MITRE ATTACK for Industrial Control Systems: Design and Philosophy - MITRE Corp.

Cameron Noakes

November 2021

1 Overview

I CANNOT USE THIS PAPER AS IT WAS CREATED BY MITRE ABOUT THE FRAMEWORK, NOT A THIRD PARTY.

These are my notes on the alexander2020mitre. These are unofficial notes to summarise and outline what each paper is describing. Do this for every paper I review and take notes on.

This is my literature review for the paper, each paper will have its own note document (check menu showing all my documents in overleaf)

2 Exec Summary (abstract) - Notes

Discussion and reasoning of the Mitre Attack Framework for Industrial Control Systems (ICS) - Attack for ICS. It describes how the framework has progressed and how it can be used in the industry of ICS.

It continues to describe how an adaptation of the Mitre Attack Framework was developed in order to better suit industry sectors requiring secure industry control systems (ICS). The official Mitre Attack framework is more relevant to internal infrastructure.

3 Background of 'ATTACK for ICS' - Notes

The Mitre Attack Framework and the related 'ATTACK for ICS' framework is outlined in this paper to have some overlap however due to the nature of 'ATTACK for ICS' it has a primary focus on the actions that adversaries take against industrial control systems for better mitigation strategies.

Mention of how ATTACK for ICS is often used for internal red and blue teams in ICS environments typically seen in oil, gas and power sectors. Due to the level of demand from these sectors it was said to be crucial to develop a framework better suited to these specific systems.

'Attack for ICS' is explained further, the details of tactics (each tactic has a subsection of techniques) and techniques (the tactical objective by performing the action).

4 'Attack for ICS' Concepts - Notes

The framework illustrates recommended conditions used in order to determine if new techniques should be amended to the current knowledge base.

This section describes the four fundamental concepts of the 'Attack for ICS' framework. adversary (attacker) perspective, refine based on real world activity, Unreported incidents and use of abstraction to connect offensive and defensive measures.

4.1 Perspective - Notes

perspective of offense is mentioned to understand and take into consideration possible actions an adversary could make when targeting systems. This perspective continues to then allow the 'ATTACK for ICS' a wider and more accurate frame of reference when assessing and implementing defenses and countermeasures.

4.2 Real world activity - Notes

The 'Attack for ICS' framework is primarily based on real world cyber incidents and threats on industrial control systems, allowing a better design of the framework to be made and to also allow insight into identifying what are some of the main adversarial attacks performed.

Using real world scenarios to base the framework on can have advantages due to how relevant the framework is when regarding the real world attacks, and also provides accuracy to inform readers of adversary behaviours, capabilities and offensive activities.

4.3 Unreported Incidents - Notes

Unreported cyber incidents are discussed to make it more difficult to correlate all incidents into a new framework design but due to anonymity, can outweigh voluntary confidentiality.

5 Conclusion - Notes

'Attack for ICS' is an adaptation of the Mitre Attack Framework that specifically focuses on industrial control systems and critical infrastructure.

There is a slight overlap with each framework due to their nature for both offense and defense, 'Attack for ICS' primarily concentrates on securing ICS through offensive and defensive tactics.

Key details regarding the industry sectors was discussed and various others to articulate the reasoning behind the development of 'Attack for ICS' framework and to better secure critical infrastructure and industrial control systems.

6 Research Gaps and Questions

The paper did not mention any other frameworks and comparisons to find out if 'Attack for ICS' is the best fit for applying into ICS environments.

7 What problem does this solve?

A need for a specific framework for ICS equipment and systems.

8 How do they solve it?

research about how Mitre is a useful framework but doesn't necessarily correlate to ICS environments and identifies a gap for ICS to be closed. This is outlined to be a better fit for ICS when targeting ICS equipment in various fields.

9 How do they assess it?

They assess the frameworks through comparison to determine which one is better suited to being further applied to ICS environments, 'Attack for ICS' is a more advanced, specific version of Mitre Attack Framework specifically designed for ICS network environments which makes it a better fit.