UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Malicious Manipulation in Service-Oriented Network and Software Systems: Threats and Defenses

by

Dakun Shen

By taking advantage of design flaws in software security, cyber attackers are able to breach the service system for large and small organizations in both the public and private sector. In this dissertation, I will present two approaches we have been designed to tackle threats and challenges in software security. First, I will show a new class of content masking attacks against the Adobe PDF standard, causing documents to appear to humans dissimilar to the underlying content extracted by information-based services. I will also describe a lightweight alternative mitigation method against these attacks. Then, I will describe a research agenda that protects sensitive data in binaries from being corrupted by cyber attackers. In this work, the Intel Software Guard Extensions (SGX) technology is applied to create memory isolation in a way such that data-oriented attacks cannot use traditional memory corruption methods to tamper with sensitive variables.

Examining Committee
Zhuo Lu, Ph.D., Chairperson
Yao Liu, Ph.D., Major Professor
Jay Ligatti, Ph. D.
Xinming Ou, Ph.D.
Kaiqi Xiong, Ph.D.
Qiong Zhang, Ph.D.

Monday, May 13 2019
11:00 AM - 12:00 PM
ENB 337

THE PUBLIC IS INVITED

Publications and Patents

1) Dakun Shen, Lei Ding, Zhuo Lu, Yao Liu, Jay Chien-An, “Content Masking Attack Against Data Loss Prevention Solutions”, (Under Submission).
2) Dakun Shen, Tao Hou, Zhuo Lu, Hao Han, Yao Liu, Lei Ding, “AutoEnclave: Automating Protection of Sensitive Variable Security in Binaries based on SGX Enclave”, (Under Submission).
3) Tao Hou, Tao Wang, Dakun Shen, Zhuo Lu, and Yao Liu, “Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis”, (Under Submission).
4) Yao Liu, Zhuo Lu, Ian Markwood, and Dakun Shen, “Content Masking Attacks Against Information-Based Services And Defenses Thereto”, (Under Submission)
5) Dakun Shen, Ian Markwood, Dan Shen and Yao Liu, “Virtual Safe: Unauthorized Walking Behavior Detection for Mobile Devices”, IEEE Transactions on Mobile Computing (TMC), Jun. 2018.
6) Dakun Shen, Ian Markwood, Yao Liu and Zhuo Lu, “PDF Mirage: Content Masking Attack Against Information-Based Online Services”, USENIX Security Symposium (USENIX Security), Aug. 2017. (The first two authors are co-first authors).
7) Dakun Shen, Ian Markwood, Dan Shen and Yao Liu, “Virtual Safe: Unauthorized Movement Detection for Mobile Devices”, IEEE Conference on Communications and Network Security (CNS), Sept. 2016.

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.