Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training

Cameron Noakes

December 2021

1 Sentence Overview

Real world data was analysed from the Mitre ATTCK framework to propose CyTEA, a model that can generate simulated cyber threats in a cyber security training system and blueprint cyber threats in a cyber security training system.

The simulation level was examined based on procedural, environmental, and consequential similarities to conclude if the model has real world need and if the model is acceptable for usage in the industry.

2 Introduction - Notes

The paper is a Korean translated paper, reasoning behind choosing it is due to the abundance of information and real world affect the proposed solution has.

The proposed, developed solution can model threats and generate simulated cyber threats used in real world cybersecurity training systems.

Explanations of how hyper-connected society is now and due to this, requires more cyber security in order to protect industries and society. With gives reason behind the development of the proposed and developed solution.

Explanations of how red team simulations are more common when regarding threats in cyber security and how the simulation maps itself to one of these sectors in order to generate threats automatically (automation).

CyTEA stands for Cyber Threat Emulation and Automation which is the complete name of the model developed.

Rhetorical Question:
What are the expected outcomes of training results when defending against real cyber threats?

The proposed solution is said to have a confirmed effectiveness in cyber security training.

3 Att&ck Framework

This section details the original of the Mitre Attack framework and specifics relating to its purpose, its need etc.

For the developed solution it is said that the researchers used the tactics and techniques from the Mitre Attack framework.

Statement about how, as of July 2020, the Mitre Attack Enterprise has 184 technologies identified.

Information on the attack method used from Mitre Attack for Enterprise was expressed using its tactics and techniques.

Ends with an overview of how various cyber security areas reference Mitre Attack framework (since it has so many applications within the industry when applied such as threat modelling).

4 CyTEA

The CyTEA model is said to have been modelled for cyber threats and train cyber security accordingly in order to simulate a real threats in the system.

The CyTEA model is decomposed into modules. The first module speaks about the threat process and the scenario in which the threat will unfold. The second module is to understand the authored cyber threat scenarios and execute the threat according to the plan.

5 Cyber threat emulation

Part of the proposed solution is a cyber simulation threat execution tool that executes a simulated threat and is python-based script that can execute threats and collect the results of the execution.

From these results stems further cyber threats that are created based on relating to the previous threats functions of that branch.

This setting and execution script can be in forms of a plug-in to allow other developers and researchers to add to the script for more functionality or to rewrite the use.

The unit threats are according to whether the outcome is a success or a failure which would allow the next unit threat can be executed.

This paper is very technical on topology diagrams and discusses various attacks relating to the Mitre Attack framework matrix as well as beyond this scope. Such examples are IP blocking, Spear phishing, Operation Dust Storm and training simulation environment.

6 What problem does this solve?

The apparent need for more cyber threat simulations to train cyber professionals in defending critical infrastructure which can also model cyber threats for further analysis of APTs.

7 How do they solve it?

Solving the outlined problem within the paper was done by proposing and developing a model titled CyTEA that can be used to model cyber threats and generate simulated cyber threats in a cyber security for training of cyber professionals.

8 How do they assess it?

The researchers engage in assessing the simulation after development to assess its overall functionality and its apparent need within the industry. It was examined based on procedural, environmental, and consequential similarities.

9 Conclusion - Notes

The researchers confirmed that the actual defense training using simulation threats is the same as using real cyber threats in the cyber security training system.