Expansion of ICS Testbed for Security Validation based on MITRE ATTCK Techniques - Notes

Cameron Noakes

November 2021

1 Sentence Overview

Introduces a method to expand the existing testbeds for ICS systems so information can be collected during an ICS cyber incident based on the Mitre ATTCK framework. This method is to also be useful for creating long term attack simulations for ICS systems.

2 Introduction - Notes

The papers introduction opens with how exposed systems to attackers can result in cyber attacks and a case of an attacker sitting inside of the network for 6 months gathering information, which is then explained as the reasoning behind why we need to monitor and analyse ICS systems.

2.1 Monitoring field selection - Analysis Method - Notes

Information was collected on specific fields and methods and then can be used to detect security threats within the network environment for adversaries, this was done by analysing the Mitre Attack Framework, this analysis method can also help prevent cyber threats made by adversarial attackers.

2.2 HAI testbed expansion - Analysis Method - Notes

HAI is a testbed that consists of a turbine system depending on the cyber threat scenario, the HAI testbed can reproduce the attack and also collect changes in the information of the ICS control system.

2.3 Dataset enrichment - Analysis Method - Notes

When analysing ICS data there are limitations with the availability of controllers, data enrichment helps resolve this problem. It can improve data sets scalability in various attack scenarios and can modify previous data sets.

3 Mitre Attack Framework- Notes

Explains that the Mitre Attack Framework is a threat knowledge database that contains tactics and techniques for offensive and defensive attacks based on real world observations and scenarios.

Brief mention about its history arose with regards to its original functionality and what it was specifically developed for, such as being made to target Windows originally, but now has included both Linux and Mac operating system targets.

Usage of the cyber kill chain and Mitre Attack Framework aided in the development of PRE-ATTACK, another framework for various other specific use cases.

The Mitre Attack Framework has been widely used in several projects within the industry of cyber security for adversary emulation, red teaming, behavioral analytics and various others.

4 Consideration of Target Domains - Notes

An addition to the Mitre Attack Framework is 'Mitre for ICS', a more in-depth framework based on real world Industrial Control System adversary attacks to better relate to specific industries. It requires additional data sources which are not in the original Mitre Attack Framework.

Regarding the 'Mitre for ICS' framework, the paper conducts further research into what other data sources may be of value, the conclusion came to target new tactics and as a result provided confirmation of needing OPC-based log information to be collected.

5 Data Diversity - Notes

With regards to expanding the HAI testbed it requires information to be collected from various different data sources for a more accurate response and result, this is partly due to different security applications being deployed and maintained therefore information is needed on these as well.

6 Attack Tools - Notes

This section said to have implemented three attack tools for adversarial simulations of offensive cyber threat attacks to reproduce attack scenarios in all areas of ICS.

6.1 Physics Based Attack - Notes

14 single attacks that focused on single physical points on output, set points and process value were implemented for attack scenario simulations and 19 complex attacks were implemented for multiple physical points.

6.2 Network Based Attack - Notes

This was another simulation implemented for ICS adversarial cyber attacks to better understand how to reduce and mitigate the attack threats and risks.

This simulation provided a way to generate malicious network traffic with regards to present vulnerabilities between ICS levels of 1 and 2.

6.3 System Based Attack - Notes

Uses automation of the purple team attack framework to attack system environments through simulated cyber attacks which uses post modules of Metasploit (a popular framework for exploitation of systems but also focuses its efforts on reconnaissance and post-exploitation) which reproduces the Mitre Attack Framework tactics, Msfrpcd can be used to inject user-defined attack scenarios into testbeds to take over remote control.

7 Research Gaps and Questions

The paper focused more on the theoretical implementation of attack tools to test attack simulations on ICS systems and critical infrastructure but however, did not elaborate to say what are the end goals and why it is important to simulate cyber threats.

8 What problem does this solve?

This problem solves a way to secure ICS and critical infrastructure equipment from cyber adversaries looking to exploit specific hidden vulnerabilities.

9 How do they solve it?

They propose analysis methods and attack tools to simulate cyber threats in order to better understand the adversarial behaviour behind such attacks and to be able to lower the overall risk of the ICS systems.

10 How do they assess it?

They assess the attack simulations performance through analysis of three components:
1. Monitoring field selection
2. HAI testbed expansion
3. Data enrichment

Which in turn result in a better, more secure ICS network environment that cyber professionals can isolate cyber threats more quickly and efficiently.

11 Conclusion - Notes

The paper proposed building a testbed that can collect datasets by analyzing the Mitre Attack Framework tactics and techniques to build attack simulations to enhance the overall security posture of critical infrastructure.