Linking Common Vulnerabilities and Exposures to the MITRE ATTCK framework: A Self-Distillation Approach - Notes

Cameron Noakes

November 2021

1 Sentence Overview

A model titled CVE Transformer (CVET) is developed that automatically maps CVEs to MITRE ATT&CK framework techniques within the matrix to provide better mitigation strategies. Data is extracted from the 24,863 total CVEs from various exploitation databases.

2 Abstract - Notes

Harmful cyber attacks have cost on average 7.91 million dollars per breach, leading to over 446,000,000 exposed records containing sensitive information in 2019.

24,863 total known CVEs in which 8,482 were defense evasion CVEs and 6,647 were Open source intelligence (OSINT)/ Reconnaissance.

Clearly outlines how the industry does not have proper mitigation strategies when referring to common vulnerabilities and exposures (CVEs). The solution for this issue is to map CVEs to the Mitre Attack framework, providing a real world implementation of Mitre and increase the protection of critical infrastructure due to its mitigation strategies.

It continues to explain how the problem does not have a solution yet (since CVEs and Mitre Attack framework are separate entities) and proposes a model titled 'CVE Transformer' (CVET) to label each CVE with a corresponding tactic from one of the ten in the Mitre Attack framework to better understand the risk and how to better remediate/mitigate the vulnerabilities.

3 Introduction - Notes

Explains what CVEs are and how they are used to the reader to engage an understanding of what the paper is outlining and proposing.

Continues to explain what each CVE metadata outlines and how mitigation strategies are less present in this metadata, providing less remediation steps to resolve the vulnerabilities.

Each tactic in Mitre Attack framework comes with a mitigation strategy, which identifies a key aspect to remediating vulnerabilities.

Continues to explain how mapping each known CVE to a Mitre tactic for mitigation strategies is an exhaustive task manually which provides reasoning behind creating the automatic model of CVE Transformer (CVET) to efficiently aid in this task completion.

4 CVE Machine Learning - Lit Review - Notes

A literature review of a data machine learning paper to better predict the severity of a given CVE vulnerability was completed. It built graphs based on current knowledge, common weakness enumeration (CWE) list and also attack patterns.

Previous models have been used for similar purposes such as BERT, a pre-trained transformer model that gathers information from Exploit-DB to better enhance textual descriptions of the CVEs.

CVE Transformer (CVET) model is of similar design and is a more advanced, re-purposed version of BERT model to better outline mitigation strategies for known CVE vulnerabilities.

5 Self-Knowledge Distillation - Notes

These are developed by having a pre-trained model train a new, untrained model and due to this, allows a better analysis to unseen data in comparison to a model without knowledge distillation.

6 Research Gaps and Questions

The paper speaks about how the data machine learning models for CVEs do not directly tie them to the Mitre Attack framework and only tie them to metadata such as CWEs and vulnerabilities.

rhetorical Question is given:
"How can we create a novel and accurate link between CVEs and ATTACK tactics through their textual descriptions and long-term dependencies?"

7 CVET Architecture Modelling

The CVET model that is proposed in this research paper is based on the trained BERT-based model due to the effective nature of text classification tasks and its high performance, fine-tuning and self-Knowledge distillation designs. This model used python and the library 'Keras' for all deep learning modeling.

Mathematics was used to explain the model and benchmark experiments.

8 What problem does this solve?

The proposed model (CVET) and the paper helped to map out known CVEs to aid in better remediation and mitigation for vulnerabilities.

9 How do they solve it?

They provided a solution by creating a model to automatically map CVEs to Mitre framework tactics to better understand how to fix the vulnerabilities.

10 How do they assess it?

They assess the model and outputs from previous models, analysis outlines that the F1-Score sits at one of the lowest.

Text classification performance was measured and concluded that pre-training of the transformer models improved the performances of text classification tasks.

11 Conclusion - Notes

A model was proposed to automate the process of mapping known CVEs from the Exploit-DB to that of the Mitre tactics to better mitigate the vulnerabilities since CVEs do not outline mitigation to a good standard.

The mentioned model is pre-trained from a parent/teacher model to influence the performance of the newer CVET to conduct better functionality when it comes to the mapping of CVEs.