Attack Hypothesis Generation

Cameron Noakes

February 2022

1 Sentence Overview

The research and proposed solution is the Attack Hypothesis Generator (AHG) developed which takes advantage of a knowledge graph derived from threat intelligence to generate hypotheses regarding attacks that may be present in an organizational enterprise networks. Based on five recommendation algorithms, preliminary analysis can be provided by a security analyst.

AHG provides an attack hypothesis comprised unobserved attack patterns and tools presumed to have been used by the attacker. The proposed algorithms can aid security analysts by improving attack reconstruction and proposing new directions for investigation. Experiments can show that when implemented with the ATT&CK framework knowledge base, the algorithms can significantly increase the accuracy of the analyst's preliminary analysis.

2 Introduction

The researchers acknowledged how there are currently no fully automated Security Operations Centers (SOCs). Analysts often have responsibility for understanding, prioritizing, investigating, and responding to alerts since automation and machines/computers cannot fulfill these tasks.

Identification of how accumulated Cyber Threat Intelligence (CTI) can help analysts with reasoning about the goals and methods of relevant attack actors was expressed.

The proposed solution present is the Attack Hypothesis Generator (AHG), which leverages threat intelligence to provide insights on the methods and tools used in the attack to understand the attack and the attack pattern to a better standard to be able to protect systems better in the future.

AHG applies recommended system techniques on a threat intelligence graph level to generate insights about the ongoing attack which can be used to map the attack out properly and identify evidence. This can increase the efficiency of his investigations by improving the analyst's hypotheses and resulting in actionable investigative items.

AHG simplifies the investigations performed by computer forensic analysts. Its main contributions and elements are:

- 1) utilizing threat intelligence to improve attack hypotheses

- 2) improving the accuracy of hypotheses provided by the analyst by a factor of 1.37 on average

- 3) suggesting actionable items to guide the analyst through further forensic investigation.

3 Background and Related Work

Traditional methods for threat intelligence and forensic analysis are becoming insufficient due to the rapidly changing and evolving cyber threat landscape. One of the most significant challenges is the need to translate the accumulated CTI into operational steps.

Most of the traditional Artificial Intelligence (AI) methods do not take advantage of the knowledge accumulated through sharing CTI information.

A related work cited reference of resource 9 in the appendix built a platform that unified CTI reports into a graph representation and enabled information retrieval search based on their a novel similarity algorithm. This literature of related work was known to be useful to the researchers for providing the research on CTI reports to identify a better understanding for when it comes to the proposed solution.

4 Proposed Solutions

The researchers build a knowledge graph consisting of the following types of SDOs: Campaign (C), Malware (M), Intrusion Set (IS), Attack Pattern (AP) etc. They then distinguish between the attack representation SDOs and attack descriptive SDOs.

Definitions of knowledge graphs (KGs) are given and the definitions are expressed through mathematical expressions.

Further more in-depth mathematics and mathematical algorithms are used for instance, the score of each descriptive SDO d D is calculated and specific edge weighting. Another mathematical algorithm is used for calculating the ProjD which takes into account the similarity between descriptive SDOs in terms of the attacks associated with them, the topology of KGD is not considered there.

5 Evaluation

The applications of ATT&CK knowledge base of adversarial tactics and techniques were used to build knowledge graph (KG). Algorithms are shown for the 'EvaluateAlg' variable which represents the average precision score and average precision improvement.

6 Conclusion

Within this literature, the researchers propose an approach toward an Attack Hypothesis Generator (AHG) that utilizes a knowledge graph (KG) derived from CTI information sets such as the ATT&CK framework matrix to improve the analyst's hypotheses of the related work papers. The proposed approach is said to be the first to focus on strategic CTI using recommender system techniques for attacks analysis and prediction.

7 What problem does this solve?

Traditional methods for threat intelligence and forensic analysis are becoming insufficient due to the rapidly changing and evolving cyber threat landscape.

8 How do they solve it?

Within this literature, the researchers propose an approach toward an Attack Hypothesis Generator (AHG) that utilizes a knowledge graph (KG) using CTI information sets such as the ATT&CK framework matrix to improve the analyst's hypotheses.

The proposed approach is said to be the first to focus on strategic CTI using recommender system techniques for attacks analysis and prediction.

9 How do they assess it?

In the literature in the evaluation section there was mention of the evaluation of the proposed solution through mathematical algorithms and code, however it was difficult to pinpoint an actual evaluation assessment method used as the literature continued with examples instead of how it would be actually evaluated.