UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Defence

Wednesday March 20, 2024 at 1PM, online via Zoom (Remote)

Izabela Savic

Adversarial Sampling Attacks and Defense in DNS Data Exfiltration

Chair: Dr. Stefan Kremer
Advisor: Dr. Xiaodong Lin
Co-Advisor: Dr. Dan Gillis
Non-Advisory: Dr. Rozita Dara

Abstract:

The Domain Network System (DNS) protocol is used on a daily basis to access the internet. It acts as a phone book that allows users to access websites using words rather than remembering address numbers. In recent years it has become clear that there are serious vulnerabilities in the DNS protocol, and the lack of attention to these vulnerabilities (e.g. data exfiltration) is concerning. The widespread use of the DNS protocol opens a door that could possibly allow for companies and users to be hacked through malicious network traffic. Machine learning is a popular tool for malicious traffic detection, however they are vulnerable to adversarial samples. This leads to the security arms race, where researchers aim to discover and counter malicious threats before malicious actors do.

In this work, we demonstrate the success of adversarial samples of DNS exfiltration packets in bypassing machine learning detection techniques. We then propose a voting ensemble method to improve adversarial attack detection. The voting ensemble proposed increases the accuracy of adversarial detection, providing a new level of protection against adversarial sample attacks.