An ATTCK-KG for Linking Cybersecurity Attacks to Adversary Tactics and Techniques

Cameron Noakes

February 2022

1 Sentence Overview

The study conducted in this literature outlines a way to map cyber security attacks to tactics, techniques and procedures (TTPs) from the MITRE ATTCK framework.

The researchers leverage knowledge graphs techniques to detect and analyse cyber attacks, the study builds upon prior work and develops a vocabulary to extend a cybersecurity knowledge graph (KG) with adversary tactics and techniques from the ATTK framework. All for cyber threat intelligence (CTI).

Through the use of the vocabulary developed, a representation of rich threat intelligence instance data from ATTCK can be put into a knowledge graph (KG).

2 Introduction

Cybersecurity Threat Intelligence (CTI) can aid defenders in identifying vulnerabilities and attack patterns. The ATTCK framework supports various security use cases which can provide data for the CTI.

Often CTI resources can be very useful for security experts, and are typically difficult to relate to other cybersecurity information, due to this, several researchers addressed this limitation and started introducing knowledge graphs (KG) for cybersecurity information. Some KGs can integrate a number of cybersecurity standards such as STIX, CAPEC and CVE into an available ontology (branch of metaphysics).

Neither the Unified Cyber Ontology (UCO) or the SEPSES Cybersecurity Knowledge Graph (SEPSES CSKG) outlined in the literature for relevant models include the similar CTI used in the ATTCK framework, so a different threat modelling language called enterpriseLang based on the MITRE ATTCK framework Matrix was used as a solution that could be used to incorporate similar CTI as used in ATTCK for the development of the proposed solution. It uses a domain specific language (DSL) based on the popular Meta Attack Language (MAL) framework.

3 Knowledge Graph Construction

The researchers started developing the proposed solution by first by progressing and defining a knowledge graph. This was done by an ontology based on the existing schema used by MITRE in the ATTCK framework to represent and published attack data. The ontology developed for the knowledge graph creation consists of five main classes (Tactic, Technique, Mitigation, Adversary Group, and Software).

A linkable was defined (att:preventsTechnique) property to be able to link between the mitigations and any techniques. The "att:usesTechnique" property links the group to the Technique class in a similar approach to how the att:preventsTechnique can link remediation and techniques from the ATTCK framework.

The researchers then used RML16 (a declarative RDF mapping language) for mapping and transformation of MITRE ATTCK framework resources into an RDF-based developed ATTCK ontology.

4 Conclusion

In this paper, the researchers develop an extension to the SEPSES CSKG with cyber threat intelligence (CTI) similarities pointed out in the MITRE ATTCK framework and continue to then use it to link indicators of compromise to adversarial tactics and techniques.

5 What problem does this solve?

An extension was needed for the SEPSES CSKG to incorporate more CTI in relation to the ATTCK framework to provide better mapping of mitigations to ATTCK techniques.

6 How do they solve it?

By developing an extension of a knowledge graph and the use of cyber threat intelligence, this was about to better map ATTCK techniques to possible mitigation strategies such as link alerts from log messages to rich knowledge on techniques, providing in an overall better SEPSES CSKG model.

7 How do they assess it?

The researchers did not outline any specific way the proposed solution and extension to the SEPSIS CSKG model would be evaluated or assessed.