UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Thursday July 29, 2021 at 11AM via Teams

Protecting Critical Infrastructures with
Efficient Cyber Threat Hunting and Intelligence

Abbas Yazdinejad

Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour
Advisory Member: Dr. Gautam Srivastava [Brandon University]
Advisory Member: Dr. Reza Parizi [Kennesaw State University]

ABSTRACT:

The exponential growth of the internet interconnections has led to increased threats and attacks against Critical Infrastructures (CIs). The vulnerabilities also toward CIs have increased dramatically over the last few years. Without any doubt, CIs play a vital role in our life. CIs are systems, technologies, and networks for any organization, government, or industry in electric grids, water networks, and transportation. Due to CI's critical role, the environment's and operations' security is a top priority. Therefore, the growing frequency of cyberattacks invokes the need to develop and implement more efficient security strategies.

Traditional preventive security measures are not able to counter cyber threats effectively. Cyber Threat Intelligence (CTI) and Cyber Threat Hunting (CTH) breed emerging security solutions in this regard. Indeed, CTI and CTH are applied as existing key solutions to tackle security issues in CIs. These minimize cyber threats by generating Indicators of Compromise (IoCs) feeds of the recent emerging cyberattacks to help organizations mitigate the attacks more effectively and efficiently. CTI and CTH provide the context needed for cybersecurity professionals to make well-informed decisions about security CIs. Threat feeds have a vital role here. Feeds incessant streams of real-time threat data to make information available on potential or existing threats, vulnerabilities, and risks.

This research proposes an efficient CTI and CTH framework to enhance the security of CIs via create a threat correlation engine, create new CTI techniques, and multi-view and multi-kernel deep learning system for CTH. Indeed, the development of the proposed framework will be a viable tool in CTI and CTH for CIs, which can apply in the vast area of the industry. Furthermore, this framework is comprehensive and useful in sensitive industrial systems and environments to deal with the growing cyber threats.