Investigating Potential Indicators against Cyber-Attacks in Industrial Control Systems

Mohammed Asiri, Neetesh Saxena, and Pete Burnap
School of Computer Science and Informatics, Cardiff University, United Kingdom

Introduction

- Capabilities of identifying footprints of the of the attack.
- Indicators of compromise (IOCs) helps operators at utilities to react quickly to similar compromise incidents.
- Examine how effective the IOCs used in IT systems are in detecting cyber-attacks in the Industrial Control Systems (ICS).

Motivation

Cyber incidents 2,000% in 2019.

- **Stuxnet attack.**
- **Ukraine Power Grid attack.**

Research Questions

• What are industry people's perceptions on how effective these IOCs are for detecting security incidents in ICS?

• What additional IOCs to indicate a compromised system in an ICS environment?

• What challenges do security experts encounter in terms of developing IOCs associated with the ICS system?

Approach

Attack scenarios: *Stuxnet malware, Ukraine Power Grid attack, Man-in-the-Middle (MITM) attack, and Distributed Denial-of-Service (DDoS) attack*

Participants from the focus group: ***(n =9)*** *OT/ICS security experts.*

Identified IOCs: *based on similarities between traditional IT and ICS.*

Preliminary Results

- ***Perception of the effectiveness of IT's IOCs in the ICS domain:***

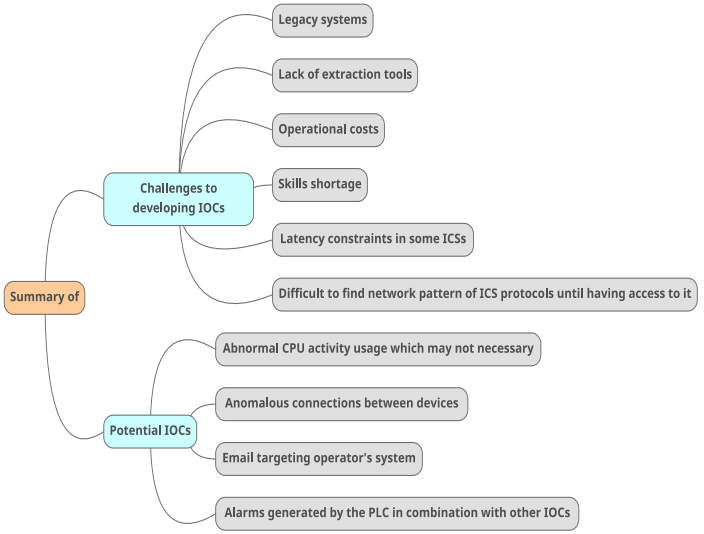
IOCs in ICS are quite similar to those in IT

Identified IOCs are effective in ICS domain

- ***Usability of additional IOCs:***

Anomaly detection can trigger an alarm + Combined with Other IOCs to be effective

- ***Developing IOCs:***



Conclusion & Future Work

- Most of IOCs are **applicable** and **effective** in ICS.
- Challenges associated with building such indictors are highlighted.
- Apply concrete approaches used by **SOC** in identifying IOCs associated with ICS systems.
- Extend questionnaire with more deep questions, managing collected responses and the overall results.

References

V. Atluri and J. Horne. A machine learning based threat intelligence framework for ICS network traffic indicators of compromise. SoutheastCon 2021, pp. 1–5.
A. Cook et al. The industrial control system cyber defence triage process. Computers & Security, pp. 70:467-481, 2017.