Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets

Cameron Noakes

January 2022

1 Sentence Overview

Acknowledgement of how attack situations (representing the execution order of techniques) should be according to the users objective and outlines the issue of how there is a limit to manually generating various attack sequences reflecting the characteristics of the intrusion process. This literature proposes an automatic generation method of various attack sequences that satisfy the characteristics of the attack desired by the user based on the tactics and techniques of the ATT&CK framework.

The researchers analysed existing ICS incident reports to determine the probability of a successful attack sequence, this metric was then used as a parameter for the HMM Markov model. Incorporating attack sequence generation based on the hidden Markov model (HMM) for ATT&CK framework representation.

2 Introduction

Attack situations are described to be essential for security research that is carried out on specific infrastructure. An attack sequence is defined as a series of attacks made by an adversary.

The researchers proposed developing diverse datasets for ICS testbeds to generate and reproduce attack sequences since these attack situations require data in order to be created and based upon.

Implementation of a method incorporating attack sequence generation based on the hidden Markov model (HMM), which is capable of representing the ATT&CK framework was integrated into the proposed solution dataset.

The researchers analysed existing ICS incident reports to determine the probability of a successful attack sequence, this metric was then used as a parameter for the HMM Markov model.

3 Background for Mitre for ICS

The researchers outlined the definition for Attack for ICS matrix: compiles security threats relating to control systems from the viewpoint of an attacker perspective and mindset to outline possible attacks and grouping of threats that could be attempted. ATTCK for ICS constructed a matrix by mapping a total of 96 types (81 types when excluding duplicates.

4 Attack Sequence Generator

The literature created a set of attack sequences required to be differently generated as user objectives can be a variety, user requirements are commonly reflected in ATT&CK for ICS hence the infrastructure of ICS as an example. ATT&CK for ICS provides a framework that can express various attacks on embedded critical infrastructure.

5 Generating Attack Sequence

From the research conducted and the usage of some datasets for ICS, incident reports and vulnerabilities for ICS equipment, correlated into the overall results that aided in the development of the proposed automatic attack situation generation. Analysis of the results, can calculate the frequency of transition between each tactic and the frequency of observed technique according to the tactic as a probability.

6 Future work - execution tool

Reproduction of the proposed solution was created for Purple Team ATT&CK Automation module. the researchers are currently developing an attack reproducing the automation tool based on Metasploit's msfrpc module to facilitate various attack reproduction and create a dataset of the information found from various runs of the model to develop over time.

7 Conclusion

This literature identified gaps in research and attack situations and steps where static manual versions would only be possible. This paper concluded on a proposed model of dynamic attack patterns and situations to further better develop cyber skillsets and give a vairety to attacks to help prepare individuals better.

8 What problem does this solve?

Various attack situations within cyber security have a limit to manually generating various attack sequences for different situations and alternation of such situations, since manually generating these situations takes time it is time spend where it could be used elsewhere. The automatic generation of attack situations mitigates this problem.

9 How do they solve it?

This literature identified the problem and continued to then propose an automatic generation method of various attack sequences that satisfy the characteristics of the attack desired by the user (the user objectives) based on the tactics and techniques of the ATT&CK framework.

10 How do they assess it?

attack cases were analyzed from the viewpoint of the ATT&CK framework and an attack sequence was generated based on self-defined rules.