UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Models of Software Enforcement and Development
by
Hernán M. Palombo
For the Ph.D. degree in Computer Science and Engineering

Although a plethora of security solutions have been proposed and implemented throughout the years, security continues to be a problem for at least two important reasons, (1) implementations of runtime enforcement mechanisms have not been modeled rigorously and thus may not be enforcing the policies that are expected to enforce, and (2) there are conflicting tensions in the software development process that hinder the implementation and maintenance of secure software. To investigate these issues, this dissertation is divided into two parts.

The first part takes the lessons learned from earlier models of runtime enforcement---developed over the past nearly twenty years---and proffers a new general model called *Stream-Monitoring Automata (SMAs)*. SMAs unify previous models and is suitable for modeling security mechanisms that operate over infinite event streams, which are now widespread and have been previously left out.

The second part presents the results of an ethnographic work that spanned 1.5 years and studied secure software development processes using a unique adaptation of the participant observation method. Two researchers were embedded as software developers in a company, where they participated in everyday work activities such as coding and meetings, and observed and provided intervention on software (in)security phenomena as it unfolded. They observed developers' reactions to the discoveries of several vulnerabilities and their evolving attitudes towards security. The study found that (1) vulnerability discoveries produce different reactions in developers, often times contrary to what a security researcher would predict; (2) security vulnerabilities are sometimes introduced and/or overlooked due to the difficulty in managing the various stakeholders' responsibilities in an economic ecosystem, and cannot be simply blamed on developers' lack of knowledge or skills.

Examining Committee
Daniel Lende, PhD., Chairperson
Jay Ligatti, PhD., Co-Major Professor
Hao Zheng, PhD., Co-Major Professor.
Xinming Ou, PhD.
Dmytro Savchuk, PhD.
Nasir Ghani, PhD.

March 31, 2020
12:30 PM
Online (Google Meet)
Email hpalombo@usf.edu for more information.

THE PUBLIC IS INVITED

Publications

*1) **H. Palombo**, E. Dolzhenko, J. Ligatti, and H. Zheng, "Stream-Monitoring Automata", (ICSCA 2020)*
*2) Y. Cao, **H. Palombo**, S. Ray, and H. Zheng, "Enhancing Observability for Post-Silicon Debug with On-chip Communication Monitors", (ISVLSI 2018)*
*3) Y. Cao, H. Zheng, **H. Palombo**, and S. Ray, "A Post-Silicon Trace Analysis Approach for System-on-Chip Protocol Debug", (ICCD 2017)*
*4) **H. Palombo**, H. Zheng, and J. Ligatti, "Towards Precise and Automated Verification of Security Protocols in Coq", (Poster, CCS 2017)*
*5) **H. Palombo**, A. Tabari, D. Lende, J. Ligatti, X. Ou, "An Ethnographic Understanding of Software (In)Security and a Co-Creation Model to Improve Secure Software Development", (Submitted to SOUPS 2020)*

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.