SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING

COMPUTER SCIENCE COLLOQUIUM SERIES

Xiaojing Liao

College of William & Mary

Friday, March 2, 2018

3:00 pm

Luddy 0117

Attack, Cybercrime and Threat Intelligence: Towards Automatically Evaluating Security Risks and Providing Threat Intelligence

Abstract: The cyber threat landscape is quickly changing and it is of vital importance to stay abreast of emerging threats and to proactively work to improve security. To adapt to the rapidly evolving landscape of cyber threats, security professionals are actively exchanging cyber threat information through a public source. Such information, often presented in articles, posts, white papers etc., can be converted into a machine-readable format for automatic analysis and quick deployment to various security mechanisms like an intrusion detection system and anti-virus tool. With hundreds of thousands of sources in the wild, threat information is produced at a high volume and velocity today, which becomes increasingly hard to manage by humans.

In this talk, I will first present a set of high-impact attacks we found in the modern and security-enforced Operation Systems (iOS and OSX). Then, I will investigate how such vulnerabilities or exploits being weaponized and affecting millions of users in the wild. Finally, I will present iACE, an innovative solution for fully automated cyber threat intelligence investigation. It takes advantage of semantic-aware inspection technique to extract cyber intelligence of newly-appearing cyberweapons. This study sheds new light on the links across hundreds of seemingly unrelated attack instances, particularly their shared infrastructure resources, as well as the impacts of threat intelligence on security protection and evolution of attack strategies.

Biography: Dr. Xiaojing Liao is an Assistant Professor in the Department of Computer Science at William and Mary. She received her Ph.D. from Georgia Institute of Technology in 2017. Her research interests include data-driven security and web security, with the specific focus on the investigation of cybercrime and threat intelligence. Her works were published in the top-tier security conference including IEEE S&P, ACM CCS, etc. and were widely covered by the mainstream media including New York Times, CNN, Fox News, etc.

INDIANA UNIVERSITY

SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING