Poster: Cybersecurity Chess Manual: A Security Concept Predicting Typical Future Confrontation Scenarios

Xingchen Wu[*], Jiaqi Li[†], Yang Yu[‡], Jian Chang[§], Yang Zhao[¶], Lvyang Zhang[‖], Lidong Zhai[(✉)**]
[*]6School of Cyber Security, University of Chinese Academy of Sciences
[*]267Institute of Information Engineering Chinese Academy of Sciences, Beijing, China
[‡]Tencent Security Xuanwu Lab, Beijing, China
[§]China Unicom Online Information Technology CO.,Ltd, Beijing, China
[¶]China National Software & Service Co.,Ltd, Beijing, China
Email: zhailidong@iie.ac.cn

***Abstract*—The development of advanced network security concepts such as Zero Trust is in full swing, and cutting-edge network security technologies such as active defense, mimic defense, and trusted computing all attach great importance to upgrading strategic thinking. Cyberspace has become the frontier of confrontation, and national and urban infrastructure has become a key ”target” of cyber warfare. To this end, we propose to design a security concept called ”Cybersecurity Chess Manual” to summarize past theories and predict typical confrontation scenarios in the future. Cybersecurity Chess Manual is a strategic leap to realize the leap of concept and technology level.**

keywords: Network Attack And Defense; Network Security Confrontation; Cyber Range

I. Introduction

At present, network attacks are increasing day by day and have become the primary security issues faced by fast-growing industries such as the Internet, Industrial Internet and Space Internet. National and urban infrastructure have become cyber warfare’s key ”target” [4]. In 2021, Colonial Pipeline, a large U.S. oil product pipeline operator, was attacked by ransomware and shut down four of its primary product oil pipelines [3]. In 2022, the FBI and CISA disclosed in a new joint security bulletin that the Cuba ransomware gang had earned more than $60 million in ransoms by targeting entities in the U.S. critical infrastructure sector [2].

The cyber security industry formulated the Penetration Testing Execution Standard (PTES) penetration testing implementation standard in 2010, Lockheed Martin proposed the cyber threat model Cyber Kill Chain in 2021, and MITER launched the ATT&CK model in 2013. ATT&CK improves on the existing framework, describes and classifies confrontation behaviors based on real observation data, and aims to create a detailed list of known countermeasures and techniques for cyber attacks [1]. ATT&CK highlights the many techniques required to build a TTP chain but does not provide sufficient technical correlation to illustrate how adversaries can combine different techniques to achieve their goals. The Cybersecurity Chess Manual starts from the perspective of the attack target, covers multiple scenarios, detects as many attack modes as possible, screens the attack surface, and responds to the confrontation behavior at each attack stage to prevent the opponent’s attack.

II. Network Attack Model Framework

Whether it is the Penetration Testing Execution Standard (PTES) in 2010, the Cyber Kill Chain in 2011, or the MITER ATT&CK in 2013, we conducted a unified scientific analysis of the typical network attack model framework and extracted the network attack model framework attributes 4 basic attributes and 8 core features.

The four basic attributes of the typical network attack model framework are summarized as CIID and sorted according to the construction principles, namely C (connection), I (insight), I (inheritance), and D (deduction). ’Connection’ refers to both **’Connectivity’** and **’Scalability’**. ’Insight’ refers to **’Temporal’** and **’Comprehensive’**. ’Inheritance’ refers to **’Succession’** and **’Practical’**. ’Deduction’ refers to **’Sustainability’** and **’Intelligence’**(Figure 1).

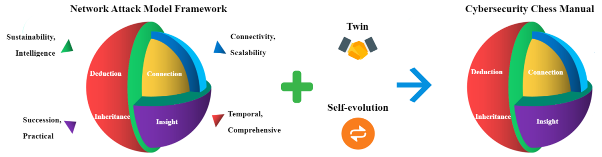

Fig. 1. Characteristics of Network Attack Model Framework

In addition to the above eight core features, Cybersecurity Chess Manual also has two subjective features of twin and self-evolution.

Twin: It is possible to build different scenarios based on digital twins according to the actual environment.

Self-evolution: According to the enhancement of the defensive atomic ability, the attack ability can be correspondingly strengthened to realize its own iterative evolution.

Combining the above two subjective features, based on knowledge engineering, digital twins and artificial intelligence, we propose a security concept called Cybersecurity Chess

Manual based on past events and predicting typical future confrontation scenarios.

III. Cybersecurity Chess Manual

Cybersecurity Chess Manual takes endless security incidents as long-term analysis objects, conducts focused research on the essence of network security, that is, offense and defense, and condenses the needs of the national economy and people's livelihood into scientific issues, and continuously accumulates and iterates to form Cybersecurity Chess Manual.

In this security concept, victory, defeat, and harmony are regarded as the **"goal"**, humans and AI are regarded as **"chess players"**, key information infrastructure is regarded as **"chess pieces"**, the experimental environment is regarded as a **"chessboard"**, and many network security incidents are the summary of the scenario reappears as a **"chess game"**. Conduct threat research by actively testing and validating the effectiveness of relevant cybersecurity vulnerabilities by reproducing techniques used in real-world attack scenarios. Realize the network security detection and verification scenarios of "hacker's perspective" intrusion and attack simulation, and can automatically and continuously conduct actual network attack simulations, thereby helping to efficiently locate potential security risks and vulnerabilities, and accurately verify the effectiveness of the security defense-in-depth system. After reproducing many classic scenes, all chess games are combined into "Cybersecurity Chess Manual".The twin of Cybersecurity Chess Manual is presented in the form of building different scenarios. Multiple actual scenarios are constructed through digital twins, and multiple attack angles are provided, which is convenient for deploying troops and adding corresponding protective measures. Its self-evolution is to atomize and decouple security capabilities, which facilitates orchestration and scheduling, and removes duplicate capabilities to make iterative updates faster.

In the Cybersecurity Chess Manual, we propose an active defense strategy based on simulated attacks in different scenarios and design eight chess tracks in the field of network security(Figure 2). By collecting various The cybersecurity confrontation chess script of the track eventually formed the Cybersecurity Chess Manual, providing solid support for the development of cybersecurity offense and defense.

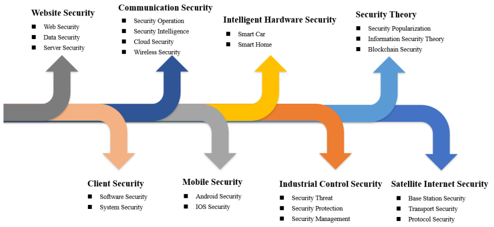

Fig. 2. Angle of the track of "Cybersecurity Chess Manual"

IV. Implementation Path

The design and implementation of the "Cybersecurity Chess Manual" concept is divided into four stages, and will be designed from the bottom up in accordance with the following four steps.

Step 1: Design Cybersecurity Chess Manual track attack scripts according to different types of network security attacks and defenses, and summarize and refine past security incidents.

Step 2: Build a network security attack and defense platform, quickly deploy lightweight attack targets such as operating systems, reproduce well-known technologies used in real attack scenarios such as BAS, VPT and other attack technologies, and CSMA, ShockTrap and other defense technologies, test and verify the effectiveness of relevant network protection detection tools [5].

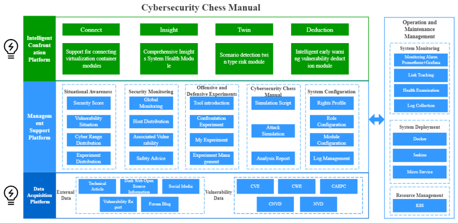

Fig. 3. Technical Architecture of the "Network security attack and defense platform"

Step 3: Relying on SpaceSpider, build a scene based on digital twins, realize the scene demonstration in the field of satellite Internet, and verify the effectiveness and economy [6].

Step 4: Empowered by artificial intelligence, use AIGC such as ChatGPT to generate and cover different scenarios, and complete the automatic attack and defense simulation deduction in the scenario.

V. Conclusion

This paper defines eight objective features of the network attack model framework. And based on knowledge engineering, digital twins and artificial intelligence, a security concept "Cybersecurity Chess Manual" based on past events to predict future typical confrontation scenarios is proposed, which realizes the "hacker's perspective" intrusion attack simulation verification scenarios, thereby helping to efficiently locate hidden security dangers and accurately verify the effectiveness of the defense system.

References

[1] Att&ck 101. https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

[2] Cisa and fbi say cuba ransomware's lifetime earnings crossed $60m in 2022. https://www.cybersecuritydive.com/news/cuba-ransomware-group-us-critical-sectors/637974/.

[3] Colonial pipeline hack explained: Everything you need to know. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[4] Gregory J Falco. *Cybersecurity for urban critical infrastructure*. PhD thesis, Massachusetts Institute of Technology, 2018.

[5] Quan Hong, Yang Zhao, Jian Chang, Yuxin Du, Jun Li, and Lidong Zhai. Shock trap: An active defense architecture based on trap vulnerabilities. In *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, pages 24–31. IEEE, 2022.

[6] Jiaqi Li, Lvyang Zhang, Quan Hong, Yang Yu, and Lidong Zhai. Space spider: a hyper large scientific infrastructure based on digital twin for the space internet. In *Proceedings of the 1st Workshop on Digital Twin & Edge AI for Industrial IoT*, pages 31–36, 2022.

Cybersecurity Chess Manual: A Security Concept Predicting Typical Future Confrontation Scenarios

Xingchen Wu, Jiaqi Li, Yang Yu, Jian Chang, Yang Zhao, Lvyang Zhang, Lidong Zhai
School of Cyber Security, University of Chinese Academy of Sciences
Institute of Information Engineering Chinese Academy of Sciences, Beijing, China
Tencent Security Xuanwu Lab, Beijing, China
China Unicom Online Information Technology CO.,Ltd, Beijing, China
China National Software & Service Co.,Ltd, Beijing, China
Email: zhailidong@iie.ac.cn

ABSTRACT

The development of advanced network security concepts such as Zero Trust is in full swing, and cutting-edge network security technologies such as active defense, mimic defense, and trusted computing all attach great importance to upgrading strategic thinking.

Cyberspace has become the frontier of confrontation, and national and urban infrastructure has become a key "target" of cyber warfare.

To this end, we propose to design a security concept called "Cybersecurity Chess Manual" to summarize past theories and predict typical confrontation scenarios in the future.

INTRODUCTION

At present, network attacks are increasing day by day and have become the primary security issues faced by fast-growing industries such as the Internet, Industrial Internet and Space Internet. National and urban infrastructure have become cyber warfare's key "target".

ATT&CK highlights the many techniques required to build a TTP chain but does not provide sufficient technical correlation to illustrate how adversaries can combine different techniques to achieve their goals.

The Cybersecurity Chess Manual starts from the perspective of the attack target, covers multiple scenarios, detects as many attack modes as possible, screens the attack surface, and responds to the confrontation behavior at each attack stage to prevent the opponent's attack.

NETWORK ATTACK MODEL FRAMEWORK

We conducted a unified scientific analysis of the typical network attack model framework and extracted the network attack model framework attributes 4 basic attributes and 8 core features.

The four basic attributes of the typical network attack model framework are summarized as CIID and sorted according to the construction principles, namely C (connection), I (insight), I (inheritance), and D (deduction).

***C:** Connectivity, Scalability*
***I:** Temporal, Comprehensive*
***I:** Succession, Practical*
***D:** Sustainability, Intelligence*

In addition to the above eight core features, Cybersecurity Chess Manual also has two subjective features of **twin** and **self-evolution** (Fig. 1).
Twin: It is possible to build different scenarios based on digital twins according to the actual environment.
Self-evolution: According to the enhancement of the defensive atomic ability, the attack ability can be correspondingly strengthened to realize its own iterative evolution.

Combining the above two subjective features, based on knowledge engineering, digital twins and artificial intelligence, we propose a security concept called Cybersecurity Chess Manual based on past events and predicting typical future confrontation scenarios.

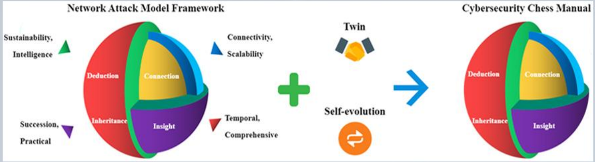

Fig. 1. Characteristics of Network Attack Model Framework

CYBERSECURITY CHESS MANUAL

Cybersecurity Chess Manual takes endless security incidents as long-term analysis objects, conducts focused research on the essence of network security, that is, offense and defense, and condenses the needs of the national economy and people's livelihood into scientific issues, and continuously accumulates and iterates to form. In this security concept:

Goal: Victory, Defeat and Harmony
Chess players: Humans and AI
Chess pieces: Key Information Infrastructure
Chessboard: Experimental Environment
Chess game: A Summary of the Recurrence of Many Network Security Incident Scenarios

Conduct threat research by actively testing and validating the effectiveness of relevant cybersecurity vulnerabilities by reproducing techniques used in real-world attack scenarios. Realize the network security detection and verification scenarios of "hacker's perspective" intrusion and attack simulation, and can automatically and continuously conduct actual network attack simulations. After reproducing many classic scenes, all chess games are combined into a "Cybersecurity Chess Manual".

We propose an active defense strategy based on simulated attacks in different scenarios and design eight chess tracks in the field of network security(Fig. 2). and continue to collect The network security confrontation chess script of each track.

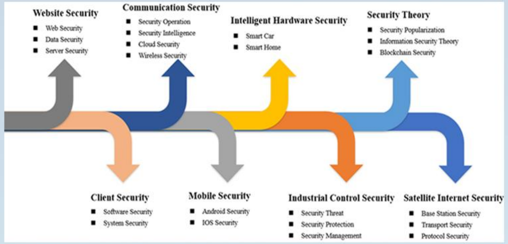

Fig. 2. Angle of the track of Cybersecurity Chess Manual

IMPLEMENTATION PATH

The design and implementation of the "Cybersecurity Chess Manual" concept are divided into four stages and will be designed from the bottom up in accordance with the following four steps.

Step 1: Design Cybersecurity Chess Manual track attack scripts according to different types of network security attacks and defenses and summarize and refine past security incidents.

Step 2: Build a network security attack and defense platform, quickly deploy lightweight attack targets such as operating systems, reproduce well-known technologies used in real attack scenarios such as BAS, VPT and other attack technologies, and CSMA, ShockTrap and other defense technologies, test and verify the effectiveness of relevant network protection detection tools.

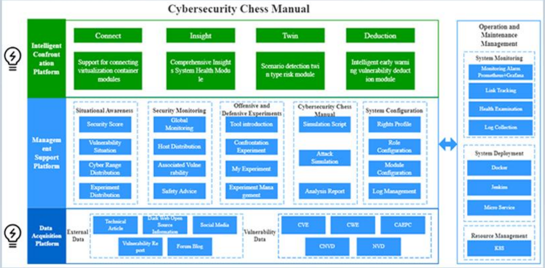

Fig. 3. Technical Architecture of the "Network security attack and defense platform"

Step 3: Relying on SpaceSpider, build a scene based on digital twins, realize the scene demonstration in the field of satellite Internet, and verify the effectiveness and economy.

Step 4: Empowered by artificial intelligence, use AIGC such as ChatGPT to generate and cover different scenarios, and complete the automatic attack and defense simulation deduction in the scenario.

CONCLUSION

This paper defines eight objective features of the network attack model framework. And based on knowledge engineering, digital twins and artificial intelligence, a security concept "Cybersecurity Chess Manual" based on past events to predict future typical confrontation scenarios is proposed, which realizes the "hacker's perspective" intrusion attack simulation verification scenarios, thereby helping to efficiently locate hidden security dangers and accurately verify the effectiveness of the defense system.