Cyber Defense Operation using CyCOP: A Cyber Situational Awareness Tool to Support Decision-Making

Sungyoung Cho* Koohyung Kwon† Sungmo Koo‡ Haengrok Oh§

The 2nd Research and Development Institute, Agency for Defense Development, Republic of Korea

Abstract

We have developed the Cyber Common Operational Picture (CyCOP) that helps users to recognize current cyber situations and make appropriate decisions for cyber defense. There is an operational concept based on the OODA (observation, orientation, decision, and act) loop for decision making in CyCOP. CyCOP provides several views that visualize the current state of cyber assets, the network topology of the organization and cyber threat situations. It also presents information to the users to determine the best course of actions (CoAs) against potential or current threats.

Keywords: cyber defense operation, Cyber Common Operational Picture, attack graph, mission-asset dependency, course of action

Index Terms: Human-centered computing—Visualization—Visualization application domains Human-centered computing—Visualization—Information visualization

1 Introduction

Various analysis and visualization techniques for cyber situational awareness have been studied from the academic and industrial areas. Many organizations, including the military, are interested in applying and utilizing techniques related to cyber situational awareness. Specifically, a decision-making support system is required that helps decision-makers such as commanders to recognizing and evaluating cyber situations through analysis and visualization techniques so that the organizations can actively and effectively respond to potential or current cyber threats.

We previously proposed CyCOP [2] which is an effective visualization tool for cyber situational awareness. Our system has been developed with the purpose of communication and decision support for the cyber defense in organizations, reflecting the operational concept based on the OODA loop for decision-making. Decision-makers can recognize cyber assets, network topology, and cyber threat situation visualized in various views of CyCOP and choose the appropriate CoAs.

2 Operations Concept

The decision-making process for cyber defense can be represented as an operating concept based on OODA loop. First, a system collects and aggregates data from various devices (network devices, network-based security appliances, endpoints such as servers and PCs, and separate sensors) to manage up-to-date asset information and vulnerabilities they have. The network topology is also kept up-to-date (observation phase). The organization analyzes the dependencies between the missions, tasks to perform missions and assets in advance. The users generate attack graphs based on network topology and asset vulnerability information (orientation phase) and analyze candidate CoAs based on attack graphs to select the appropriate one that can counter potential threats against important assets effectively [5] (decision phase). Also, the users can identify the current cyber threats from hyper alerts generated from security information and event management (SIEM) that can collect and correlate low-level alerts generated from various security sensors, assess the amount of damage for victims against cyber threats, (orientation phase) and select appropriate CoAs to prevent additional damage caused by cyber threats [7] (decision phase).

*e-mail: sycho@add.re.kr
†e-mail: koohyung@add.re.kr
‡e-mail: smkoo12@add.re.kr
§e-mail: haengrok@add.re.kr

3 CyCOP: Cyber Common Operational Picture

CyCOP is a tool that visualizes cyber assets and cyber threats in cyberspace [2]. However, it is not a simple visualization tool, but a visualization tool that enables the users (**commanders** and **staff officers**) who perform cyber operations based on visualized information to conduct decision-making that can effectively respond to cyber threats. Using CyCOP, users can recognize the current state of cyber assets and cyber threats, assess the damage to cyber assets and the impact on missions to accomplish using assets, and take appropriate CoAs to respond against threats accordingly.

3.1 Main View

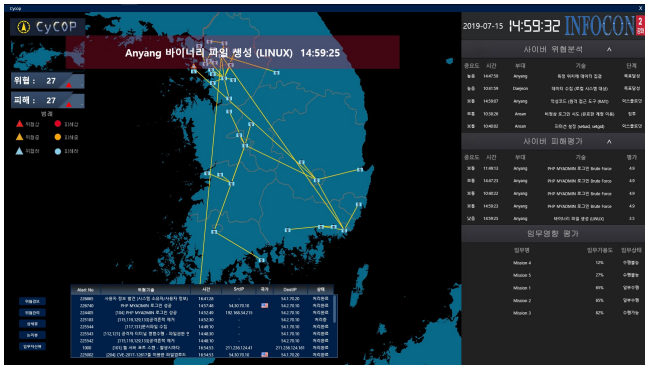

Figure 1: Main View of current CyCOP

Main View (Fig. 1) represents the geographical location of organizations and their network configuration and the cyber threat to the organization's assets on the geographic map. Hyper alerts, which are generated from SIEM which collects and correlates events, logs, and alerts, are displayed on *Main View*. They are presented as icons and colors according to the security status and displayed upon the icon representing the organization. Based on ARMOUR [5], they appear above the icon that shows organization by icon and color depending on security status. Also, the response state to the incidents by the security operation centers (SOCs) and the damage caused by the cyber threat are displayed. *Main View* helps users to recognize the overall situation, including previous and current cyber threats. It also works with other views and systems that can respond to cyber threats, enabling users to make decisions at a higher level.

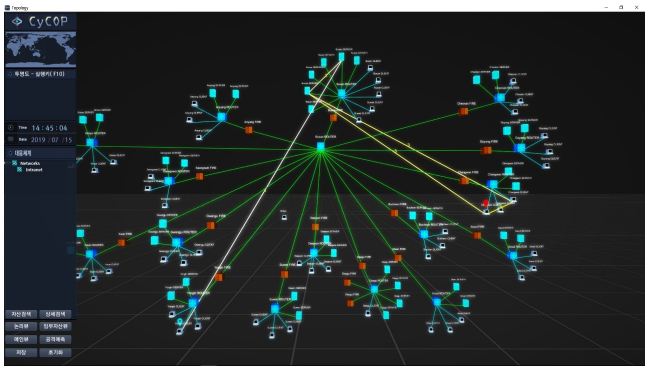

Figure 2: Network Topology View of currently designed CyCOP. Attack graph is shown on current network topology.

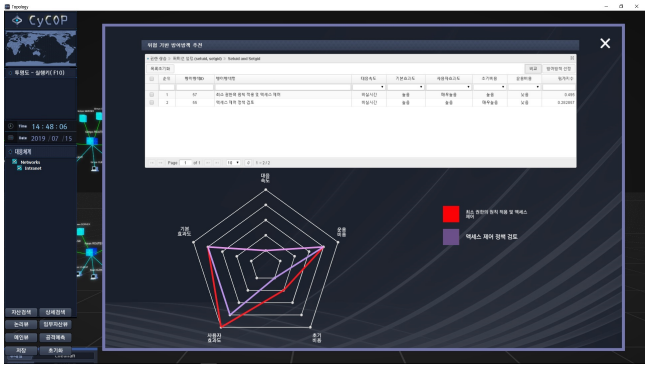

Figure 3: Course of Action Comparison in Network Topology View

3.2 Network Topology View

Network Topology View (Fig. 2) shows the cyber assets and the network topology consisting of them operating in the organization. Cyber assets include network equipment such as backbone routers, routers and switches, network security appliances such as firewalls, IPSs, web firewalls, and endpoints such as servers and PCs. Cyber asset information is collected using sensors and kept up to date. They are presented as icons according to asset types and arranged in the order of backbone routers (the bottom layer), network equipment, network security equipment, and endpoints (the top layer).

On network topology, attack graph analysis (based on MulVAL (Multi-host, Multi-stage Vulnerability Analysis Language) [6], NetSPA (Network Security Planning Architecture) [1], and TVA (Topological Analysis of Network Attack Vulnerability) [4]) is performed by selecting the start host and end host of the attack. The result is visualized upon the network topology by yellow lines as shown in Fig. 2, so that the users can intuitively understand the analysis result. The users can anticipate plausible future attack routes as for current cyber threats and establish CoAs to prevent further spread of attacks. First, the system presents a list of CoAs based on the analyzed attack graph [5] and current cyber threat [7]. Then, users can check the analysis results based on five factors (response speed, basic effectiveness, custom effectiveness, initial cost, and operation cost) (see Fig. 3) and choose the best CoA.

3.3 Mission-Asset Dependency Analysis View

Mission-Asset Dependency Analysis View (Fig. 4) presents the impact of cyber asset threats on missions, tasks for missions, and associated cyber assets. First, several missions are listed on the left side of this view. By choosing a specific mission, the user can

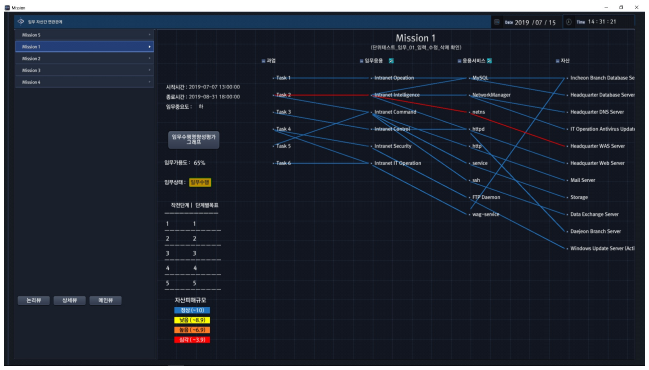

Figure 4: Mission-Asset Dependency Analysis View of currently designed CyCOP

see tasks, application services for tasks, applications (such as web servers and databases), physical cyber assets, and their relationships to perform missions. This model is based on MITRE Crown Jewel Analysis (CJA) [3]. When attacks affect specific physical cyber assets, impact on the applications running on those assets, application services, and tasks performed on the cyber assets are displayed on the graph with numerical calculation, and the overall degree of availability and mission status are also shown.

4 Conclusion and Future Work

We proposed CyCOP, a tool for various user groups to recognize cyber assets and cyber threats in cyberspace and prepare countermeasures for effective protection. CyCOP is a component of cyber operations in the military field. It is possible to proactively respond to potential cyber threats by analyzing and presenting the attack graphs using the cyber asset information which is kept up to date. Besides, it is possible to perform systematic security operations and cope effectively by identifying cyber attacks at a high-level by correlating logs, events, and alerts generated by sensors that detect cyber attacks at a low-level.

In the future, it is required to develop symbols that can visually recognize cyber threats commonly. Also, it is required to integrate security orchestration, automation and response (SOAR)-based technologies that can perform automated responses to cyber threats.

References

[1] M. L. Artz. *Netspa: A network security planning architecture*. PhD thesis, Massachusetts Institute of Technology, 2002.

[2] S. Cho, I. Han, H. Jeong, J. Kim, S. Koo, H. Oh, and M. Park. Cyber kill chain based threat taxonomy and its application on cyber common operational picture. In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–8. IEEE, 2018.

[3] G. Hastings, L. Montella, and J. Watters. Mitre crown jewels analysis process. *The MITRE Corporation, MTR*, 90088, 2009.

[4] S. Jajodia, S. Noel, and B. Oberry. Topological analysis of network attack vulnerability. In *Managing Cyber Threats*, pp. 247–266. Springer, 2005.

[5] N. Nakhla, K. Perrett, and C. McKenzie. Automated computer network defence using armour: Mission-oriented decision support and vulnerability mitigation. In *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–8. IEEE, 2017.

[6] X. Ou, S. Govindavajhala, and A. W. Appel. Mulval: A logic-based network security analyzer. In *USENIX security symposium*, vol. 8, pp. 113–128. Baltimore, MD, 2005.

[7] J. Wynn. Threat assessment and remediation analysis (tara). Technical report, MITRE CORP BEDFORD MA BEDFORD United States, 2014.