Attack Scenario Visualization for Situational Awareness in Cyber Defense Operation

Yongwoo Park* Minchul Kim Hansam Seo Jaepil Youn Insung Han Sungyoung Cho†

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

Abstract

Complex Advanced Persistent Threat (APT) campaigns are made up of multiple attack phases, which can seriously damage organizations such as government agency or military. Alert correlation can be used to detect and analyze multistep attacks like complex APT campaigns. It is required to visualize the analysis results so that users can comprehend multistep attacks more intuitively. In this paper, we discuss a hierarchical visualization method that enables various user groups who conduct cyber defense operations to comprehend multistep attacks.

Keywords: multistep attack, alert correlation, attack scenario, cyber defense operation

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

1 Introduction

Individual security sensors such as IDSs and IPSs have limitations in detecting APT campaigns performed against enterprise, organization, or national level. Alert Correlation has been continuously studied aimed at identifying high-level situation awareness of attacks by correlating low-level alerts generated by various security sensors. Currently, security information & event management (SIEM) collects low-level alerts and correlates them using predefined correlation rules. However, hyper alerts generated from SIEM by correlation enable analysts to recognize attacks with the individual attack instances that may make up APT campaigns, rather than the context of the whole APT campaign.

We proposed a Bayesian network-based alert correlation method [6] to analyze attack scenarios such as APT campaign. It is also important to visualize analyzed attack scenarios to help different user groups to comprehend past and current attack situations and perform appropriate and effective course of actions (CoAs). In this paper, we discuss a visualization method that enables various user groups performing cyber defense operations to aware attack situations by considering their roles and interests.

2 User Groups and Requirements

Three user groups who perform cyber defense operations on cyber warfare; analysts, staff officers, and commanders.

Analyst investigates incidents by analyzing low-level alerts generated by security sensors and reports investigation results to staff officers to help them comprehend the past and current attack situations. Analysts are interested in low-level and detailed data such as indicators of compromises (IOCs) and the presence or pattern of individual attack instances. They are also interested in comprehending attack situations at detailed levels, such as identifying false positives from low-level data or possible attacks that have not been detected.

Staff officers support commanders to conduct appropriate decision-making. They analyze and understand the information reported by analysis system and analysts, and synthesize it so that commanders can recognize past and current attack situations and make appropriate decisions. They select and synthesize useful information reported by analysts for the commanders to comprehend. Although staff officers can understand low-level and detailed data such as IOCs, they are interested in synthesized information and summarized flow and/or patterns of attack scenarios.

Commanders, who are the highest-level user group performing cyber defense operations, recognize the overall attack situation based on information reported by staff officers, and make final decisions by reviewing CoAs established by system and staff officers. Therefore they are interested in comprehending overall attack scenario flows.

Three user groups are commonly interested in comprehending past and current cyber attack situations and make corresponding appropriate decisions. However, because these user groups have different roles to perform cyber defense operations according to their rank and position, it is required to visualize the analyzed attack scenarios with various levels to help each user group intuitively comprehend.

3 System Design

Our system for analyzing and visualizing attack scenarios is composed of SIEM, cyber threat taxonomy, offline correlation module, and online correlation module.

At the lowest level, SIEM collects and correlates various alerts, and generates the correlation result as a hyper alert. SIEM collects low-level alerts and correlates them based on predefined rules to reduce the amount of data to analyze attack scenarios by generating hyper alerts. Each hyper alert matches one of the attack techniques described in our Cyber Threat Taxonomy.

Cyber threat taxonomy defines and classifies cyber attacks for common and consistent expression of cyber attacks. Also, it is used as a reference model for analyzing causal relationships between attack types using hyper alerts. The hierarchy for cyber threat taxonomy consists of kill chain phases, tactics, actions, techniques, and procedures. It based on MITRE ATT&CK [4] and CAPEC [5], and National Security Agency (NSA) Cyber Threat Framework [2].

The offline correlation module models the causal relationship between attack types (techniques in taxonomy) by analyzing hyper alerts using Bayesian network-based algorithms.

For hyper alerts generated in real-time, the online correlation module uses the causal relationship model between attack types to reconstruct plausible attack scenarios that might be occurred in the past and anticipates possible future attack scenarios. Reconstructed and predicted attack scenarios are stored in the form of attack chains.

4 Attack Scenario Visualization Approach

Fig. 2 shows the layered visualizations for three user groups (analysts, staff officers, and commanders) who can comprehend analyzed attack scenarios.

*e-mail: yongwoozz@add.re.kr

†e-mail: sycho@add.re.kr

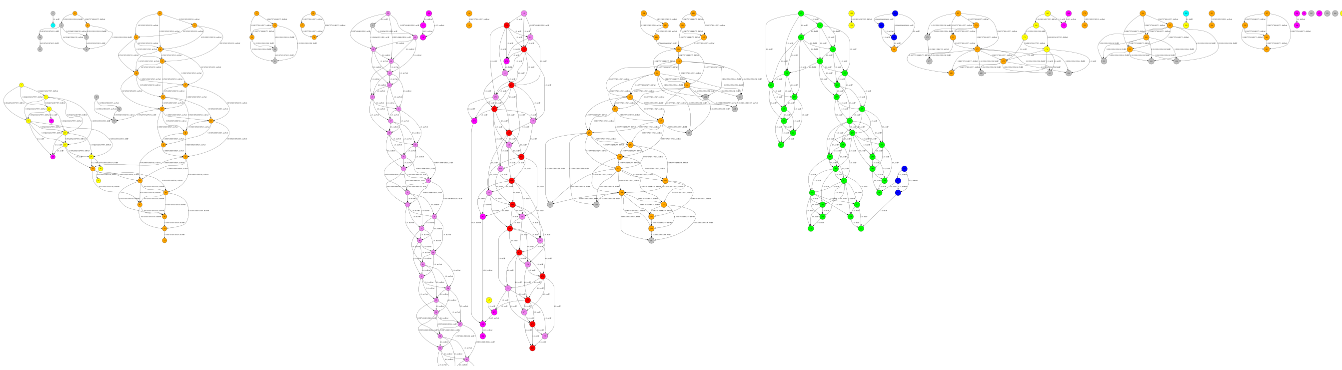

Figure 1: Visualization of attack scenarios for analysts (the lowest-level visualization). Each attack scenario composed of hyper alerts (nodes) generated from SIEM, and the relationship (edge) determined by the correlation table made by Bayesian network-based offline alert correlation module [6]. Colors in nodes are determined by corresponding attack type (techniques) defined in cyber threat taxonomy.

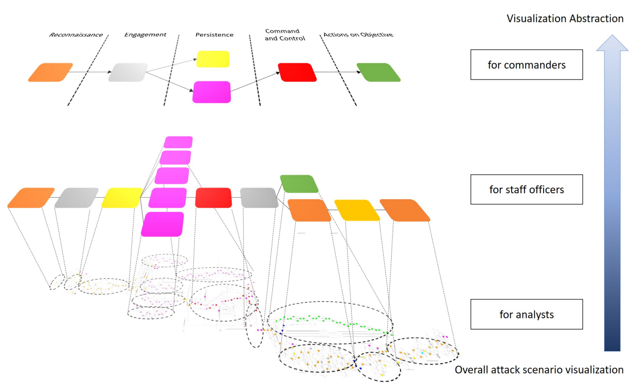

Figure 2: Visualization of attack scenarios for three user groups. (Bottom) For analysts, all of hyper alerts constituting attack scenario must be visualized. (Middle) For staff officers, hyper alerts are clustered with the same attack type according to one of the attack levels (techniques, actions, or tactics). (Top) For commanders, attack scenarios are shown based on the kill chain phases and mapped attack types.

Analysts can see the lowest-level visualization of attack scenarios composed of hyper alerts, as shown in Fig. 1. Fig. 1 is a visualization of the analysis results of DARPA 2000 dataset [3] using our system and correlation analysis algorithm [6]. Each hyper alert is expressed color in the node or on a separate label according to the mapped attack technique. Although there may be a lot of hyper alerts that make up an attack scenario, all of them must be visualized. Analysts can identify false positives and remove them from analyzed attack scenarios. Although this visualization does not explicitly define the timeline as an axis, analysts can comprehend analyzed attack scenarios over time. Thus, analysts can identify possible false negatives between the identified hyper alerts.

Staff officers can comprehend attack scenarios by staff officer-level visualization that is an abstracted version of analyst-level visualization. Hyper alerts are clustered with the same attack type according to one of the levels (techniques, actions, or tactics) defined in cyber threat taxonomy, as shown in the middle part of Fig. 2. Besides, as with analyst-level visualizations, staff officers can comprehend analyzed attack scenarios over time. Staff officers can identify adversary processes [1] by analyzing common attack patterns in attack scenarios. Also, they can identify attack patterns that occur frequently in the organization so that they can find vulnerabilities that cause these attack patterns.

Commanders aim to comprehend APT campaigns against the organization at a big picture and to prevent current and future attacks so that adversaries cannot achieve the final goals such as confidence leaks or system destroy. Therefore, the commander-level visualization summarizes the analyzed attack scenarios based on the highest level (cyber kill chain) and mapped attack types (tactics or actions) defined in cyber threat taxonomy, as shown in the top part of Fig. 2. This allows commanders to comprehend the past and current attack phases which adversaries have conducted to achieve their final goal in terms of cyber kill chain model, rather than in chronological order like analyst-level and staff officer-level visualizations. Commanders can comprehend the past and present attack phases that adversaries have taken to achieve their ultimate goal from the cyber kill chain model perspective. This, on the other hand, does not visualize attack scenarios taken place over time, unlike analyst-level or staff officer-level visualization.

5 Conclusion and Future Work

In this paper, we propose a method to visualize the analysis result of APT campaigns composed of several attack phases so that various user groups can comprehend how the attack has been progressed. Attack scenario visualization methods for three user groups (analysts, staff officers, and commanders) performing cyber defense operations differ in the level and contents of the information according to their roles and interests.

At present, we present the analyst-level visualization of attack scenario analysis results using DARPA 2000 dataset. The nodes (hyper alerts) that constitute the current visualization are presented as different colors following cyber threat taxonomy so that analysts intuitively comprehend attack scenarios. We are implementing abstract visualizations that other user groups, such as staff and commander, can comprehend complex attack scenarios more intuitively.

References

[1] S. Caltagirone, A. Pendergast, and C. Betz. The diamond model of intrusion analysis. Technical report, Center For Cyber Intelligence Analysis and Threat Research Hanover Md, 2013.

[2] Cybersecurity Operations, The Cybersecurity Products and Sharing Division. *NSA/CSS Technical Cyber Threat Framework v2*. National Security Agency, Nov 2018.

[3] MIT Loncoln Laboratory. 2000 DARPA intrusion detection scenario specific datasets. `hhttps://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets`.

[4] MITRE. MITRE ATT&CK™. `https://attack.mitre.org/`.

[5] MITRE. MITRE CAPEC™. `http://capec.mitre.org/`.

[6] Y. Shin, C. Lim, M. Park, S. Cho, I. Han, H. Oh, and K. Lee. Alert correlation using diamond model for cyber threat intelligence. In *European Conference on Cyber Warfare and Security*, pp. 444–450. Academic Conferences International Limited, 2019.