UNIVERSITY OF SOUTH FLORIDA

Defense of a Master's Thesis

Detecting RTL Trojans Using Artificial Immune Systems and High-Level Behavior Classification

by

Farhath Zareen

For the MSCS degree in Computer Science

Security assurance in a computer system can be viewed as distinguishing between self and non-self. Artificial Immune Systems (AIS) are a class of machine learning (ML) techniques inspired by the behavior of innate biological immune systems, which have evolved to accurately classify self-behavior from non-self-behavior. This work aims to leverage AIS-based ML techniques for identifying certain behavioral traits in high level hardware descriptions, including unsafe or un-desirable behaviors, whether such behavior exists due to human error during development or due to intentional, malicious circuit modifications, known as Hardware Trojans, without the need for a golden reference model. The use of Negative Selection and Clonal Selection Algorithms, which have historically been applied to malware detection on software binaries, to detect potentially unsafe or malicious behavior in hardware, are explored. This work presents a software tool which analyzes Trojan-inserted benchmarks, extracts their control and data-flow graphs (CDFGs), and uses this to train an AIS behavior model, against which new hardware descriptions may be tested. The proposed model can detect the specified (Trojan or Trojan-like) behavior with an accuracy of ~85% and an average false negative rate of 12.6% for Negative Selection and 12.8% for Clonal Selection.

Friday, February 15, 2019
2:00 PM
ENB 337

THE PUBLIC IS INVITED

Examining Committee

Robert Karam, Ph.D., Major Professor
Srinivas Katkoori, Ph.D.
Mehran Mozaffari Kermani, Ph.D.

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.