Automated Security Intelligence (ASI) with Auto Detection of Unknown Cyber-Attacks

TAGATO Hiroki, SAKAE Yoshiaki, KIDA Koji, ASAKURA Takayoshi

Abstract

It has now become necessary to adopt countermeasures against cyber-attacks that are becoming more sophisticated as the years pass. Automated Security Intelligence (ASI) is a self-learning, system anomaly detection technology that collects detailed operations logs from PCs and servers using monitoring software. It then generates the usual status of the surveyed system by applying machine learning (AI) to the log and compares it with the current system operations in order to detect even unidentified attacks. When this technology is applied to a security monitoring system, more robust security can be implemented thanks to detection throughout the attack process, including in the intermediate stages such as "Exploration" and "Installation" inside the system, as well as at the initial and final stages of the attack stages.

Keywords
cyber security, cyber-attack, monitoring agent, artificial intelligence (AI), machine learning, anomaly detection

1. Introduction

Cyber-attacks targeting the information systems of enterprises and public institutions are recently becoming more sophisticated. Consequently, the risk of information leaks caused by targeted attacks or attacks on software vulnerabilities are now becoming higher than ever.

Countermeasures against cyber-attacks include those performed by individual users of information systems such as by installation of antivirus software, and those performed by administrators of information systems such as installation and operation of firewalls and security gateways. At present, the mainstream tactic is to employ countermeasures based on data obtained from known viruses and attack techniques.

As a result, it is extremely difficult to discover and detect attacks that hit not-yet-public software vulnerabilities and also those that are unprecedented and completely new (hereinafter referred to as unknown attacks). Such attacks sometimes entail a long period before detection or are not found until a notification is received from an outside source.

In this paper, we introduce Automated Security Intelligence (ASI), which is a self-learning, system anomaly detection technology that is capable of detecting even unknown attacks quickly and of automatically isolating the affected extent of an attack. This is achieved by identifying the normal operation of the attacked information system using AI technology and by detecting changes in its operation in real time rather than by monitoring the attack techniques that are renewed every day.

2. Automated Security Intelligence (ASI) Technology

Fig. 1 (Left: Traditional. Right: ASI) shows an image of a traditional security monitoring system and that of an ASI-based security monitoring system. The traditional system shown in Fig. 1 (Left) presents the following issues:

- The SIEM (Security Information and Event Management) mainly monitors the logs output by the firewall (FW) and antivirus software. It cannot monitor information that the software developer does not intend to be output.
- The monitoring is based on the information on

known attack techniques and vulnerabilities. It cannot detect unknown attacks.

- While detailed analyses covering the internal status of FW and PC are required in cases in which distribution of operation logs in many locations necessitates much labor for analysis or that sufficient data for detailed analysis is unavailable.

The System Design Guide for Thwarting Advanced Targeted Attacks published by the Japanese IT Security Center deals with the previously emphasized "Delivery and Actions on Objective countermeasures" (virus detection/blocking via firewall and detection/elimination with antivirus software installed at the terminal). In addition it may also be necessary to enhance the internal measures, assuming an internal invasion of a virus by avoiding the traditional countermeasures.

ASI has been developed in order to solve the above issues. It detects attacks at all of their stages[2)], from the invasion of an internal system by an attacker to the expansion of the extent of an infection and the theft of important information. It thereby protects the system from such attacks and its main features are as follows (**Fig. 2**).

(1) Lightweight monitoring software for detailed log information collection

Traditional system operation monitoring software (agent) sometimes had unfavorable effects, such as PC or server delays. For the ASI, we always considered the loads on the system and developed a lightweight agent capable of the appropriate control of the timing of monitoring, etc. Thus, the collection of detailed logs, including the program launch, file access and network access are enabled without delaying the system operation.

The collected operations logs are managed in an integrated database so that the security manager can handle incidents speedily using detailed log analysis and without the need of collecting the log data distributed in different locations.

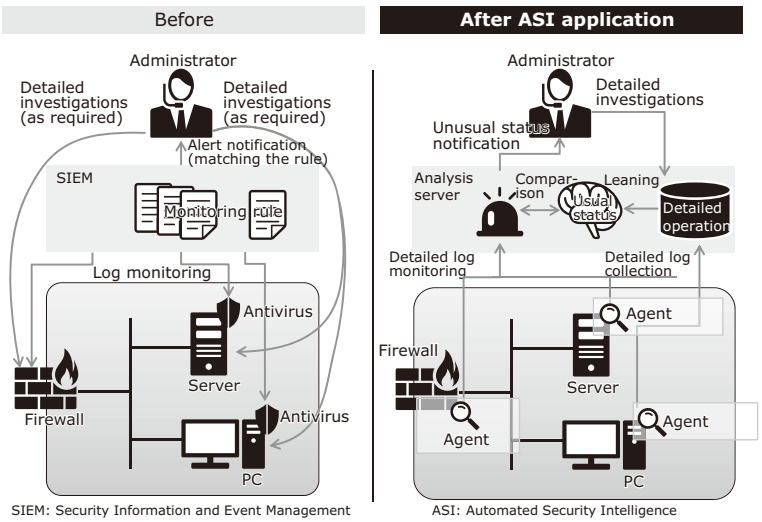

Fig. 1 Diagrams of security monitoring systems before and after application of ASI.

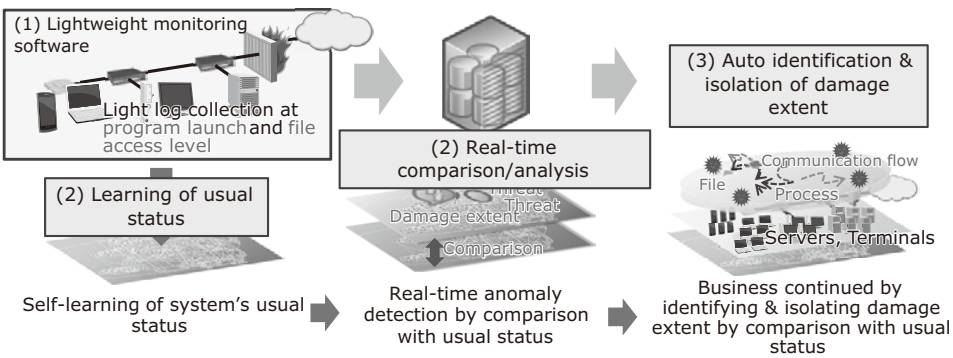

Fig. 2 Technical features of ASI.

(2) Real-time anomaly detection with AI

ASI learns (through machine learning) the usual status of OS-level activities (including program start-up, file access and network communications) of the entire system including PCs and servers. It compares the current system status with the usual status in real time and detects the deviation as an anomaly of the current system automatically from the usual status. When an anomaly is detected, it automatically identifies the series of system operations causing it and provides a defense that can minimize the damage extent without shutting down the entire system.

(3) Identification of damage extent and auto-isolation from the network

The detailed identification of system operations allows ASI to trace the series of system operations automatically over time, from the anomaly detection to the final definitive detection. This enables identification of the damage extent in 10% of the time taken previously by human labor. In future, ASI will be linked to system management tools and SDN (Software-Defined Networking) for performing auto isolation from the network by disconnecting the identified damage extent. Such measures as described above make it possible to minimize any increase in issues resulting from information leaks and system damage and to avoid an entire system shutdown.

3. Usual Status Generation Using AI Technology

As described in the previous section, ASI installs monitoring software called "the agent" in the PCs and servers in the system in order to collect the detailed operation logs of the machines in real time. It then applies AI learning processing to the collected operation logs and generates the usual status of the system as monitored by ASI.

The basic concept behind the generation of the usual status is that operations of the monitored system are stable. In this context, the operations refer to the program launch, file access from a program and network access from a program of the PCs and servers. More details on this topic are presented in the figure below.

Fig. 3 shows an enterprise network system in the usual status. The system in this example includes a subnetwork containing the servers shared within the enterprise. These include the DNS server and web proxy server, a development departmental subnetwork containing a development server and PCs used by the development staff. Also contained is an office departmental subnetwork used by the office staff.

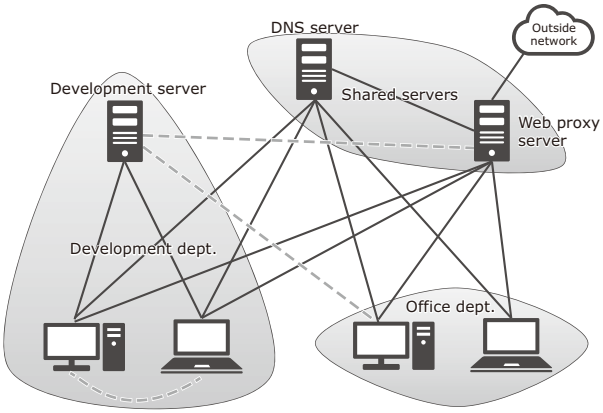

Fig. 3 Usual status of the system monitored by the ASI.

The shared servers are accessed in common by all of the enterprise PCs, while the development department server is accessed by the PCs in the development department. In general, the PCs in the office department do not access the development server in the development department. As seen here, the relationship between machines that is shown by solid lines in the figure is called the usual status.

After the learning of the usual status has completed, if a network access that does not belong to the usual status is detected, it is reported as an anomaly. For example, an anomaly is detected when two PCs in the development department communicate directly between each other, a PC in the office department accesses the development server of the development department, or the development server that usually does not communicate with the outside network communicates with the web proxy server. These events are shown by broken lines in the figure.

Direct connection between terminals in the same department is often observed in the infection spreading phase (lateral movement) of the attack process. In the case of connection from the development server to the web proxy server it is observed in the "Actions on Objective" stage (theft of important information) during the attack process.

As the main operation of a traditional cyber defense system consists of entrance/exit measures, it is accompanied with the issue of extreme difficulty of attack detection once those measures break down. Moreover, ASI increases the opportunities of attack detection because it detects attacks not only in the initial infiltration and "Action on Objective" stages of the attack process but also in the intermediate phase, in which the attacker spreads infection in order to locate the ultimate target of

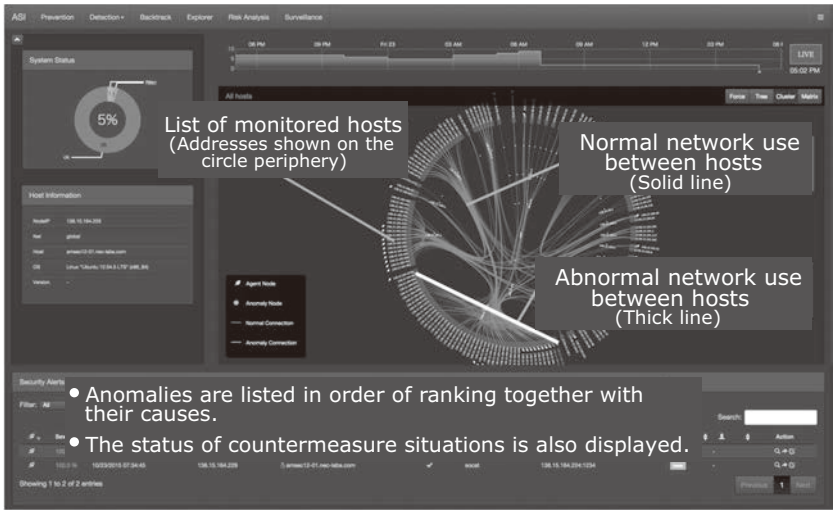

Fig. 4 Example of anomaly detection by ASI.

the system.

Although in the above we have focused on the usual status related to the network communications of PCs and servers, ASI also learns the usual status related to the program launch and file access from a program so that it can also detect any deviation from the usual status inside a PC or server that does not feature network communications.

Fig. 4 shows an example of an anomaly detection display of ASI (part of the display is modified for ease of viewing). The circular graph on the right indicates the monitored network, the thin solid line indicates the network connections of PCs and servers in the usual status, and the thick line represents the unusual network connection (detected as an anomaly).

4. Conclusion

In the above, we introduced ASI, which is a self-learning, system anomaly detection technology that employs AI technology to identify the normal operation of an information system that might be attacked. ASI detects changes in the system operation in real time, so that even when the system is actually subjected to an unknown cyber-attack, the attack is detected in real time and the extent of the damage is automatically isolated.

Reference

1) NEC Press Release: NEC technology uses artificial intelligence to automatically detect unknown cyber-attacks, December 2015
http://www.nec.com/en/press/201512/global_20151210_01.html
2) "Kill chain", Wikipedia,
https://en.wikipedia.org/wiki/Kill_chain

Authors' Profiles

TAGATO Hiroki
Principal Researcher
Security Research Laboratories

SAKAE Yoshiaki
Principal Researcher
Security Research Laboratories

KIDA Koji
Manager
Cyber Security Strategy Division

ASAKURA Takayoshi
Senior Manager
Security Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.11 No.1 AI & Social Value Creation - The World of "NEC the WISE" -

Vol.11 No.1
December 2016

Special Issue TOP