International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.315-320
http://dx.doi.org/10.14257/ijsia.2013.7.5.29

Security Management Architecture for Secure Smartwork Center

Yun sang Byun[1] and Jin Kwak[2]

[1]*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Korea*
[2]*Department of Information Security Engineering, Soonchunhyang University, Korea*
[1]*ysbyun@sch.ac.kr*, [2]*jkwak@sch.ac.kr*

Abstract

Since smartwork can provide a flexible and convenient mode of work for employees, many companies are preparing to adopt smartwork systems for their work environments. In addition, many companies are supporting a "SmartWork Center" to increase the staff's work efficiency. However, in a smartwork center, most users use public devices and work in open network environments. As a result, there can be security vulnerabilities such as the leakage of secret data, invasion of privacy, viruses, and the spread of malware. Therefore, in this paper, we proposed Security management architecture for the construction of a secure smartwork center.

Keywords: *Security management, Smart work security, Smartwork center*

1. Introduction

Smartwork is a flexible type of work that provides users with a more convenient work environment. For this reason, many companies are preparing to adopt smartwork systems for their working environments. In particular, many companies are supporting the work activities of employees using a smartwork center to promote work efficiency. However, in a smartwork center, work is often conducted in an open environment and multiple users may use public devices. Therefore, there can be security vulnerabilities such as the leakage of secret data, invasion of privacy, viruses, and the spread of malware. Therefore, in this paper, we propose a security management architecture for the construction of a secure smartwork center [1, 2]. The remainder of this paper is organized as follows. In Section 2, we analyze related work. In Section 3, we proposed security management architecture for the construction of a secure smartwork center. Finally, in Section 4, we present our concluding remarks.

2. Related Work

2.1. Smartwork Center

Smartwork is a feature of future-oriented work environments; in such environments, tasks can be performed using a variety of devices such as computers, smartphones, and tablet PCs. Therefore, a conventional physical office space is no longer necessary. In particular, a smartwork center creates a work environment that can be customized to suit the specific needs of individual companies, which then provide this new work environment for their employees. A smartwork center has several advantages which offer IT infrastructure, video conferencing systems, and certain level of security.

ISSN: 1738-9976 IJSIA

2.2. Security Management

The target of security management is to ensure that IT resources are protected from cyber-attack. In this regard, service monitoring, analysis, and the corresponding security events and logs are managed in real time at a central control center. Typically, the different types of security management are classified as remote security management, dispatch security management, and self-security management. The remote security management is performed through the service provider. The service provider is equipped management system, which enables the security event monitoring. It can prevent a security accident, and when security accident occurs, we can respond to the situation rapidly. Dispatch Security management is the controller of the target institution, which constructs its own security control system, and dispatches security monitoring specialists from the company who can take control of the situation. Self-security management is a security control system that the company constructs and operates using its own skilled workers. The types of security management are presented in Table 1 [3].

Table 1. Three Types of Security Management

Type of Security Management	Contents
Remote Security Management	- In charge of certain units of the security system operation and management. - Security management system and control personnel in a remote location.
Dispatch Security Management	- Self-built security control system under the charge of management. - Professional personnel dispatched to the target organ to perform security management.
Self-Security Management	- Self-security management performs the operations and management itself.

2.3. Critical Risk Factors

Critical risk factors are considered the major cause of a variety of risks. These factors can arise from a variety of different risk factors that can depend upon the operating environment of individual companies and organizations. Some examples of major critical risk factors are presented in Table 2 [4-5].

Table 2. Critical Risk Factors

Development stages	Infringement	Contents
Storage	Data leakage and loss at the point of information saving.	- Authentication and access control are vulnerable, resulting in leaks via viruses and malware.
Use	Illegal use.	- Information is used for purposes other than for which it is intended. - Information is used or sold to others without the consent of the company or organization.
Provide	Data leakage and loss at the point information provision.	- Data leakage and loss via a lack of encryption. - Authentication and access control are vulnerable to hacking.

2.4. Security Management Requirements

2.4.1. Attack Detection and Integration: In order to detect a variety of cyber-attacks, one must be able to collect security events from a variety of different types of security solutions such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). One should also be able to determine the factors that cause fatal security incidents.

2.4.2. Real-time Security Management: Security incidents can occur at any moment, so real-time security management should be available. Although it is difficult to prevent all security incidents and proactively prevent them, there should be a means of capturing the signs of an attack, or of providing rapid detection after the occurrence of a security incident.

2.4.3. Big Data Processing: Security events are gathered from a number of different systems; thus, a large volume of data (big data) is collected. Therefore, the processing of such big data should be continually available, and the related data processing, analysis, and data arrangement should not cause a delay.

3. Proposed System

In this section, we propose a security management architecture that can resolve the security risks that may occur in the open space of a smartwork center. The proposed system regards the use of the corporate network in smartwork center and the problem of access by malicious users and the detection of malicious codes. In addition, in the event of a security incident, there is a security management architecture that responds rapidly. The proposed architecture consists of a Risk Measurement module, a Management & Analysis module, and a Support module. The security management service in the previous step is used to access the corporate network from the smartwork center. The concept of the proposed system is described in Figure 1.

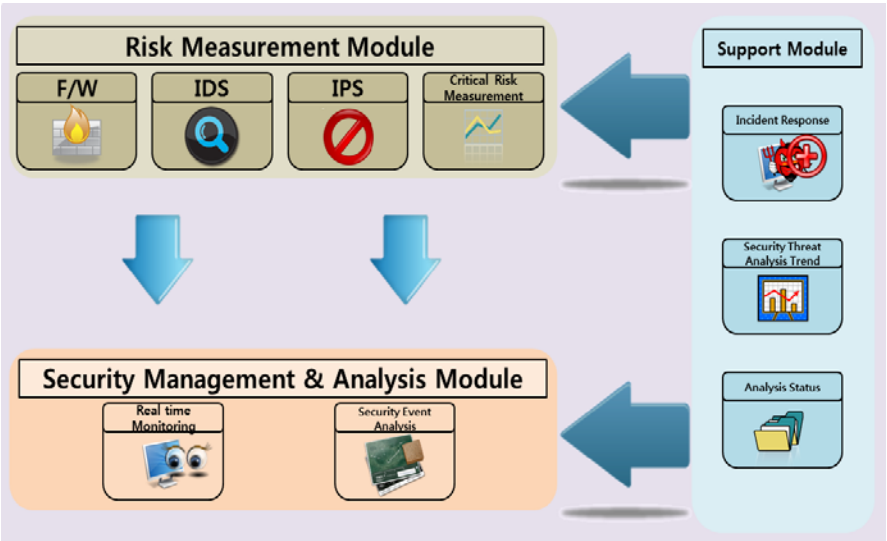

Figure 1. Proposed Architecture

3.1. Risk Measurement System

The Risk Measurement module consists of a subsystem that includes a firewall, IDS, and IPS. The module is also designed to collect security events. The Critical Risk Measurement System also shares the data collected with other subsystems, and can thus determine the factors that could cause fatal security incidents. The results are then sent to an analysis system. The concept of the Risk Measurement System is shown in Figure 2.

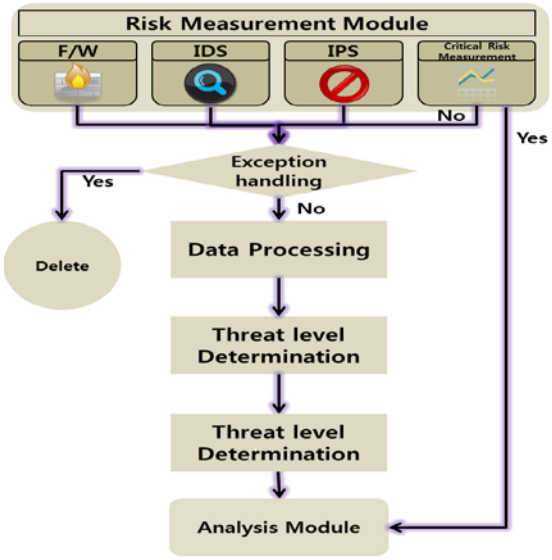

Figure 2. Risk Measurement Module

3.2. Security Management and Analysis Module

The Security Management & Analysis module consists of a real-time monitoring system and a security event analysis system. The real-time monitoring system is based on data collected by the Risk Measurement module sub-system to detect security events.

The security event analysis system receives the data collected by the Risk Measurement system. This then permits the analysis of various kinds of events and the establishment of countermeasures.

The analysis system analyzes the big data collected from the different solutions (IDS, IPS F/W). Therefore, each piece of collected data is sent to the roles set by the sub-system, and the data is stored in a temporary table for analysis. Additionally, the sub-systems are designed to be parallel, and simultaneously, can handle big amount of data.

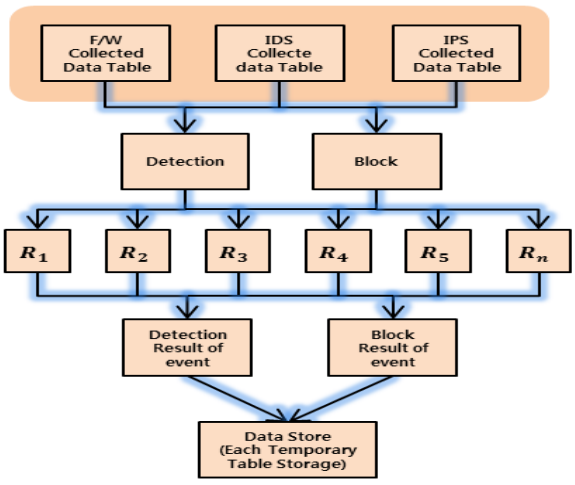

Figure 3. Security Management and Analysis Module

3.3. Support Module

The Support module consists of an incident response support system, situation analysis system, and security threat trend analysis system. The incident response support system can respond rapidly to the threat using the received data, and the situation analysis system organizes information related to the current state of the response to a security incident. In addition, the security threat trend analysis system provides support to prevent the repetition of damage that has occurred, in its analysis of the current state of various security threat factors.

When a security incident occurs, the subordinate systems of the Support module configure the appropriate databases to organize information related to threat factors, so both their detection and response can take place with speed and precision.

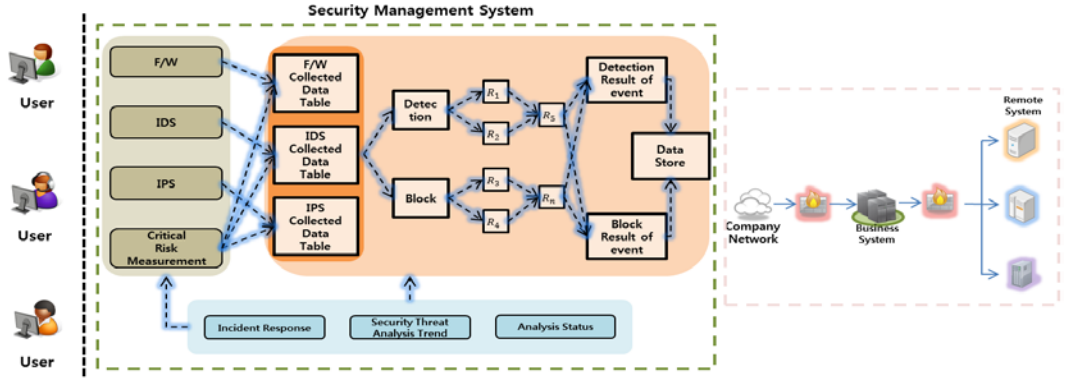

Figure 4. Security Management Structure

4. Conclusion

In this paper, we proposed a security management architecture that can provide secure service in a smartwork center. The proposed system creates databases that collect data related to various security factors. In addition, we expect that proposed system will be able to provide a rapid response in its analysis of any amount of security events through its unique design, which consists of multiple parallel subordinate systems.

The proposed security control system is expected to satisfy the requirements for work that is conducted in a smartwork center, and to contribute to the security control of that work effectively. As a future task, our intention is to perform research that analyzes the performance, efficiency, and other factors related to the monitoring system proposed in this paper.

Acknowledgement

This work was supported by the Soonchunhyang University Research Fund.

References

[1] S. K. Park and J. H. Lee, "Smartwork Technology and Standardization Trends", TTA Journal, vol. 136, **(2011)**, pp. 79-84.
[2] R. Bejtlich, "Tao of Network Security Monitoring, Beyond Intrusion Detection: What is Network Security Monitoring", Addison Wesley Professional, **(2004)**, pp. 40-41.
[3] M. S. Jeong and D. B. Lee, "Analysis of Security Threats and Security Requirements in Smartwork", Journal of the Korea Institute of Information Security and Cryptology, vol. 23, no. 3, **(2011)**, pp. 30-37.
[4] Y.-J. Jang and J. Kwak, "A Study on Secure User Authentication Protocols in Smartwork Systems", Proc. of SAM 2012, International Conference on Security and Management, Las Vegas Nevada, **(2012)**, pp. 567-568.
[5] S. K. Cho and M. S. Jun, "Privacy Leakage Monitoring System Design for Privacy Protection", Journal of the Korea Institute of Information Security and Cryptology, vol. 22, no. 1, **(2012)**, pp. 99-106.

Authors

Yun Sang Byun received his B.S. degree in Information Security from Soonchunhyang University (SCH), South Korea, in 2012. He is now a candidate for an M.S. degree in the Information Security Application and Assurance Lab at Soonchunhyang University. His research interests include user authentication in Smartwork and cloud computing security, and cryptology.

Jin Kwak received his B.S. (2000), M.S. (2003), and Ph.D. (2006) degrees from Sungkyunkwan University (SKKU), Korea. Before joining the faculty of Soonchunhyang University (SCH) in 2007, he was a visiting scholar at Kyushu University, Japan. Subsequently, he served at the Ministry of Information and Communication (MIC), Korea, as Deputy Director. Furthermore, he served as Dean of the Department of Information Security Engineering (DISE) at SCH (2009–2010) and Vice-Dean of the College of Engineering (2009) at SCH. He is now a Professor at DISE. In addition, he is Director of the SCH BIT Business Incubation Center and of the Industry-University & Institute Partnership Division Center at SCH. His main research areas are cryptology, information security applications, and information assurance.

