SAMIIT: Spiral Attack Model in IIoT Mapping Security Alerts to Attack Life Cycle Phases

Cameron Noakes

February 2022

1 Sentence Overview

The researchers present a machine learning (ML) classification approach for mapping cyber security alerts to IIoT attack phases and architectural layers. The results show the accuracy of the mapping mechanism and how it helps analysts in security operation centers to prioritize alerts and derive risk scores corresponding to each alert.

Within this research, the researchers first survey state-of-the-art IT and IIoT attack models, review their pros and cons for each in identifying detailed adversarial steps, and then propose a spiral IIoT attack model that takes all of those details into consideration.

Security analysts can use SAMIIT to visualize and classify security events to track adversary moves in each level and predict next possible activities.

This literature reviewed several attack life cycle models proposed for IT and IIoT networks, considered their limitations and future work.

They proposed SAMIIT, a spiral attack model to map IIoT cyber intrusions to different attack phases and architectural levels of IIoT environments. Then presented a machine learning classification approach for mapping security alerts to IIoT attack phases and architectural layers.

As a proof of concept implementation, the researchers evaluated their classifiers using ATT&CK dataset and showed the high accuracy of classification algorithms. This was a numerical dataset approach.

2 Introduction

Industrial Internet of Things (IIoT) networks have been discussed by the researchers to have been targeted by extremely sophisticated attacks such as Crash-override. Complex attacks are often implemented by coordinated single-step attacks organized and focused on specific targets within specific sectors.

The researchers identified a limitation with specific frameworks for how in efforts to apply CKC in identifying evidence for most of the attack phases for a cyber attack and proposing correspondent defense mechanisms, researchers have perceived that it cannot identify all phases of complex attacks due to the variance and complexity of some of the stages.

Acknowledgement of recent proposals within the same research area are expressed and identified to facilitate with the authors research on the same topic. and identify limitations with current methods Some IIoT attack models such as SANS Industrial Control Systems (ICS) cyber kill chain and ICS cyber defense triage process have been proposed in recent history.

These models are still based on Cyber Kill Chain and do not cover all of the phases of IIoT attacks due to their complexity and other reasons.

Within this research, the researchers first survey state-of-the-art IT and IIoT attack models, review their pros and cons for each in identifying detailed adversarial steps, and then propose a spiral IIoT attack model that takes all of those details into consideration.

Explanations of how applying a thorough and accurate IIoT attack model would help security analysts better understand attack life cycle, prioritize and focus on specific security controls and their logs/alerts at each phase.

3 Spiral Model

The referenced 'Figure 4' within the literature in this section depicts SAMIIT, this model consists of two parts:

- linear
- spiral.

The Spiral section of the model of SAMIIT includes architectural levels of IIoT networks. When exploitation is successful and a host is compromised, the adversary will either execute the final action and the attack life cycle ends.

Security analysts can use SAMIIT to visualize and classify security events to track adversary moves in each level and predict next possible activities.

It is almost impossible for SOC analysts to review every single alert and manually map them to a sector and a level in that sector. Therefore, an automated event classifier that maps alerts/logs to these sectors and levels is of great help and improves the performance of SOC processes. The researchers propose a machine learning classification approach to map alerts/logs to SAMIIT.

4 Conclusion

This literature reviewed several attack life cycle models proposed for IT and IIoT networks, considered their limitations and future work and proposed SAMIIT, a spiral attack model to map IIoT cyber intrusions to different attack phases and architectural levels of IIoT environments. Then presented a machine learning classification approach for mapping security alerts to IIoT attack phases and architectural layers.

5 What problem does this solve?

It is almost impossible for SOC analysts to review every single alert and manually map them to a sector and a level in that sector. Therefore, an automated event classifier that maps alerts/logs to these sectors and levels is of great help and improves the performance of SOC processes.

6 How do they solve it?

an automated event classifier that maps alerts/logs to these sectors and levels is of great help and improves the performance of SOC processes. The researchers propose a machine learning classification approach to map alerts/logs to SAMIIT.

7 How do they assess it?

As a proof of concept implementation, the researchers evaluated their classifiers using ATT&CK dataset and showed the high accuracy of classification algorithms. This was a numerical dataset approach.