Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports

Cameron Noakes

January 2022

1 Sentence Overview

The literature analyses how the key important, most valuable pieces of information tend to reside within textual descriptions in threat modelling frameworks suck as Cyber Kill Chain (CKC) and ATT&CK framework. The research authors proposed a solution that automatically takes textual descriptions and extracts the valuable information to help with implementing and designing defensive countermeasures.

The literature aims at simplifying the task of manual extracting of textual descriptions by enabling automated extraction of valuable CTI information and investigates text multi-label classification techniques that can fulfill the outlined task.

2 Introduction

There are three main types of CTI:

tactical

operational

strategical

Threat information sources have increased over time and support the development of standard technologies and various formats a common example is STIX (Structured Threat Information Expression, standardized XML language for data about cyber threats).

Structured data can be generally handled simply through the use of online web scrapers and general parsers, however, unstructured data almost always requires security experts to read and manually extract the most relevant information, which can become time consuming and less efficient.

In a world full of innovation it is ideal to allow automation to do tedious and less efficient tasks and the authors realised this and decided to create the proposed solution to fix this issue.

The research and work conducted by the author researchers attempts to overcome this the task of manual extraction of textual descriptions by simplifying the extraction of valuable security information using the ATTCK framework and automation.

3 Methodology

For the evaluation of the proposed solution the researchers tested several classifiers (the researchers only focus on binary relevance and classifier chains and conclude to test different types of classifiers) and comparing different textual representations such as term-frequency (TF) and term frequency-inverse document frequency (TF-IDF) weighting factors to identify if the solution works as planned. After this evaluation the researchers defined several post-processing approaches to help and improve the classification results obtained.

4 Metrics

Mathematical algorithms are used in the metrics of the proposed solution for: precision, recall, and F0.5 score where The F0.5 score shows the representation of an average between the precision (pi) and recall (p) where TP is 'true positives'.

More algorithmic equations are presented in the research such as a directed tree where edges have required weights corresponding to the conditional probabilities between the two nodes in question and the direction is given by a mathematical algorithm and the use of Edmond's algorithm.

5 Multi-label classification

The researchers decided to split the classification by tactics and techniques, just like ATT&CK does, applying to each of the best parameters for their category. They continued to then start testing regular models, fine-tuning the hyper-parameters of the classifiers and aim at simple models.

6 Conclusion

The work presented in this paper aims at simplifying the task of manual extracting of textual descriptions by enabling automated extraction of valuable CTI information, namely Tactics, Techniques and Procedures (TTPs) from ATT&CK and investigates text multi-label classification techniques that can fulfill the outlined task.

7 What problem does this solve?

human-readable textual reports and must be extracted manually which contains the most valuable data within threat modelling frameworks such as ATT&CK.

8 How do they solve it?

In this paper, the authors evaluate several classification approaches to automatically extract Tactics, Techniques and Procedures (TTPs) from unstructured textual descriptions in threat model frameworks. This can prove valuable for better defensive countermeasures.

9 How do they assess it?

For the evaluation of the proposed solution the researchers tested several classifiers (the researchers only focus on binary relevance and classifier chains and conclude to test different types of classifiers) and comparing different textual representations such as term-frequency (TF) and term frequency-inverse document frequency (TF-IDF)