Mapping Cyber Threat Intelligence to Probabilistic Attack Graphs

Cameron Noakes

February 2022

1 Sentence Overview

This literature contributes with an approach that resolves the outlined problem by using cyber threat intelligence (CTI) feeds of known threat actors to enrich ADGs under multiple reuse. This enables security analysts to take proactive measures and strengthen their infrastructure systems against threat actors.

The proposed solution was to take cyber threat intelligence (CTI) data from ATT&CK framework and accurately map it to generating attack graphs through the use of specialised software like securiCAD and tested and evaluated through a simulation and its results.

2 Introduction

Acknowledgement of how the task of securing large IT infrastructures as a whole, threat modelling has emerged as a decent and promising approach. In order to estimate attack tree difficulty, which is what attackers need to do as steps, the nodes are associated with forms of resilience metrics such as attacker cost, capability, or time needed to succeed with each step/phase. This metric is dependent both on properties of the attacker and the technical implementation of the attacked system.

For a given attack scenario where the attack graph represents a single attacker targeting a certain system infrastructure, this dependency does not constitute an issue for the security analyst devising the attack graph.

The researchers acknowledge that there is a need for a consistent methodology and also for reusing the resilience metrics in the graphs and the proposed research in this literature developed by the researchers takes a step towards achieving this.

Attack graphs were described and mentioned for their relevance in the research conducted for this literature by the researchers, attack graphs are mentioned to have been generated as part of the approach defined by the Meta Attack Language and is the proof of concept approach presented in this paper.

cyber threat intelligence from the ATT&CK framework is used and applied to the mentioned attack graphs generated through the use of a popular threat modelling tool software known as securiCAD.

The overall motivation behind conducting this research and any proposed solutions the researchers may develop from the research or future work is concentrated on the work of enabling the use of attack graphs in the context of Security Operation Centers (SOCs) where the analysts require information on particular attackers and attacks conducted where the analysis tooling requires a high level of automation.

Mathematical algorithms are used to express the related work for calculating results of variables such as distributions and is mention of simulations running in the related works but not identified as the proposed solution for this literature research and work.

3 Conclusion

The researchers conduct in-depth research for cyber threat intelligence and the mapping of ATT&CK framework CTI to attack graphs and present a method to map attacker properties in terms of CTI data (from the ATT&CK framework) to attack graphs.

The developed proof of concept can take CTI data from the MITRE ATT&CK database and apply it to the probabilistic attack graphs generated by the threat modeling tool securiCAD. The simulation response verified that they were accurately represented in the attack graphs.

4 What problem does this solve?

CTI data and mapping it to attack graphs for defensive measures and mitigations in blue team operations to secure infrastructure to a higher standard.

5 How do they solve it?

The researchers identified the problem at hand and a good solution to fix this outlined issue through the use of taking cyber threat intelligence (CTI) data from the ATT&CK framework and accurately mapping the ATT&CK CTI data to attack graphs and testing them through a simulation.

6 How do they assess it?

They assessed the proposed solution through a simulation that applies the CTI ATT&CK data to the probabilistic attack graphs generated by the threat modeling tool securiCAD.