A Rule Based Event Correlation Approach for Physical and Logical Security Convergence

Dongho Kang [†] **and Jungchan Na** [†],

[†]Cyber Security-Convergence Research Department,
Electronics and Telecommunications Research Institute(ETRI), Daejeon, 305-705 Republic of Korea

Summary
Cyber threats have rapidly evolved in frequency and sophistication. As a result, physical and logical security systems are an essential solution to protect enterprise assets. Most enterprises deployed different types of physical and logical security systems but manage them as independent domain. Most physical security systems focus on the protection of the physical behavior of the unauthenticated personnel. Logical security systems protect information assets. Physical and logical security systems generate a large volume of alerts. Some of them report false positives and retrieve different alerts for a single attack. Those problems may cause the delay in response and miss detection. The convergence of physical and logical security brings significant benefits, specifically identifying blended attacks. Recent event correlation techniques have become one of the most important security techniques. The objective of this paper is to overcome the limitations of existing physical and logical security systems that focus on specific problems rather than event correlation for an entire enterprise. To solve this problem, we build the correlation rules to define the relationship between physical and logical security events caused by abnormal behavior activities, and provide the correlation analysis technique to detect the multi-stage attacks.

Key words:
Enterprise Security, Security Convergence, Correlation analysis, Intrusion Detection

1. Introduction

Cyber threats have rapidly evolved in frequency and sophistication. As a result, physical and logical security systems are an essential solution to protect enterprise assets. Most enterprises deployed different types of physical and logical security systems but manage them as independent domain. Most physical security systems focus on the protection of the physical behavior of the unauthenticated personnel. Logical security systems protect information assets. Physical and logical security systems generate a large volume of alerts. Some of them report false positives and retrieve different alerts for a single attack. In example, the current implementation of intrusion detection systems (commercial and open-source) is employing signature-based detection mechanisms. In addition to these, few statistical techniques are also used for detection process. The main task of signature based systems is to inspect the network traffic and perform pattern matching to detect attacks and generate alerts. IDSs still have two well-known problems. First, current IDSs cannot ensure that all alerts reflect actual attacks; true positives (attacks detected as intrusive) are usually mixed with false positives. Second, an IDS usually produces a large number of alerts [1][2]. The high volumes and low quality (i.e., missed attacks and false positives) of the intrusion alerts make it very challenging for human operators or intrusion response systems to understand the alerts and take appropriate actions. Manually managing and analyzing these alerts is time-consuming and error-prone. Thus, it is necessary to develop techniques to deal with the large volumes and low quality of intrusion alerts [3].To better protect the information assets in the enterprise environment, we need the technology of integrating physical and logical security. Our approach is to overcome the limitations of existing physical and logical security systems that focus on specific problems rather than event correlation for an entire enterprise. To solve this problem, we build the correlation rules to define the relationship between physical and logical security events caused by abnormal behavior activities, and provide the correlation analysis technique to detect the multi-stage attacks.

The remainder of this paper is organized as follows: section 2 presents the related works on events correlation techniques. Section 3 describes our technique in detail, and then we present the experimental results. At last we summarize this paper and suggest the future wok in section 5.

3. Related work

Intrusion detection has been studied for more than 20 years since Anderson’s report [Anderson 1980]. A survey of the early work on intrusion detection is given by Mukherjee et al. [1994], and an excellent overview of current intrusion detection techniques and related issues can be found in a recent book [Bace 2000]. Research on intrusion alert correlation has been rather active recently [4]. Alert

Manuscript received January 5, 2012
Manuscript revised January 20, 2012

aggregation and correlation is defined as a process that contains multiple components with the purpose of analyzing alerts and providing high-level insight on the security state of the network under surveillance. Some researches have investigated the alert aggregation and correlation problem to facilitate the analysis of intrusions The existing alert correlation techniques can be classified into four groups: similarity based, attack scenario based, multi-stage, and filter based. Similarity based approaches correlate alerts based on the similarity between alert attributes. A function is usually used to calculate the similarity between two pairs of alerts, and the resulting score determines if these alerts will be correlated. Attack scenario based approaches correlate alerts based on predefined attack scenarios. These attack scenarios can either be specified by the users, or learned from training datasets. Multi-stage approaches correlate alerts based on the causality of earlier and later alerts. This approach tries to reconstruct some complex attack scenarios by linking individual steps that are a part of the same attack. Filter based approaches prioritize the alerts by their criticality to the protected systems [5].

Debar and Wespi (2001) proposed an aggregation and correlation algorithm for intrusion alerts from various detection sensors. There are two main parts to their aggregation and correlation relationship.

Correlation relationship The algorithm creates correlation relationships between related events according to explicit rules programmed into the ACC(Aggregation and Correlation component) or derived by the ACC from configuration information. Once events are in a relationship, they are considered part of the same trend of attacks and as such they are processed together. There are currently two kinds of correlation relationships between events: duplicates and consequences.

Aggregation relationship The algorithm groups events together according to certain criteria (similar to database views) to compute an aggregated severity level. Whereas the individual severity level of each event might not be sufficient to warrant specific analysis, the grouping may reveal trends and associations that clarify the intentions of the attacker [6].

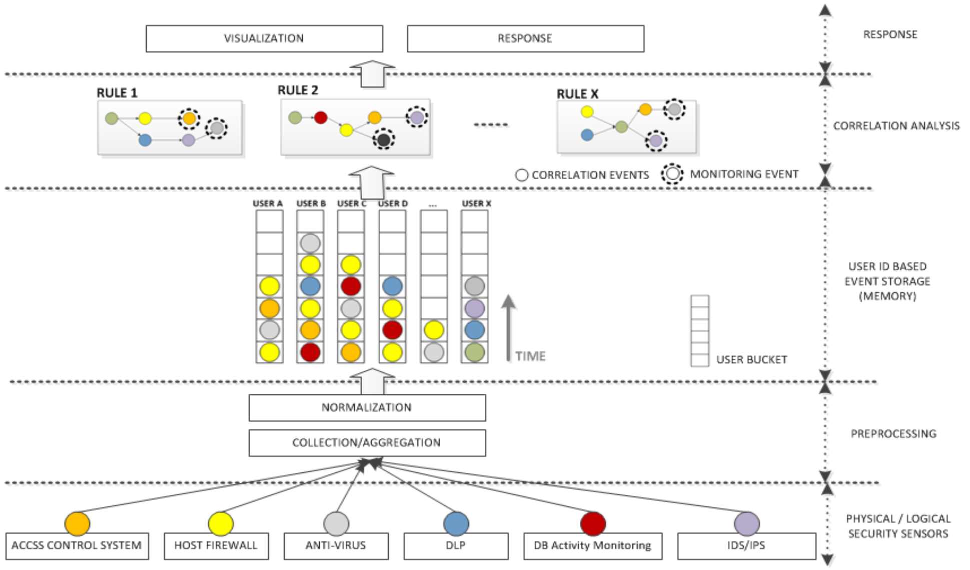
Dain and Cunningham (2001) proposed an algorithm to fuse the alerts from heterogeneous IDSs into attack scenarios by using a probabilistic approach. The proposed CIDS consists of different types of IDSs, which generate alerts separately. These alerts are then converted to a standard format and stored in an SQL database. The fusion system reads from the database to determine to which attack scenario a new alert belongs. Each time a new alert is received from an IDS, it is compared with the attack scenarios being constructed so far. Two probability assignment approaches, one heuristic and one based on a data mining approach, are proposed to estimate the membership of a new alert. A training data set is used to optimize the parameters of these two probability estimation approaches. A new alert is assigned to the scenario that has the highest probability estimate score. If all the estimate scores are below an assigned threshold, the alert will start a new scenario [5].

Ning et al. (2002) proposed a practical method for constructing attack scenarios through alert correlation, using prerequisites (e.g., existence of vulnerable services) and consequences (e.g., discovery of vulnerable services) of intrusions. For example, if we find a Sadmind Ping followed by a buffer overflow attack against the corresponding Sadmind service, we can correlate them to be parts of the same series of attacks. In

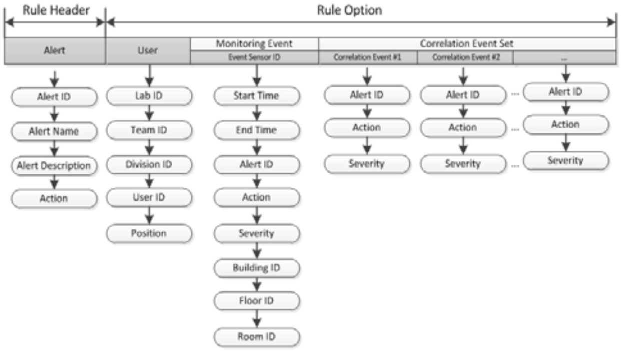
other words, we model the knowledge (or state) of attackers in terms of individual attacks, and correlate alerts if they indicate the progress of attacks[7].

3. Proposed rule based correlation

In this section we describe our technique in detail. Our correlation analysis needs to build rules to define the relationship between security events caused by abnormal behavior activities. And then correlates the security events by matching pre-defined events sequence (i.e., rule) with the security events. A rule presents a specific attack scenario and is composed of some parameters on parts of physical and logical events. Our correlation analyzer tries to identify abnormal behavior by comparing the raw security events to patterns of events as the predefined rules. Fig. 1 shows the architecture of rule based correlation system. As shown in Fig.1, Our system receives the raw security events generated by physical and logical security sensors. After security events are generated by the source sensors are normalized and automatically sent to the correlation analyzer, they are stored in user id based partitioned memory. Event consists of one more parameters such as IP address, event id, event name, and user id and so on. Physical security sensors may include user id parameter in their events because most physical sensors require user id to users for authentication. In example, physical access control systems can retrieves events with user id parameter from the readers when user access is granted or denied. There are many different types of physical and logical sensor that are deployed in most enterprises. In case of some sensors don’t need to provide several means for user authentication. Therefore they can’t retrieve any user information in their events. But we can make use of the field of IP address in the events. Because most organizations get their IP address space, they can easily notice who to use them. Consequently we can get a user id from IP address. The modified events are transferred to correlation analyzer after normalization and aggregation. As shown in the Fig. 1 above, all events is stored in user id based partitioned memory. Each event provides a potential evidence to find the behaviors of intrusion. The set of events in a rule represent a sequence of intrusion. Correlation analyzer inspects whether a stored event is a monitoring event which was defined as rule or not.



<Fig. 1> Architecture of event correlation

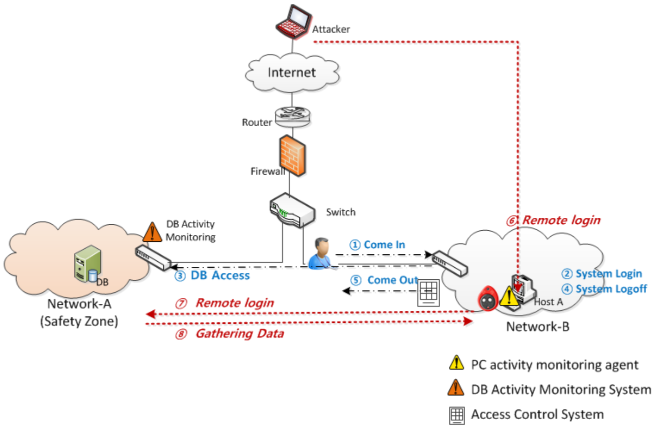


< Fig. 2>Rule format

If it is a monitoring event of a specific rule, Correlation analyzer inspects all stored events in a partitioned memory on where is the monitoring event.

Rules require manually definitions of malicious behavior. Rules are divided into two logical sections, the rule header and the rule option. The rule header contains the rule' ID, name, Alert Description and action. The rule option section contains alert id, action on which parts of the event should be inspected to determine if the rule action should be taken. Fig.2 shows the rule format. The rule describes attack scenario. The rule option's monitoring event is the last event of attack scenario. The rule option's correlation events are the rest events of attack scenario.

Botnets have been one of the most serious multi-stage attacks to obtain access to systems and to control them remotely. We introduce an example that is the multi-stage attack scenario to leakage information from bot on infected host in Fig.2



< Fig. 3> Botnet scenario

We assume that eight events are generated by sensors deployed in security areas and a malicious code which connects to attacker remotely is installed on the host A in the network-B. From ① to ⑤ events are legal action caused by an authorized personnel’s behavior. ⑥ to ⑧ are illegal events caused by an attacker. In this scenario, most security sensors cannot distinguish between normal and abnormal if a malicious code isn’t detected. In this scenario, we can present rules to detect an abnormal behavior:

Rule 1:
Alert Action: Log
Monitoring Evt: ⑦
Correlation Evt: ⑤&⑥

Rule 2:
Alert Action: Alert
Monitoring Evt: ⑧
Correlation Evt: (⑥||⑦)& ⑤

If those rules are built into our system, we can find abnormal activities undetected by sensors. Our approach handles the integrated physical and logical security management to prevent unblended attacks occurred from the inside.

4. Conclusions

Recent event correlation techniques have become one of the most important security techniques. The objective of this paper is to overcome the limitations of existing physical and logical security systems that focus on specific problems rather than event correlation for an entire enterprise. To solve this problem, we build the correlation rules to define the relationship between physical and logical security events caused by abnormal behavior activities, and provide the correlation analysis technique to detect the multi-stage attacks. To find sophisticated attacks needs correlation analysis for all events generated by physical and logical systems are deployed in an enterprise. One of the most important works in the future is to enrich rules, the effect of intrusion detection depends on the knowledge in attack scenarios.

Acknowledgments

This study was performed as a part of Industrial Original Technology Development Project (10035237, Development of Intrusion detection and response technology based on the security convergence for protecting Information assets of Industrial facilities) sponsored by the Ministry of Knowledge Economy(MKE) and Korea Evaluation Institute of Industrial Technology(KEIT).

References

[1] Tian Zhihong, Qin Baoshan, and Zhang Hongli, “Alertclu: A Realtime Alert Aggregation and Correlation System”, IEEE International Conference on Cyberworlds, 2008

[2] Faeiz Alserhani, Monis Akhlaq, Irfan U Awan, and Andrea J Cullen, “Detection of Coordinated Attacks Using Alert Correlation Model”, IEEE Progress in Informatics and computing, 2010.

[3] K. Julsch, “Dealing with false positives in intrusion detection”, In The 3 th Workshop on Recent Advances in Intrusion Detection. 2000.

[4] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang xu, “Techniques and Tools for Analyzing Intrusion Alerts”, ACM Journal, May 2004

[5] Chenfen Vincent Zhou, Christopher Leckie, Shanika Karunasekera, “ A survey of coordinated attacks and collaborative intrusion detection”, ELSEVIER Applied Soft Computing Volume 12, Issue 3, 2012

[6] DEBAR,H. ANDWESPI,A. 2001. Aggregation and correlation of intrusion-detection alerts. In Recent Advances in Intrusion Detection. Lecture Notes in Computer Science, vol. 2212. 85–103

[7] Ning P, Cui Y, Reeves DS. Constructing attack scenarios through correlation of intrusion alerts. In: Proceedings of the 9th ACM conference on computer and communications security (CCS); 2002. p. 245–54.

[8] Shaula Alexander Yemini, Shmuel kliger, and Eyal Mozes, “High Speed and Robust Event Correlation”, IEEE Communication Magazine May 1996.

[9] http://en.wikipedia.org/wiki/Event_correlation

Dongho Kang received the M.E. degree in Computer Science Engineering from Hannam University in 2001. He has been a senior member of engineer staff at Electronics and Telecommunications Research Institute (ETRI) in Korea since 2001. His research interest includes network security and security management.

Jungchan Na received the B.S. degree from Chungnam National University in 1986, the M.E. degree from Soongsil University in 1989, the Ph.D. degree in Computer Science from Chungnam University in 2004. He has been a principal member of engineering staff and the leader of managed security research team at Electronics and Telecommunications Research Institute (ETRI) in Korea since 1989. His research interest includes network security management, visualization of network security, and security situational awareness