UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Unifying Security Policy Enforcement: Theory and Practice

by

Shamaria Engram

For the Ph.D. degree in Computer Science and Engineering

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.

Friday October 30, 2020
3:30 PM
Online (Collaborate Ultra)
Please email for more information
sengram@usf.edu

THE PUBLIC IS INVITED

Publications

1) **Shamaria Engram** and Jay Ligatti. “Through the Lens of Code Granularity: A Unified Approach to Security Policy Enforcement.” In *IEEE Conference on Applications, Information, and Network Security (AINS)*. 2020. To appear.
2) Jean-Baptiste Subils, Joseph Perez, Peiwei Liu, **Shamaria Engram**, Cagri Cetin, Dmitry Goldgof, Natalie Ebner, Daniela Oliveira, and Jay Ligatti. "A Dual-Task Interference Game-Based Experimental Framework for Comparing the Usability of Authentication Methods." In *IEEE International Conference on Human System Interaction (HSI)*, pp. 95-100. 2019.
3) Jay Ligatti, Cagri Cetin, **Shamaria Engram**, Jean-Baptiste Subils, and Dmitry Goldgof. "Coauthentication." In *ACM Symposium on Applied Computing (SAC)*, pp. 1906-1915. 2019.
4) Jay Ligatti, Cagri Cetin, **Shamaria Engram**, and Dmitry Goldgof. "Systems and methods for generating symmetric cryptographic keys." U.S. Patent 10,291,403, issued May 14, 2019.
5) Jay Ligatti, Cagri Cetin, **Shamaria Engram**, and Dmitry Goldgof. "Systems and methods for generating symmetric cryptographic keys." U.S. Patent 10,298,391, issued May 21, 2019.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

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.