UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Defence

Tuesday May 30, 2023 at 2pm via Zoom [Remote]

Hamed Haddadpajouh

An adversarially robust multi-view multi-kernel framework for IoT malware threat hunting

Chair: Dr. Joe Sawada
Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour [SoE]
Non-Advisory: Dr. Lei Lei [SoE]
External Examiner: Dr. Shahram Heydari [Ontario Tech University]

Abstract:

Increasingly complex cyber threats are resulting in significant losses of social, political, and financial resources. One of the major cyber threats is malware attacks, which can target various platforms ranging from computer devices to critical infrastructure. With the rise of the Internet of Things (IoT), there are both promising prospects and security challenges. However, IoT systems are facing more security challenges than ever before due to their diversified and numerous applications. Malware remains one of the primary tools that cybercriminals use to infect and exploit IoT devices.

Detecting malware threats, also known as threat hunting, is a complicated task that requires security analysts to design a robust security posture against attackers' tactics, techniques, and procedures (TTPs). However, timely threat hunting is difficult as security mechanisms face new malicious payloads that do not have a single behavior. Moreover, threat actors use evading techniques such as generating adversarial examples to bypass artificial intelligence (AI)-powered defensive mechanisms.

To address these challenges, this research proposes an adversarial robust Multiview multi-kernel malware threat hunting framework for IoT environments. The framework consists of three elements: a multi-kernel IoT malware threat hunting module, a malware example generative module based on code-cave vulnerability, and an adversarial malware example prevention module based on statistical bytecode analysis. The multi-kernel approach uses an aggregation function to detect malicious payloads from a different view, including bytecodes and opcodes. The generative model attempts to bypass deep neural network models using adversarial techniques such as code caves. Finally, the prevention mechanism detects adversarial examples based on their feature spaces and an ensemble structure for deciding whether incoming samples are adversarially generated or not.

To evaluate the proposed framework, Precision, Recall, and Confidence Interval metrics are used to assess its accuracy in hunting malware samples. Additionally, an evasion rate metric is used to assess the robustness of the machine learning-based threat-hunting model against adversarial examples.

The framework is tested using an IoT cloud-edge malware dataset. This research contributes to the development of a robust malware threat-hunting framework that can detect IoT malware threats while mitigating adversarial attacks.