

UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

A Review of Formal Models of Security Mechanisms

by

Shamaria Engram

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

Verifying the correctness of computer systems with respect to a specification has been a long-standing area of computer science research. One increasingly popular way to ensure the correctness of a system is through the use of formal methods. Formal methods provide mathematical means to prove the correctness of computer systems and can be used in verifying and proving the security of such systems. Security policies are specifications that state the legal or illegal behaviors of computer systems. These policies can be ensured to hold on computer systems by enforcement mechanisms, which are traditionally classified by whether they operate statically (i.e., before the program under consideration executes) or dynamically (i.e., while the program under consideration is executing). This paper reviews both static and dynamic enforcement techniques and compares and contrasts the formal models employed to reason about these different types of mechanisms and the security policies that they enforce. Through this review, we identify a gap in the literature where there does not exist, as far as we are aware, a unified model to reason about arbitrary mechanisms.

August 21, 2019

11 AM

ENB 337

Examining Committee

*Yu Sun, Ph.D.
Graduate Program Director
Computer Science and Engineering
College of Engineering*

*Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering*