ThreatZoom: Neural Network for Automated Vulnerability Mitigation

Cameron Noakes

February 2022

1 Sentence Overview

The proposed solution is to conduct mapping all the way from CVE to CAPEC and then to the ATT&CK framework automatically using various methods of machine learning (ML), deep learning, and natural language processing to find the appropriate mitigations for each publicly known information security model (CVEs and CAPEC) vulnerabilities.

The researchers introduced a neural network model which successfully classifies CVE to CWE automatically and are working on a deep learning model to automatically map and classify CWEs to CAPEC.

A hierarchical neural network is used to estimate the class associated with each instance of vulnerability databases such as CWEs and CVEs.

2 Introduction

Conclusions on attacks are given by the researchers identifying how mapping a vulnerability to CWE leads to understanding software, system, or architecture flaws that allow relevant exploits. Mapping vulnerabilities to threat models can also help to understand potential impacts and identifying ways to prevent attacks.

Threat actions (attacker steps) were extracted from CWE, CAPEC and ATT&CK framework matrix.

The researchers start the initial literature with a proposed novel algorithm that automatically estimates the CWE class corresponding to a CVE instance.

Their novel algorithm takes textual descriptions from each CVE instance as an input and then outputs the list of CWE classes it relates to.

Visualisation is provided through a flow diagram to determine how each topic and area relates to the others and in what order. It is shown that CVEs are mapped to CWE weaknesses and then these are subsequently mapped to CWE mitigation strategies where the 'cause and effects' for CWE weaknesses are further mapped to CAPEC and the ATT&CK framework and these are then mapped to mitigation strategies for both of them as well. The threat actions can be mapped to CIS critical security control mitigations (CIS CSC).

The classification procedure consists of three steps:

- (1) pre-processing
- (2) feature extraction
- (3) hierarchical decision-making process.

With the novel algorithm extracting the textual descriptions from the name and existing CWE classes and their associated CVE instances.

3 Conclusion

The literature proposed a solution of mapping from CVE to CAPEC and then from CAPEC to the ATT&CK framework automatically using machine learning (ML), deep learning, and natural language processing do understand threat modelling more at an advanced level and provide better mitigation strategies.

4 What problem does this solve?

The researchers have identified a major challenge and limitation which was to discover an automated solution employing machine learning to process the in-

formation extracted from data without relying on humans to have cheaper and more precise defensive system so the human resources can be applied to other areas which require it more. The researchers solved this occurring problem.

The proposed model leads to prevent, detect, and mitigating the vulnerability flaws by mapping to mitigation strategies.

Exclaims and conclusions were made based on how there is currently as of now, no system to automatically perform these classifications which is a compelling reason for why manual classification is currently needed.

Removing the need for manual classification can free up resources for cyber security professionals to dedicate themselves to other areas of interest whilst also providing a result with minimal errors and no human errors since the automation mapping would be done through several generations of deep and machine learning.

5 How do they solve it?

This very short literature identified how conducted mapping all the way from CVE to CAPEC and then to the ATT&CK framework automatically using various methods of machine learning (ML), deep learning, and natural language processing can help with mitigation strategies.

6 How do they assess it?

There was no use of assessments.