Defender Policy Evaluation and Resource Allocation Using MITRE ATTACK Evaluations - Notes

Cameron Noakes

November 2021

1 Sentence Overview

present a methodology that applies a game-theory procedure to the attack data derived from the Mitre ATTCK framework. GPLADD game is first translated into a Markov chain representation, then a simplification of advance persistent threat (APT) attacks, conclusively developing a method to estimate the transitional probabilities.

2 Abstract - Notes

Defender Policy assessments and resource allocation using the framework.

Time duration increase for multi-stage attacks, making it hard to pinpoint location and start date of initial attack.

3 Introduction - Notes

Explanation of infrastructure cyber defenders and how they resolve ongoing and persistent attacks in real time. Due to cyber defenders securing networks and infrastructure (internal or external) it requires resource allocation, how many resources will be dedicated to securing assets.

Implementing the Mitre Attack Framework into resource allocation and defense policies will help allow the cyber defenders to identify the common vulnerabilities which have a higher attack success rate to be able to mitigate these risks ahead of time.

The proposed solution outlined in this white paper enables numerical evaluation of defender policies against multi-step attacks. The solution calculates

the attack success metrics, such as:

time-to-success, distribution, and steady state distribution.

This process will allow real-world data from the Mitre Attack Framework into attack success metrics and defender response evaluations to help better defend critical infrastructure and company assets which will in turn reduce the attacker success rate and limit the risk.

Abstracted bullet points detail what is discussed within this white paper and each section will delineate information on the specified topic of discussion.

The papers introduction section details how an attacker attempts achieving his goals by executing attacks against enterprise network users in an attack campaign composed from multiple single attacks instead of multi-staged attacks.

4 Prior Work

The proposed solution is a theoretical model built on an extension of GPLADD games. GPLADD is a game-theoretic approach to indicate the attack success conditions as attack graphs and to also quantify attack success metrics. GPLADD game-theory is a 'game'/simulation between attacker and defender.

The Mitre Attack Framework information was leveraged to organise their Attack Evaluations which tested the capabilities of Extended Detection and Response (EDR), this made the application for the Mitre Attack Framework useful and a real world implemented activity.

Attacker options can be informed and develop the methodology and give ideas of attacks from Mitre Attack Framework since the framework adjoins all possible attacks and situates them under tactics and techniques to help aid cyber professionals (adversarial or not).

The researcher deconstructs some literature reviews he developed his paper on, these papers are referenced at the bottom as [26], [45], [2] and [3], where they deal with the problem of detection related trade offs and sensor data aggregation through game models like the GPLADD, but details how these papers

do not represent each step within an attack.

5 Approach

The GPLADD game is first translated into a Markov chain representation, then a simplification of advance persistent threat (APT) attacks, conclusively developing a method to estimate the transitional probabilities based on attacker and defender capabilities on available data.

There are also alternative approaches when it comes to these games models such as the PLADD game, where the defended offensively protects the infrastructure or assets which sets the attacker to reverting back to a previous stage of the multi-stage attack or back to the start entirely.

A GPLADD game consists of multiple PLADD games together connected by a graph structure. A PLADD game is a contest for control of a single resource where the control is fought for by the attacker and the defender.

These games, once applied, through the use of the Mitre Attack Framework will be able to evaluate the defence policies put in place and dedicate resources to vulnerabilities with high impact, risk and severity.

6 Markov Chain Representation

The representation for the models is explained here with various algorithmic equations using mathematics, a Markov transition matrix was also created and populated with transitional probabilities which was shown in the adjacent image in the research.

7 Research Gaps and Questions

"A full review of the corresponding literature is outside the scope for this paper" - It did not do much literature review due to this but still detailed findings from other papers found in the resource section.

Why did the researcher not provide conclusions for future work?

8 What problem does this solve?

A better solution for defense measures and resource allocation can be ascertained from the use of applying the Mitre Attack Framework and game theory models to defender policies which can conclude in an overall lower risk and a more secure critical infrastructure.

9 How do they solve it?

They propose the solution by developing a model based off of game theory model approaches whilst simultaneously applying the implementation of the Mitre Attack Framework to evaluate defense policies and risks and to also delineate resource allocations.

10 How do they assess it?

no mention of how they would assess this new model was mentioned. All that is mentioned is:

"The resulting attack metrics assessment can be used to develop or improve the defender policy for a given system"

11 Conclusion - Notes

A model was developed for specific classification for where resources should be allocated to, which improves the security of company assets since the most high risk assets are secured before any lower severity rating ones are.

This allowed evaluated trade offs for the defender actions, such as attack detection efforts and different stages of an attack.

The proposed model solution developed used the Mitre Attack Framework Evaluations APT3 data to numerically quantify attack success parameters and difficulty.