Towards automation of threat modelling based on a semantic model of attack patterns and weaknesses

Cameron Noakes

February 2022

1 Sentence Overview

The literature manages to unite the ATT&CK framework, CAPEC, CWE, CVE security enumerations. Active threat model development of a knowledge base was underwent in the proposed solution. The proposed model can be used to learn relations between attack techniques, attack pattern, weaknesses, and vulnerabilities to aid in building various threat landscapes for threat modelling. This is the usage application for the research and development of the solution.

The model is created as an ontology (a set of concepts and categories in a subject area or domain that shows object relationships) from open source datasets in Web Ontology Language (OWL) and Resource Description Framework (RDF) formats. The use of ontology's is an alternative structure to graph based approaches to help integrate the security enumerations.

The research conducted and the proposed solution consider an approach of threat modelling with the data components of ATT&CK framework knowledge base and an ontology driven threat modelling framework.

An evaluation is also mentioned to have been concluded for the results on the research and development, such as how it can be possible to use the ontological approach of threat modelling and which challenges were faced.

2 Introduction

The literature identified for threat modelling that having a list of potential threats to a system and its threat models, it can be possible to consider and implement the right security controls, mitigations or patterns for protecting the system fro Advanced Persistent Threats (APTs).

Questions were outlined in the literature in reference to threat modelling to identify key crucials when it comes to system security and these questions helped develop the research:

- Who could attack the system?

- How could attacks be done?

- Which weaknesses could exist in a system implementation?

A proposed answer to the above questions should be ideally a starting point for building a threat landscape. a common approach for quantitative criteria and metrics is proposed in the literature as to classify the security threats, mitigations and assets by the CIA triad (Confidentiality, Integrity, Availability), which would identify the key areas the security topics above relate to.

For the development of the knowledge base (proposed solution) by the researchers, the literature outlined how well known security enumerations can be used for the proposed solution development, such as Adversary Tactics, Techniques, and Common Knowledge (ATT&CK), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), and Common Vulnerabilities and Exposures (CVE).

Acknowledgement of specific challenges that arise was considered, of how the mentioned above enumerations are not organized in relation to their integrations and a challenge exists of automatic threat modelling, based on the security enumerations.

The proposed model developed can be used to learn the relations between attack patterns, weaknesses, and vulnerabilities, evaluate the quality of such links, and to build various threat landscapes to help protect systems from threats.

The literature explained how Description Logics (DLs) are a formal background of OWL datasets and enables knowledge-based analysis of system structure in order to enhance the security. The ATT&CK data components and sections such as tactics and techniques should be placed in a system in order to recognize and monitor selective attacks from within the ATT&CK framework matrix.

3 Linking security enumerations

The proposed model developed by the researchers links the ATT&CK framework, CAPEC, CWE, and partially CVE entities into a single ontological knowledge base with also using references from their descriptions.

The datasets used were OWL and RDF to help develop and structure the research which also in turn helped with the overall analysis and development of the proposed solution and the datasets can be found here: https://github.com/nets4geeks/OdTM

To build the knowledge base solution, a scraping tool using Java, OWL and an API was used that takes files of the enumerations and creates the resulting datasets of an informal representation of concepts and properties.

The process of the united mapping is done in the format and order of threat attack pattern is first mapped to ATT&CK tactics and ATT&CK techniques (separately) and then the ATT&CK techniques are mapped to CAPEC, CAPEC is further mapped to CWE and then finally CVE. As demonstrated in the diagram of figure 1.

The ATT&CK STIX representation also has the entities of tactics that are mapped with the attack patterns by the 'refToTactic' property in the ontology. The ATT&CK techniques have external references to the CAPEC entities that are placed in the ontology by the 'refToCAPEC' property. The 'refTOCAPEC' and the other properties also were referenced and included in figure 1 within the literature.

The referenced work in this section was mentioned by the researchers for how two improvements to their framework were done in relation to this work referenced which was the Ontology driven Threat modelling (OdTM) framework which utilizes an idea of representation a system structure. One of the improve-

ments was an option of starting modelling threats from a set of CAPECs, CWEs, or CVEs.

4 Conclusion

Within the literature, for this work, it described the ontological approach of integration of well-known security enumerations (ATT&CK, CAPEC, CWE, and partially CVE) into the single formal knowledge base for threat modelling. The ontological approach could be an alternative to graph based methods. The researchers exclaimed how quantitative challenges can be overcome by applying various statistical, machine learning, and natural language processing techniques.

5 What problem does this solve?

The researchers found an issue of how there is currently not a lot of resources or models mapping common knowledge bases, threat models and security enumerations together.

6 How do they solve it?

The literature research and proposed solution developed a knowledge base that can be used for threat modelling that incorporates all security enumerations and the ATT&CK framework to provide better and more information for how to secure systems.

7 How do they assess it?

There was mention of evaluation happening in the introduction but apart form some automation that was not elaborated upon, there was none.