation that enables security policies to be enforced on Java bytecode applications at various levels of code granularity. The precision and effectiveness of the implementation hinges on an extensible Java library that we have developed, called JaBRO, to enable runtime code analysis on optimized Java bytecode at runtime. It is shown that JaBRO allows some security policies to be enforced more precisely at runtime than statically operating mechanisms.

Examining Committee
Lawrence Morehouse, Ph.D., Chairperson
Jay Ligatti, Ph.D., Major Professor
Yao Liu, Ph.D.
Lawrence Hall, Ph.D.
Sanjukta Bhanja, Ph.D.
Theodore Molla, Ph.D.

Publications

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.