Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix - Notes

Cameron Noakes

November 2021

1 Sentence Overview

The researchers focus their study on enterprise networks and specifically aimed to propose a solution of a threat modelling language for enterprise network security and to make the model based on the Mitre ATT&CK framework matrix.

The proposed solution is developed by using the meta attack language framework to help detail specific information about the given environments (assets, security, attack steps, defences etc).

2 Introduction - Notes

The introduction briefly states examples of adversarial attacks such as Wanna-cry to outline a point that the topic is relevant but also prevalent but does not detail or explain what Wanna-cry is.

Acknowledges how cloud is now more developed than ever and due to this, has given threat actors another attack surface/ attack vector. An example is given for how a Trojan horse can be created from using an APIs metadata in cloud architecture.

Explains why a threat modelling solution is proposed - due to it being a common approach and allows identifying of main assets and the associated risks to such assets.

Explanation of the Mitre Attack Framework is given and how it is a knowledge-base matrix for offensive and defensive cyber professionals which will be used for the treat modelling language proposed solution.

3 Related Work - 2.2 Attack Simulations

States how threats can be modelled by attack trees and attack graphs and aim to show all the paths through a system that could lead to exploitation of a system with the end goal being that of the adversarial threat actor.

Various security tools are discussed about how they relate to security controls and vulnerabilities such as the topological vulnerability analysis (TVA) tool.

Speaks about how there are various open source tools that can create attack graphs fro interpreting vulnerabilities.

4 Enterprise architecture

Before outlined enterprise attacks can be discussed, the researchers understand the importance of explaining what an enterprise network is and the theory behind EA models which help with an increased understanding of enterprise systems with various types of analysis.

Metamodels are determined to be the core of EA models that identifies and explains the fundamental artifacts of enterprise networks. Metamodels help provide a clear overview of the structure and enterprise network dependencies.

One limitation with EA models is that they lack semantics making ti difficult for systems to understand the architecture description.

5 Tools based on the ATTCK framework

Mention of a system titled 'CALDERA6' was given which is detailed to be an automated adversary emulation system based on the ATTACK framework, it enables automated security assessments, however, one limitation is that it does not incorporate all tactics and techniques within the Mitre Attack Framework matrix.

6 Background

6.1 Adversary tactics

Outlines how the matrix in the framework has 12 tactics used for adversarial techniques to compromise a system but also its perspective to defend against such attacks.

The research conducted for the Mitre Attack Framework matrix is very throughout, they systematically take each tactic and expand on what the tactic covers, why it is important and how the end goal can be achieved.

Most papers did not go into as much depth as this paper did, by expanding on all the framework tactic allows the reader to fully comprehend how adversarial attacks and threats are executed and provides a perspective on how to mitigate outlined issues and risks.

7 Meta Attack Language

the proposed enterprise language is based on the MAL threat model that combines the analysis of probabilistic attack and defense graphs which can lead to automation of security analysis.

A throughout example of what the security analysis could entail is given, by providing a domain asset of an Operating system, a specific instance (OS and version) and attack steps such as viewing the bash history. This clearly details an example attack that would come under the tactics of the Mitre Attack Framework.

8 Design methodology

Design science research (DSR) is used to develop information security artifacts which offers a systematic structure for developing artifacts such as constructs, models, methods, or instances.

This section identifies the key steps in order for developing a DSR model for the artifact creation. The first section explains how it is necessary to increase

the level of security for enterprise networks so that they are more resistant to cyber threats.

9 Enterprise threat modeling language

enterpriseLang is said to be designed as an attacker based technique threat modelling language that can assess the overall risk against enterprise systems and infrastructure. To create a enterpriseLang there are three main steps for a construction process which the paper discusses:

1. extract information for each technique from the Mitre Attack Framework matrix.
2. convert the extracted information into MAL files (format of .mal).
3. Combine the created files into one language (such as enterpriseLang.mal).

The given section also describes detailed information regarding accounts targeted (admin account and windows accounts) when outlining an overview of the language however, this is out of scope for discussion in this paper. (the paper i will create).

10 Evaluating enterpriseLang

An evaluation is considered for the enterprise language created in the previous section. The researchers detail five methods in which can be used to evaluate the output of DSR and the enterprise language. The researchers decide on choosing 'testing' as the evaluation method since the enterpriseLang can be compared to that of source code

The paragraph then speaks about how 44 unit tests are conducted to ensure each function works as expected, secondary tests are done of integration to ensure the combination of different techniques function as expected as well.

Adjacent subsections describe and explain various examples of cyber attacks which are not too relevant to Mitre being implemented or that of the research conducted.

11 Research Gaps and Questions

The paper included very little about enterprise network internal infrastructure systems such as computers, routers, firewalls etc.

no mention of other threat modeling relating to Mitre were discussed which would allow transparency and considered further tactics to be implemented from various spin offs of Mitre (such as Mitre for ICS SCADA systems).

12 What problem does this solve?

The problem that is outlined is that enterprise networks are a huge asset and often get targeted by malicious threat actors, therefore, developing a threat model to mitigate these risks will overall create a better impact to security of such systems.

13 How do they solve it?

The research proposed a solution in which the researchers create a threat modelling solution with usage of an enterprise language to better secure systems relating to enterprise networks.

14 How do they assess it?

They assess the enterprise language after the construction of it through the use of testing in order to accurately assess the functions within the enterprise language file since the file is similar to source code, and the best way to assess the source code is by testing it.

15 Conclusion - Notes

The researchers detailed research on the Mitre Attack Framework and mapped it to a new threat model which did a developed job of identifying vulnerabilities and risk to better secure systems that belong to that of enterprise networks.

the proposed solution using enterpriselang allows attack simulations based on the Mitre Attack Framework for enterprise systems. The simulation data when conducting analysis can allow information regarding security settings and infrastructure changes to secure devices more effectively.