Research on System Architecture and Methodology based on MITRE ATT&CK for Experiment Analysis on Cyber Warfare Simulation - Notes

Cameron Noakes

November 2021

1 Sentence Overview

Proposed a system configuration model (specific elements that define or prescribe what a system is composed of) based on the Cyber Kill Chain and the Mitre ATT&CK framework to return analytical data resulting in providing infrastructure protection mitigation strategies.

2 Abstract - Notes

This is a Korean paper and has been translated.

The analytical data mentioned originates from the original attack threat simulation developed as the proposed solution.

The introduction gave a proposition for system architecture and methodology based on the MITRE ATT&CK framework to help aid in cyber warfare simulations and analysis.

MITRE ATT&CK Framework has been applied to industry for a specific purpose of analysis on cyber warfare. The framework is said to be used in conjunction with the cyber kill chain (CKC) to create a solution for strategic decision making, offensive or defensive. Allows for mapping out of cyber attacks and for preemptive defence measures.

3 Introduction - Notes

The system architecture and virtual model discussed uses the MITRE ATT&CK Framework for design and implementation.

This paper focuses on cyber warfare architecture and virtual models based on the MITRE ATT&CK framework to better understand the continuous development of sophisticated attacks.

The evaluation of the risk in infrastructure from preparation for cyber attack and defense simulations is reduced due to improving network resilience and allowing professionals to have more applied knowledge.

4 Cyber Kill chain and Mitre Framework - Notes

Details about CKC and how the usage of the MITRE ATT&CK Framework would help to create virtual models and system architecture for threat simulations for advanced cyber warfare training.

The framework described was explained to be the adversarial attackers life cycle for Advanced Persistent Threats (APTs).

Continues to delineate the reasoning behind why the Mitre framework is used for this simulation modelling and how it has been implemented for the purpose of Threat Detection and Response due to it being knowledge based and continuously reflecting new attack objectives and methods.

5 System Configuration - Notes

The simulation outlined in this paper refers to using both cyber kill chain and MITRE ATT&CK framework to uncover attacks and leveraging defense policies for APTs. Analysis of the results will conclude on mitigation strategies recommended through the involvement of the simulation to increase the overall security of internal infrastructure.

6 Cyber Attack Modeling - Notes

Detailed specifics of the techniques in Mitre framework and cyber kill chain are expressed. An explanation is given for how an attacker could compromise a system from initial access to then move laterally around the network.

7 Experiment - Notes

Discussion of analysis of the possible risk and degree of damage and how it can establish mitigation measures in order to protect the critical infrastructure. The analytical data originates from the original attack threat simulation.

8 Conclusion - Notes

This paper proposed a system configuration and model based on the cyber kill chain and MITRE ATT&CK framework to return analytical data resulting in providing infrastructure protection mitigation strategies.

MITRE ATT&CK was used for this cyber warfare simulation research objective in order to design and implement a clear resulting solution for analytical data based on the simulation model to mitigate high risks for infrastructure.

9 Research Gaps and Questions

The paper did not specify much information about what the cyber kill chain is and how it relates to the Mitre Framework, but did elaborate well on the MITRE ATT&CK Framework, where it is used, how it is used and so on.

The paper outlined how analysis of the simulation and cyber professional actions would help secure infrastructure but did not say how they would analyze the information and what methods would be used.

10 What problem does this solve?

The simulation aids to train cyber professionals to help reduce overall risk by further training of what attacks that could be presently executed, making critical infrastructure and network environments more secure and at the same time protect information.

11 How do they solve it?

They solves the problem at hand by proposing a solution, a simulation that would help train cyber professionals in cyber warfare to be able to identify malicious intent faster and more effectively, making the overall risk decreased and the overall cyber security of an environment increase.

12 How do they assess it?

They assess through the analysis of the simulation to determine if the simulation is a success and what attacks and defenses have been outlined within the simulation to know what is more prevalent to secure/mitigate.