UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Tuesday Nov 5, 2019 at 10:30 AM in Reynolds, Room 2224

A Multi-view Deep Neural Network Framework For APT Malware Threat Attribution

Hamed Haddadpajouh

Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour [School of Engineering]
Advisory Committee: Dr. Xiaodong Lin
Advisory Committee: Dr. Raymond Choo [University of Texas San Antonio]

ABSTRACT:

Today, cyber threats are becoming more complicated than they were ever before. These threats cause a massive loss in social, political, and financial resources. Malware attacks have a significant share of cyber threats on different platforms ranging from computer devices to critical infrastructure. Malware is the main tool for threat actors, including Advanced Persistent Threat (APT) actors to conduct cyber attacks. Identifying the threat actors behind malware (also known as threat attribution) allows security analysts to design a robust security posture against attackers' tactics, techniques, and procedures (TTPs). However, timely threat attribution is a complicated task as threat actors keep changing their TTPs and produce new malicious payloads every day.

In this research, we propose a multi-view deep neural network framework for malware threat attribution. This the framework consists of three elements 1) a stack of deep learning models for attributing malware threats to malicious actors; 2) a fuzzy multi-view consensus clustering model for attributing the misattributed (by the stack of deep learning) malware samples, and 3) a decision support system for generating actionable malware threat attribution reports.

The stack of deep learners uses an aggregation function that grabs all deep models' attribution confidence rate and attributes a malware sample to a malicious actor. The fuzzy consensus clustering model tries to attribute samples that were misattributed by the stack of deep learning agents (because of the overlap between malware attributes). At last the proposed DSS generates a malware threat attribution report and recommends a course of action based on attribution accuracy generated by the stack of deep learners and the fuzzy consensus clustering model.

The main contributions that are offered in this research are: 1) building an aggregation function for a stack of deep learners to attribute an APT malware to its malicious actor; 2) developing a multi-view fuzzy consensus clustering model to attribute misattributed malware samples, and c) building a decision support system for generating attribution reports based on generated confidence interval from the stack of deep leaners and fuzzy consensus clustering models. Besides, we offer a vectorized APT malware dataset and an automated malware feature extraction system.

We evaluate the elements of our framework by Precision, Recall, and Confidence Interval metrics to assess the accuracy of the framework in attributing malware samples. Moreover, we test our framework by an APT malware dataset and the Microsoft malware competition dataset.