UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Qualifying Examination

Hamed Haddadpajouh

Monday June 28, 2021 at 2:30PM on Zoom

An Adversarially Robust Multi-View Multi-Kernel IoT Malware Threat Hunting Framework

Chair: Dr. Joe Sawada
Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour [Engineering]
Non-Advisory: Dr. Lei Lei [Engineering]
Non-Advisory: Dr. Charlie Obimbo

Abstract:

Today, cyber threats are becoming more complicated than anytime before. These threats cause a massive loss in social, political, and financial resources. Malware attacks have a significant share of cyber-threats in different platforms ranging from computer devices to critical infrastructure. The emerging trends of using Internet of Things (IoT) in our daily life bring up both promising prospects and security challenges. With diversified and numerous applications, IoT systems are now facing more security challenges than ever before. Malware is among the primary tool of cybercriminals to infect and exploit IoT devices.

Detecting malware threats (also known as threat hunting) allows security analysts to design a robust security posture against attackers' tactics, techniques, and procedures (TTPs). However, timely threat hunting is a complicated task as not only the security mechanisms encounter new malicious payloads that do not include single behavior, also threat actors use evading techniques like generating adversarial examples to bypass Artificial Intelligence (AI) powered defensive mechanisms.

In this research, we propose an adversarially robust multi-view multi-kernel mal-ware threat hunting framework for IoT environments. This framework consists of three elements:
1) multi-kernel IoT malware threat hunting module; 2) a generative model for evaluating malware threat hunting module against adversarial attacks in order to make an adversarially robust threat hunter model; and 3) a stack of deep models to detect adversarial IoT malware samples. The multi-kernel approach uses an aggregation function that grabs all kernels information to detect malicious payloads from a different view (bytecodes and op-codes). The generative model tries to bypass deep neural network models like the Malconv that use adversarial techniques such as Code-caves. Finally, the prevention mechanism tries to detect adversarial examples based on their feature spaces.