UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Tuesday April 25, 2023 at 3pm via Zoom [Remote]

Elnaz Rabieinejad Balagafsheh

Breaking the code: developing a framework for malware threat hunting using application logs

Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Fattane Zarrinkalam [SoE]
Advisory: Dr. Rozita Dara
Advisory: Dr. Jeff Schwartzentrub [eSentire]

Abstract:

Cybersecurity has become a critical concern in our daily lives as computer systems and networks continue to proliferate. Malware, in particular, poses a significant threat to system security, and detecting these threats can be challenging due to the rapidly evolving nature of malware and the sheer volume of data generated by computer systems. As a result, protecting against these attacks requires a range of advanced security techniques.

One such technique is malware threat hunting, which involves actively searching for indicators of compromise and using machine learning algorithms to identify anomalous behavior that may indicate a malware attack. While these methods have shown promise, they can also be limited by false positives, data quality issues, and other challenges.

An alternative approach to enhancing system security and detecting malware attacks is to leverage application logs, which contain valuable information about system events and user activities. By analyzing these logs, security experts can detect potential vulnerabilities, troubleshoot security problems, and conduct forensic analysis in the event of a security breach. However, analyzing application logs can be difficult due to issues such as massive data, limited contextual information, and device performance degradation.

This research proposes an efficient framework that addresses these challenges and improves malware threat hunting using application logs. This study aims to provide a practical and effective approach to enhancing system security and combating malware threats by detecting existing challenges and outlining the proposed framework and its benefits.