Security Situation Awareness and Situation Information Generation based on Spatial Linkage of Physical and IT Security

Hyeonkoo Cho†, Jungchan Na†

†Knowledge-based Information Security & Safety Research Department,
Electronics and Telecommunications Research Institute(ETRI), Daejeon, 305-705 Republic of Korea

Summary
In modern business human beings, information, infrastructure and system are organically bound; physical and virtual worlds coexist. Threats against information assets involve leakage through mobile storage media or physical break-in by an intruder, or leaking information by hacking, worm, virus and malicious bot in the cyber space. Therefore, the fragmentary technology like the existing physical security or IT security technologies alone cannot prevent the leak of the assets. To protect the information assets in the business environment, the technology of integrating physical space (work space) and the logical space (cyber space) to detect and prevent security violation accidents is needed. The objective of this paper is to propose the approach of mapping the security events with the real objects like the business space and PC in order to organically integrate and analyze the individual security events of the physical space and logical space based on the real spatial data in the business environment and detect the security situation after an event occurs using the real spatial data of the event and create the spatial linked security situation data according to the space-time association analysis of the security events in the space.

Key words:
Security situation, Situation awareness, Spatial linkage, Convergence security

1. Introduction

In most organizations currently, a security management process consists of three independent domains; physical security domain, managerial security domain and technical security domain. It is very difficult to link these domains as the manager and managed objects are different although the security system is under the same governing structure. In other words, even when each security system is properly established, it is difficult to prevent or respond the security accident enterprise-wide when vulnerability is generated in a domain. Therefore, managing these three domains from the integrated viewpoint is needed to prevent or respond security accidents, and such security is called convergence [1]. To protect the information assets under such convergence security in a business environment, the technology to organically integrate physical space (work space) and logical space (cyber space) to detect and prevent security violation is needed [2].

Although the technology of monitoring and controlling the access to the physical space and logical space using an integrated authentication card (smart card) has already been developed as one of the convergence security technology converging the IT security and physical security, there is a problem of having to change the existing infrastructure. There is the method of monitoring the user activities in the logical and physical spaces to detect the security violation by interfacing with IdM (Identity Management) which collects the security events from various sensors of the access control system and network security system in the physical/IT space, integrates and analyzes the linkage. However it is simple interface of the physical security technology and IT security technology or syntax based formalization of various security sensor events to analyze the event linkage to detect the security violation.

Such methods remains merely monitoring the security situation using the virtual spatial data and are considered to be inadequate to timely alarm the security violation and promptly and accurately perform the countermeasures by recognizing the security situation based on the actual spatial data of the business environment and to create the spatial linked situation data for chronological and spatial analysis. As such, we intend to propose the method of recognizing the security situation by cross linking the security events based on the security generation point and time through actual spatial mapping of the security events in the IT space and physical space and generating the spatial based situation data.

2. Security Situation in the Business Environment

Although the definition of convergence security and procedure of security management are not yet standardized, various organizations have been discussing and studying

Manuscript received January 5, 2011
Manuscript revised January 20, 2011

them. OSE (The Open Security Exchange) defines convergence as “the migration of physical security and IT security toward the same objective, process and architecture” [3] while Gartner explains it as the physical security and information protection having the similar, linked or same process and functions to manage the IT risk [4].

This paper defines convergence security as integrating and analyzing the security events on mobile data, host, network and classified files generated by the access information, CCTV image and location sensor in the actual space of the events in order to predict or detect the security violation and follow up to the security situation. It means the security management process based on the real space of the security events in the logical space and physical space. Such security process is defined in terms of the security situation awareness, analysis and response technology based on spatial linkage.

Spatial linkage of technologies to recognize, analyze and respond the spatially linked security situation means interface of the security sensors in the logical/physical spaces for convergence security and interface of security systems in the various security environments to analyze the relations in the spatial unit in order to recognize the security situation and following up based on the real space. It means the recognition of the security situation by analyzing the linkage in the work space (domain) unit through the actual spatial mapping based on the data detected and analyzed in the various IT security systems, generation of the situation data, determination of the security threat level by the association analysis of the security events, and performance of the monitoring, control and tracking function of the assets and manpower.

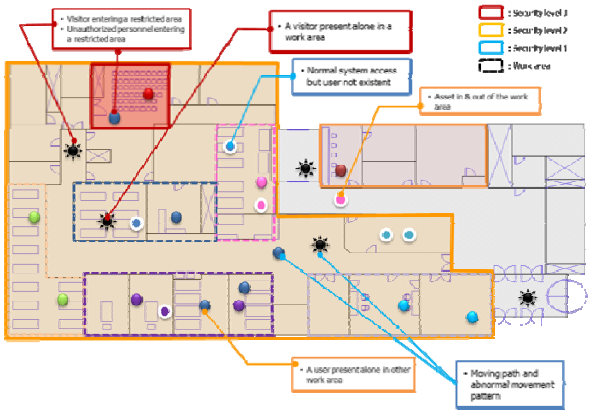


Fig. 1 Example of Spatially Linked Security Situation in the Business Environment

Figure 1 depicts an example of the security situation that is possible in the convergence security environment in which the events like entry/exit of the employees in the work space unit containing the information asset, use of the information asset, existence (individual existence, existence in unauthorized area, etc.) of the employee or visitor in the specific space, or change of location of the mobile information asset. This can be considered as the situation which cannot be detected or enables only the limited response by the fragmentary security system like the IT security or physical security alone.

The physical and logical security events under such security environment can be detected by various security sensors as shown in Table 1. The security events are interlinked, and such linkage will be the basic concept for recognizing and analyzing the spatially linked security situation in this paper.

Table 1: Linkage of Physical/Logical Spatial Security Sensors and Events

	CCTV	RFID/ Smart Card	Location sensor (e.g. GPS)	Environment sensor (e.g. temperature, humidity)	u-Sensor (Facility abnormality detection)	IDS/IPS/WIPS /FW	Anti-Virus/ Spyware	Router / System Logger	DLP	WEB
CCTV	Video surveillance/ control	Intelligent access control	Moving object security / control	Video surveillance	Video surveillance	X	X	Forensic	Forensic	Personnel and security profiling
RFID/ Smart Card	Intelligent access control	Personnel / asset in & out control	Moving object security / control	X	X	X	Host data / location	Host data / location	Asset in & out control	Intelligent access control
Location sensor (e.g. GPS)	Moving object security / control	Moving object security / control	Moving object surveillance and tracking	-	Abnormality generation location	Attack generation / target location recognition	Abnormal host location recognition	O Abnormal host location recognition	Information leakage point recognition	Location-based security data collection
Environment sensor (e.g. temperature, humidity)	Video surveillance	X	X	Disaster surveillance	X	X	X	X	X	X
u-Sensor (facility abnormality detection)	Video surveillance	X	Abnormality generation location	X	Technical facility (equipment) abnormality detection	X	X	X	X	X
IDS/IPS/WIPS /FW	X	X	Attack generation / target location recognition	X	X	Network attack	-	Intrusion prevention	Information leaking prevention	Advance detection / response
Anti-Virus/ Spyware	X	Host data / location	Abnormal host location recognition	X	X	-	Intrusion accident	-	-	Advance detection / response
Router / System Logger	Forensic	Host data / location	Abnormal host location recognition	X	X	Intrusion prevention	-	Abnormal host detection	-	X
DLP	Forensic	Asset in & out control	Information leakage point recognition	X	X	Information leaking prevention	X	△	Information asset leaking	X
WEB	Intelligent access control	Intelligent access control	Location-based security data collection	X	X	Advance detection / response	Advance detection / response	X	X	Personnel and security profiling

: Physical Security : Logical Security : Physical & Logical Security

The procedure for recognition and analysis of spatially linked security situation is organized of Action – Situation – Analysis & Decision – Visualization & Response (Figure 2). Action is the step of receiving the security event and detection data. Situation is the step of collecting the security events linked to the same space and time and generating the security situation data. Analysis & Decision determines the type and details of the security situation as well the degree of the security threat through the space time analysis. Lastly, Visualization & Response visualizes the recognized and analyzed security situation data and generates the message for the follow-up.

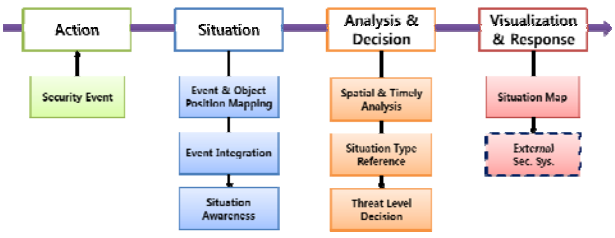


Fig. 2 Security Situation Recognition, Analysis and Follow-up Procedure

3. Method of Recognizing the Spatially Linked Security Situation and Generating the Situation Information

3.1 System Architecture for Spatially Linked Security Situation Recognition and Situation Information Generation

Figure 3 below depicts the system to recognize the security situation in the real space, recognize the spatially linked security situation to generate the situation data.

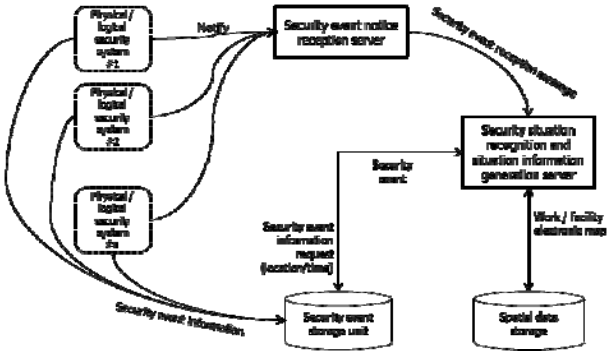


Fig. 3 Spatially Linked Security Situation Recognition and Situation Information Generation

The spatially linked security situation recognition and situation information generation system consists of the security event storage unit, spatial data storage unit, security event generation notice reception server, and security situation recognition and situation information generation server.

The security event notice reception server receives the security event notice from the physical/logical security system or sensors operating in the field and creates the received security event message to send it to the spatially linked security situation recognition and situation information generation server. The spatially linked security situation recognition and situation information generation server collects the event data from the security event storage unit according to the received message and map them with the real spatial data saved in the spatial data storage unit to integrate the linked security events to verify the security situation. It then recognizes the type of event to create the situation data and display the information on the real space based situation map.

3.2 Spatially Linked Security Situation Recognition and Situation Information Generation Server

The spatially linked security situation recognition and situation information generation server stores and utilizes the various security events and real spatial data using the security event storage unit storing the security events generated by the multiple security systems installed in the physical space or logical space with the unique information and the spatial data storage unit storing the location or object data of the real space in which the security event storage unit and security systems are installed.

Figure 4 depicts three major units of a spatially linked security situation recognition and situation information generation server. First, the security event collection unit maps the unique data of the security device with the real space location and object data stored in the spatial data storage unit, queries the security event storage unit according to the mapped data, and collects the related security events. Second, the security situation recognition unit determines the security situation type and threat level based on the security event and pre-defined security situation guidance upon detection of the security event. Last, the situation information generation unit analyzes the relationship between the security events linked to the security situation type and detected security events while the situation map display unit visualizes the recognized security situation on the electronic map based real space.

The notice message reception module of the security event collection unit receives the security event reception message to extract the security event generation time and ID data. The ID/location mapping module maps the security event to the location or object in the real space. The security event collection module uses the mapped location data to collect the security events linked to the same location or space and stored in the security event storage unit.

The security event verification module of the security situation recognition unit uses the security event location data to verify the validity of the event. The security situation type reference module refers to the security situation criteria defined to recognize the security situation of the abnormal security event. The security situation recognition module determines the security situation validity, type and degree of threat according to the abnormal security events and referred security situation criteria.

The space time association analysis module of the situation information generation unit defines the linkage of the security events according to the security situation type to generate the security situation information. The situation information generation module generates the security situation information that includes the real space data, security situation type and threat details based on the defined relations.

The situation map display unit displays the business/security section, personnel/asset object data on the electronic map of the business/facility and visualizes the recognized and generated security situation and its

details so that security officer can intuitively recognize them.

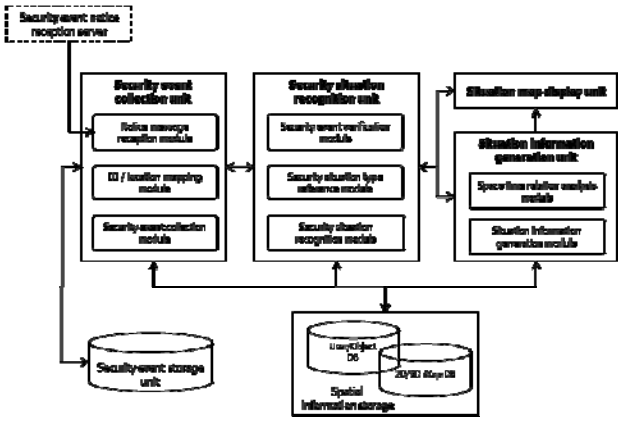


Fig. 4 Spatially Linked Security Situation Recognition and Situation Information Generation Server Function Architecture

3.3 Security Situation Recognition and Security Information Generation

Figure 5 shows the flow diagram of the security situation recognition and security information generation server.

The security situation recognition and situation information generation server processes all security events collected from the various security systems and sensors such as the access control system, RFID, GPS, temperature/humidity sensor, movement sensor, network intrusion detection/prevention system (IDS/IPS), firewall, system log, traffic analysis, information asset surveillance system, and data loss prevention system (DLP) in the physical and logical space and stored in the security event storage unit. When it receives the notice of a security event from the sensors or security systems, it maps it to the physical object or space (office, etc.) based on the business/facility electronic map based real space data and generates the integrated security event set by collecting the related security events from the security event storage unit based on the event generation time and location.

Based on the integrated security events, each security event is verified for consistency and validity using the security event generation time and location. If a security event is judged to be abnormal, the security situation criteria defined by the security policy referred to determine the situation type and degree of security threat. The space time linkage of the integrated security events is analyzed according to the recognized security situation type, and the relations between the security events within the security event set are defined. Then the meaning based security situation information containing the determined situation type and degree of threat is generated. The generated situation information is visualized on the electronic map based real space displayed on the situation map to complete the security situation recognition and situation information generation through the special linkage of physical/logical spaces. The security officer will then intuitively recognize the current security situation.

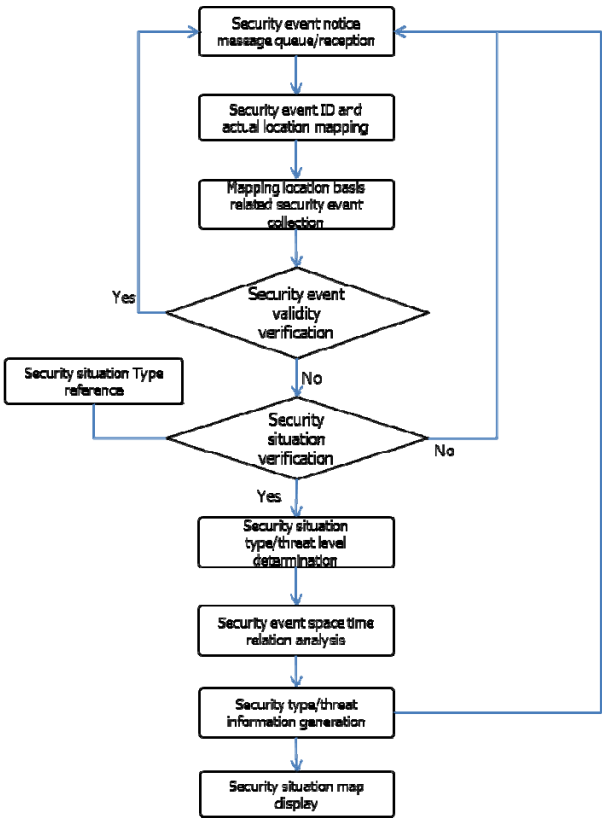


Fig. 5 Security Situation Recognition and Situation Information Generation Flow Diagram

4. Application of Spatially Linked Security Situation Recognition and Situation Information Generation

The proposed spatially linked security situation recognition and situation information generation system was applied to a scenario as shown in Figure 6. In the scenario, the security situation types included entry/exit, system access, access to files like classified documents, and moving path situation.

The degree of threat of each situation type was defined in levels 0 ~ 4. Table 2 summarizes the definition of mutual relations of the threat level of the logical/physical security events.

Spatially linked security situation recognition and situation information generation considers user (employee) entry/exit, system access, and usage of the system asset in a specific working space to recognize and analyze the

security situation and performs the response to provide the security function linked to entry/exit of the space (office, etc.) and asset access/usage event. This provides the means to recognize the situation and generate the situation information by linking with the physical or logical event (action) and to predict the threat level and perform the response using the result of analysis of the similarity of the security level and situation information to the security accident type and consistency of the logical/physical spatial action

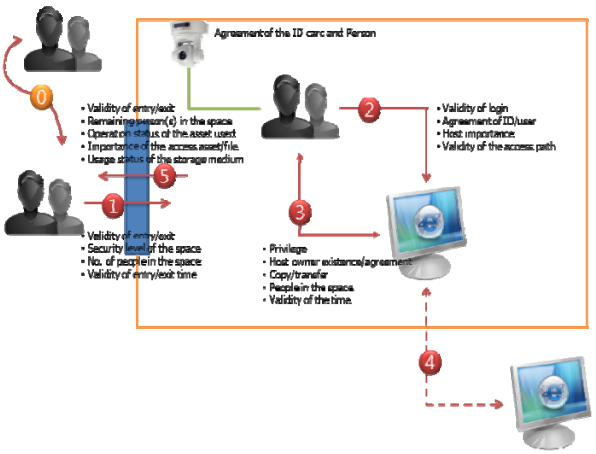
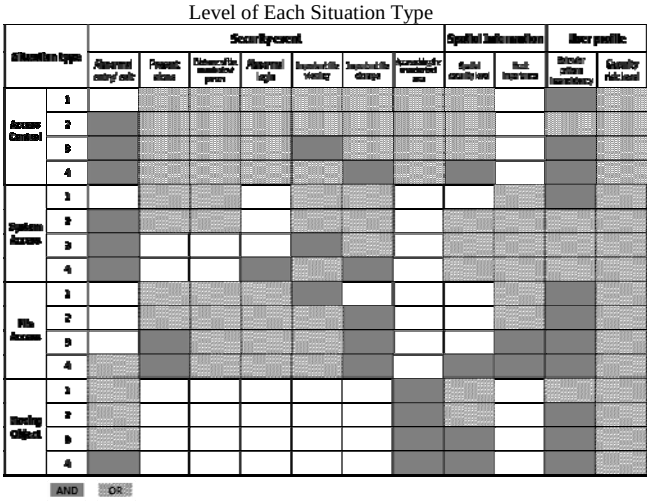


Fig. 6 Scenario of Applying the Security Situation Recognition and Situation Information Generation System

Table 2: Description of Determination of Event Relation and Threat Level of Each Situation Type



5. Conclusion

This paper describes a spatially linked security situation recognition and situation information generation system which more accurately and timely recognizes the various security situations and allows the real-time response compared to the individual security environment or simple physical/logical integrated security environment. It recognizes the security situation by mapping and spatial linkage analysis of the security events to the physical object or real space such as the business domain based on the location of the security event detected in the physical/logical security space in the various industrial environment in which the humans, information, infrastructure and system are organically bounded, generates the security situation information accordingly, and displays it on the situation map so that the security officer can intuitively recognize it. The proposed system uses the security event generation location to map the event with the actual space data and analyze the relationship in order to link the securities in the physical space and logical space. As the result, it can minimize the change to the infrastructure and architecture of the existing security systems and provides the basis to effectively monitor and track the security situations occurring around the industrial facility information assets based on the actual spatial information so that they can be responded. Furthermore, since it recognizes the security situation and generates the information through the convergence of the physical security and IT security and actual spatial linkage, it can easily detect the security violation by insiders (illegal ID stealing, etc.) that cannot be detected with the IT security alone. It resolves the fictiveness of IT security and ensures the consistency and substantiality with the actual space through the spatial linkage. The system is expected to provide the measures to detect the security threats in advance and take the responsive action by mapping the IT security events with the essence of the information assets on the field for monitoring and management.

For that, enhancing the definition of linkage of security events in the logical space and physical space in the ontology and studying the inference algorithm to recognize the security situation from the definition. The study of system framework for communication with the security system, interface and event processing to interface with various types of security system and process large volume of security events is also needed.

Acknowledgment

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] J. D. Kim, K. W. Kim and Y. D. Lee, “Establishment of Convergence Security Concept and Approach Method,” Journal of KIISC, vol.19, no.6, pp.68-74, 2009.
[2] Watson, James. “Physical and IT Security Must Go Together.” Computing, May 4, 2005.
[3] The Open Security Exchange (OSE), “Physical/IT Security Convergence: What It Means, Why It’s Needed, and How to Get There”, 2007.
[4] Nicole S. Latimer-Livingston, “Let's Get Physical What Clients Are Asking About the Integration of Physical and Logical (IT) Security", Gartner, November 9, 2007
[5] J. M. Choi and J. O. Kwon, “ Converged Security Market Trend Report,” Samsung SDS Journal of IT Service, vol.7, no.2, pp.13-29, 2010.

Hyeonkoo Cho received the B.E. and M. E. degrees in Information Communications Engineering from Chungnam National University in 1999 and 2001, respectively. During 2001-2005, he stayed in Virtual I Tech. Inc. to research image communication, and parallel processing. After four year stay in GTOPIA Inc. to research spatial image processing, GIS, and LBS. Currently, He has been a senior member of technical staff at Electronics and Telecommunications Research Institute (ETRI) in Korea since 2010. His research interest includes image processing, GIS, security management, security situational awareness, and visualization of security situation.

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.