UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Wednesday April 27, 2022 at 3pm via Zoom

Sofiya Makar

A Framework for Automated Malware Authorship Attribution

Advisor: Dr. Ali Dehghantanha
Advisory: Dr. Fattane Zarrinkalam [SoE]
Advisory: Dr. Gautam Srivastava [Brandon University]

Abstract:

It is critical to have the ability to attribute the malicious software (malware) back to its source. The attribution process requires lots of resources and is time-consuming. However, it is not easy to automate this process using Machine Learning (ML) technologies due to various challenges such as different data distributions between criminal organizations or evasion techniques used by threat actors. We propose a Malware Authorship Attribution (MAA) framework, which is robust against these challenges. The idea is to pre-train a set of models on samples with the same distribution and transfer the knowledge from each mode into a single agent using the newly emerged Transfer Learning (TL) approach. We propose to implement a Graph Neural Network (GNN) as a backbone of the pre-trained models to deal with the evasion techniques. The final framework will be able to link the previously unseen piece of malware back to its author.