Automated generation of CTI knowledge graphs and attack graphs for continuous cybersecurity risk management

Record number : OPR-1265

Overview

RESEARCH DIRECTION

Amine Trabelsi, Professeur - Department of Computer Science

INFORMATION

amine.trabelsi@usherbrooke.ca

ADMINISTRATIVE UNIT(S)

Faculté des sciences
Département d'informatique

LEVEL(S)

3e cycle

LOCATION(S)

Université de Sherbrooke, campus principal

Project Description

In a context where cyber threats evolve at an unprecedented pace, traditional cybersecurity risk management approaches demonstrate their limitations when confronted with the complexity and diversity of modern attacks. This research project proposes an innovative approach based on artificial intelligence to automate and optimize real-time understanding of the cyber threat landscape.

The central objective consists of developing a continuously fed and updated CTI (Cyber Threat Intelligence) Knowledge Graph system, capable of integrating threat intelligence automatically extracted from heterogeneous information feeds and cybersecurity reports. This platform will leverage advanced natural language processing and machine learning techniques to identify, extract, and structure relevant information concerning threats, vulnerabilities, indicators of compromise, and attack tactics.

The project will concurrently develop a systematic pipeline for attack graph construction, establishing intelligent connections between the CTI knowledge graph and recognized external frameworks such as MITRE ATT&CK and CAPEC. This integration will enable the creation of sophisticated attack models providing a holistic view of threat scenarios and their complex interconnections.

The proposed architecture will integrate adaptive learning mechanisms enabling the system to automatically evolve with emerging threats. The graphs will be enriched through reasoning algorithms capable of identifying hidden patterns, predicting threat evolution, and suggesting proactive mitigation measures.

This research will produce reusable datasets and fine-tuned models made available to the scientific community, ensuring reproducibility and encouraging future developments in this critical domain for digital security.

Discipline(s) by sector

Sciences naturelles et génie

Informatique

Funding offered

Yes

Annual amount : 30 000$

The last update was on 26 August 2025. The University reserves the right to modify its projects without notice.