UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

Qualifying Exam

Friday February 16, 2024 at 1PM, online via Zoom (Remote)

Elnaz Rabieinejad Balagafsheh

A Framework for Threat Surveillance and Intelligence

Chair: Dr. Stacey Scott
Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Fattane Zarrinkalam [SoE]
Non-Advisory: Dr. Hassan Khan
Non-Advisory: Dr. Charlie Obimbo

Abstract:

In today's cybersecurity landscape, threats are growing in complexity, often involving unauthorized users who gain and maintain covert access to systems over extended periods. Log analysis stands as a robust tool for addressing these advanced threats. However, multiple challenges undermine its efficacy. Firstly, the complexity and volume of logs translate into unwieldy provenance graphs that demand advanced summarization. Unfortunately, existing summarization methods lack the specificity to detect advanced threats accurately, potentially eliminating nodes and relationships crucial for effective threat detection.

Transitioning from this initial challenge, we recognize that even if these graphs were perfectly optimized, the difficulty in predicting the next moves of attackers remains an unsolved issue. Current graph summarization techniques lack the specificity crucial for effective threat prediction, leaving security analysts in the dark about potential subsequent actions from attackers within the system. Finally, assuming we can appropriately summarize system logs and predict an attacker's actions, we confront the challenge of responding. Current incident response techniques are static and unsuited for the dynamic nature of cybersecurity. They struggle to balance between known and unknown threats to respond.

To address these interlinked challenges, the proposal introduces a ground-breaking framework to optimize threat detection and response. This framework employs specialized graph summarization techniques, incorporates predictive analytics, and advocates for dynamic incident response strategies. The paper serves as a comprehensive literature review, elaborates on the architecture and advantages of the proposed framework, and provides a well-defined research plan for furthering threat detection and response improvements.