JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 2: 207~214, Feb. 2019

스마트워크 시스템을 위한 사이버 공격 및 사이버 보안 설계

천재홍[1] · 박대우[2*]

Cyber-attack and Cybersecurity Design for a Smart Work System

Jae-Hong Cheon[1] · Dea-Woo Park[2*]

[1]Ph.D. Student, Department of Convergence Science and Technology, Hoseo Graduate School of Venture at Hoseo University, Seoul, 06724 Korea
[2*]Professor, Department of Convergence Science and Technology, Hoseo Graduate School of Venture at Hoseo University, Seoul, 06724 Korea

요 약

기술 발전 속도가 증가되고, 고성능의 디지털 기기가 확산되고 있다. 기존 유선 환경에 최적화 되어 제한적으로 활용되던 PC와 같은 유선 디지털 기기에서 시·공간의 제약에서 벗어나, 언제 어디서나 효율적인 업무 수행이 가능한 스마트워크로 전환되고 있다. 유선환경에 비해 물리적 위협(단말기 분실, 도난 및 파손 등), 기술적 위협(도난, 서비스 거부, 비인가 접근 등) 등 다양한 보안 위협에 대해 무결성과 가용성을 확보할 수 있는 시스템 보안설계가 필요하다. 본 논문 연구에서는 스마트워크의 네트워크시스템, 유·무선 링크시스템, 디지털 스마트기기를 분석한다. 현재 업무에 사용되고 있는 스마트워크 유선시스템과 향후 무선시스템을 위한 보안설계 방안을 연구한다. 본 연구는 안전한 스마트워크 구축에 기초자료로 활용될 것이다.

ABSTRACT

The speed of technological development is increasing, and high-performance digital devices are spreading. Wired digital devices such as PCs have been optimized for existing wired environments, but needs are shifting away from the constraints of space and space to smart work that enables efficient work anywhere and anytime. The Smart Work System security design is needed to secure integrity and availability in the face of various security threats including physical threats (lost, stolen, and damaged terminals), technical threats (data theft, DoS: denial of service), and unauthorized access outside the wired environment. In this study,, we analyzed smart work network systems, wired / wireless link systems, and digital smart devices. We also studied cyber-attack analysis and cybersecurity design methods for a Smart Work wired system and a future wireless system. This study will be used as basic data for building a secure Smart Work system.

키워드 : 사이버 공격, 사이버 보안, 스마트워크, 네트워크 장치, DDoS 공격

Key word : Cyber-attack, Cybersecurity, Smart work, Network Device, DDoS Attack.

Received 12 October 2018, **Revised** 29 October 2018, **Accepted** 12 November 2018

*** Corresponding Author** Dea-Woo Park (E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Professor, Department of Convergence Science and Technology, Hoseo Graduate School of Venture at Hoseo University, Seoul, 06724 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.2.207 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. Introduction

Smart Work is a way to take advantage of fast-growing ICT technology to release users from time and place constraints. Companies are investing in developing and applying technologies for smart work using mobile devices to reduce costs and improve work productivity.

Smart work technology provides a flexible work environment that allows people to work in a Smart Work center built by corporations, governments, and public agencies, or to telework through a variety of mobile terminals such as laptop computers, smart phones, and tablet PCs.

In November 2010, the Ministry of Public Administration and Security opened the Smart Work Center, which could be used by government ministries, municipalities, public institutions, and private companies, for the first time in Korea.

The Ministry of Public Administration and Security plans to lead the establishment of domestic Smart Work environments by supporting the establishment and operation of Smart Work centers for public and private companies. This will be done by enacting standards and operating methods for Smart Work Center facilities, and by creating the legal and institutional bases for the spread of Smart Work [1].

For Smart Work, we use ICT technology such as wired and wireless networks and high-performance digital devices. The Smart Work environment is being set up by providing high-performance digital smart devices such as smart phones and tablet PCs, including existing laptop computers, and expanding the pertinent infrastructure.

As companies configure and operate Smart Work systems, efficiency can be improved through higher productivity and cost reduction.

However, there are new security threats such as malicious code intrusion and hacking, as well as new security threats such as device security threats, app security threats, and network security threats due to the use of smart devices.

In this study, we investigated the security threats to wired and wireless networks and attacks and defenses among the security threats to Smart Work, and constructed a network to enable secure Smart Walk operation through a security design for wired and wireless networks.

Ⅱ. Related Work

Smart Walk is a future-oriented work environment that can use both ICT technology and existing business methods to balance work and home life. In the Smart Work environment, environmental constraints such as time and place are minimized so that necessary tasks can be efficiently performed anytime and anywhere. In addition, it is possible to solve problems through real-time communication using a variety of tools such as teleconferencing and messengers [2].

2.1. Smart work types

The types of work done in the Smart Work environment can be classified as telecommuting, Smart Work center, and mobile work, depending on the work environment characteristics shown in Table 1 [3].

- Telecommuting

Telecommuting is the process of conducting work at home rather than at the company. Work is conducted online on the company's internal network, and includes work conducted through remote meetings and collaboration with other workers.

Telecommuting has the advantage of saving time and transportation costs by removing the need for some workers to commute (arrive and leave), and by minimizing the office space needed by the company.

- Work in the Smart Work Center

The Smart Work Center is a space equipped with a remote business system built by government agencies, public institutions, or corporations. It allows work to be performed by utilizing the office space required for the work and by providing computer equipment such as

computers. A Smart Work Center provides a basic management system and security such as for access control and vaccine program provision, and can work in an environment similar to a business operation within the enterprise.

- Mobile work

Mobile work is performed on the move, utilizing exchange of information and collaboration without relying on a particular place by utilizing various mobile terminals such as laptop computers, smart phones, and tablet PCs in mobile office environments.

This approach is suitable for the types of work that involve many business hours away from the company on business trips, customer interviews, and consulting.

Table. 1 Smart work types

Shape	Contents
Telecommuting	Connect to company business system and work at home
Work in the Smart Work Center	Visit the nearest Smart Work Center to work
Mobile work	Work on-site or on-the-go using the company's mobile business system work environment

2.2. Smart Work Technology

Security-related technology is needed to cope with malicious code in such as information communication devices. Network related technology is needed for digital smart devices and network configuration operation, user authentication, content encryption, network control and encryption, and digital smart device security for secure configuration. Smart work and operational management technology is also needed for Smart Work solution operation.

Smart Work technology involves a variety of elements such as Smart Work network technology, Smart Work service technology, Smart Work content technology, and Smart Work platform technology [4][5].

2.3. Smart Work Standardization

For application overseas, Smart Work standardization is conducted by international standardization organizations such as ITU-T and IETF, mainly for telepresence. Smart Work standardization is not being handled in Korea, but a Smart Work forum for Smart Work activation (a Smart Work project group) is in preparation [4][6].

2.4. Smart Work Security-attacks

In a Smart Work environment, security threats include software security threats (leakage of important data, malicious code infections, remote access using applications, and information leakage), physical threats (theft and loss of digital smart devices like smartphones and tablets), and network security threats via connection to the Internet [7][8].

Cybersecurity is an issue because digital smart devices equipped with high-capacity memory and high-performance CPU can store personal information such as call history, messages, contacts, schedule and location information, financial information, and company confidential information according to business performance [9].

When a digital smart device is stolen or lost, there is a possibility that the stored personal information and business information could be leaked to the outside. It might become possible to exploit and access the internal business system of the company to leak, destroy, or alter information [10].

In digital smart devices, a personal firewall must be installed to suit the corporate network environment or external environment [11]. To enable remote deletion and location tracking in preparation for loss or theft of digital smart devices, a digital terminal for a dedicated security system such as MDM should be applied [12].

Ⅲ. Smart Work Wired / Wireless System Analysis

3.1. Network System Analysis

In Smart Work, users mainly work from outside the company by connecting to the internal business system.

Accessing the enterprise internal business system

from the outside via external Internet or computer equipment exposes the company to a relatively large number of security threats compared to similar access from within the enterprise. Moreover, the risk of exposing the internal system to the outside is increased.

3.2. Analysis of Wired and Wireless Link Systems

Access to corporate internal business systems via open devices such as wireless LANs and public networks can be used for malicious code propagation and infection paths, or used as a dissemination route of unauthorized and harmful software. These could be used to collect personal information, leak corporate information, or set up zombie terminals.

3.3. Digital Smart Device Analysis

To secure personal and business information such as contacts, messages, and location information, digital smart devices should be equipped with a dedicated terminal, firewall, data encryption and a double backup system to cope with the threat of lost or stolen access.

3.4. DDoS Attack Analysis

- HTTP-Get Flooding

Unlike a DDoS attack targeting the connectivity of the network, this threat involves analysis and attacks to the HTTP layer mainly by attacking the application part of the TCP / IP layer.

- Cache Control Attack

This is an attack that causes the server to overload by sending a value containing the Cache Control code to the HTTP User Agent Header using the NetBot DDoS tool.

- VoIP Attack

This is an attack that interrupts the normal VoIP communication service between users by attacking the VoIP server. The server is called continuously so that it cannot respond.

- SQL Attack

After constructing the SQL Query statement about the ID and Password entered by the user, an SQL Query for DB access is created using the value input from the user. The SQL attack hinders normal operations of the user by manipulating the SQL Injection attack technique to modulate normal SQL Queries.

- TCP SYN Flooding

This is an attack that causes overflow of the Listen Queue, which processes the TCP session of the attacking target equipment by sending the TCP SYN packet to the attack target equipment instantaneously, thereby blocking the normal session connection due to failure of the system. (Fig. 1)

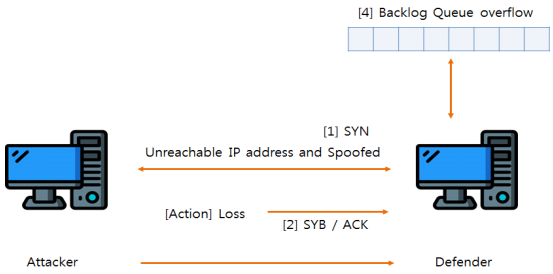

Fig. 1 DDoS Attack forms of Transport classes - TCP SYN Flooding

- TCP ACK Flood Attack

When a TCP session is connected using ACK, a TCP ACK packet is randomly transmitted without a TCP session, and the receiving system sends an RST packet and ICMP host unreachable packet to the transmission IP. This causes an overload of the receiving system and constitutes an attack. (Fig. 2)

- IP Spoofing

This is an attack that exploits a security weakness of the IP and accesses another system by modifying its IP to appear to be a trusted IP.

- ICMP Flooding

This is an attack on the network part of the TCP / IP layer and causes ICMP echo replies to be sent to the attacking target in large quantities, causing the ICMP echo reply to cause the receiver to overload the target system. (Fig. 3)

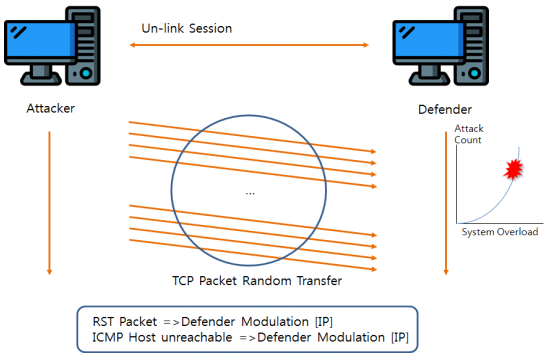

Fig. 2 Forms of DDoS Attacks by Transport classes - TCP ACK Flooding

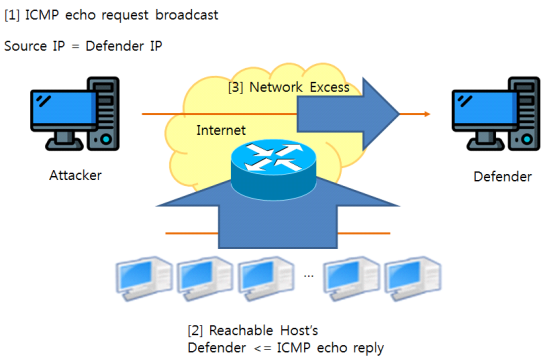

Fig. 3 Network (DDoS Attack forms - ICMP Flooding of Internet) Classes

Ⅳ. Security Design of Smart Work Wired and Wireless Systems

4.1. Security Design of Smart Work Wired and Wireless System

To cope with cyber security threats such as hacking and malicious code, and to control access by unauthorized persons, it is necessary to establish and operate an intrusion prevention system in a section connected to an external wired / wireless communication network. It is also needed to provide a harmful-traffic detection system for abnormal access and traffic monitoring of DoS, DDoS, and other denial-of-service attacks.

4.2. Design of Wired and Wireless Link Security Systems

The internal business system connection is designed to allow selective connection only to the mobile communication network (Wibro, CDMA, W-CDMA), and to block all connections through a wireless LAN and Bluetooth (such as WiFi and tethering).

A virtual private network (VPN) communication channel using AES 128-bit, ARIA 128-bit, SEED 128-bit or more cipher algorithms is designed to be used for blocking voice and data traffic.

4.3. Design of a Digital Smart Device Security System

To secure the data, it is encrypted using AES 128-bit, ARIA 128-bit, or higher encryption algorithm. It is designed to be backed up or stored in the user's digital smart device and within dedicated storage inside the enterprise.

To authenticate a user of the digital smart device, one-way encryption with a password of nine or more digits must be performed, and the connection should be blocked when the password is not set, or when an input error occurs more than a predetermined number of times. In cases of high security, authentication using biometric information such as PKI, OTP, and fingerprints should be applied.

4.4. Defending Against DDoS Attacks

For overall detection and defense we use a method that complements the functional advantages and disadvantages required for effective defense against DDoS attack. These include such as availability based on bandwidth extension, behavior-based detection defense, signature-based detection defense, and zero-day attack detection defense.

- Availability due to bandwidth expansion

When a DDoS attack occurs, a traffic overload occurs in a moment, and a failure occurs such that normal service cannot be performed. Even if a DDoS attack occurs, the bandwidth of the network line must be expanded to cover traffic due to DDoS attacks, to guarantee normal service.

However, the method of responding to the DDoS attack by increasing the bandwidth has the problem that excessive cost is incurred. Therefore, rather than expanding availability by bandwidth expansion, a logical Ethernet channel can be configured to expand the network traffic path, thereby ensuring bandwidth and availability and appropriate response to DDoS attacks. (Fig. 4, 5)

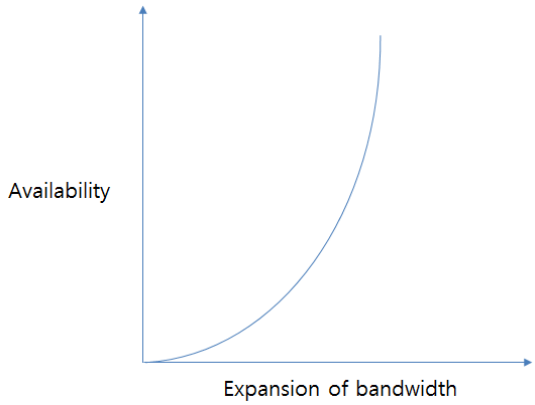

Fig. 4 Relationship with expense and bandwidth

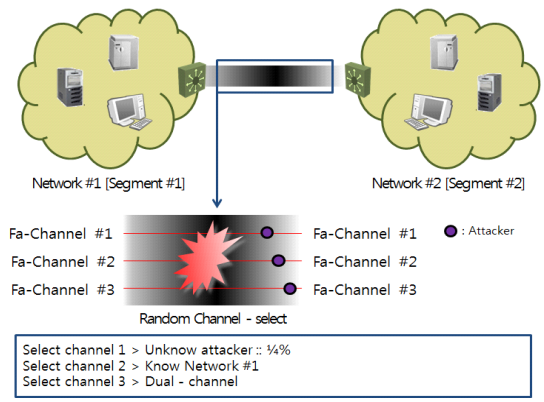

Fig. 5 Ethernet Channel - bandwidth expansion that is logical

- Behavior-based detection defense

Behavior-based detection defense is one of the detection methods for cognitive defense against DDoS attacks. Using this method, it is possible to detect and block malicious code and DDoS attack types by similar analysis and management of information about various access types in the past. (Fig. 6)

When an action similar to a malicious code or a DDoS attack occurs, by monitoring all the actions occurring in the computer system and the network, this defense tracks and analyzes the executable file or network information that caused the action; then, it terminates and blocks the executable file or the specific network.

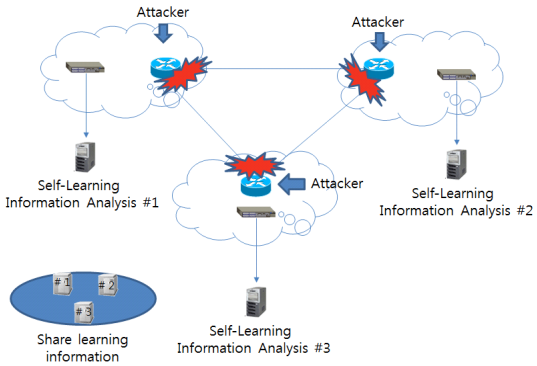

Fig. 6 Study style technique detection stamp

- Signature-based detection defense

The most effective way to detect an attacker is a “signature-based detection” technique that uses a specific pattern of network traffic to detect a malicious attack.

A signature can be generated using the pattern traits of malicious network traffic. It is possible to identify the target sequence of packets without examining all packets, check each connection state, and block packets using the illogical sequence Method.

- Zero-day attack detection defense

This is an attack method that uses the time taken until the first report on malicious code, virus and system vulnerability, etc., to develop, deploy, and install malicious code.

New vulnerabilities, malfunctions, and viruses can take a long time to analyze and to apply security patches, signatures, and solution development and deployment, and attackers use these vulnerabilities to create and spread malicious viruses. (Fig. 7)

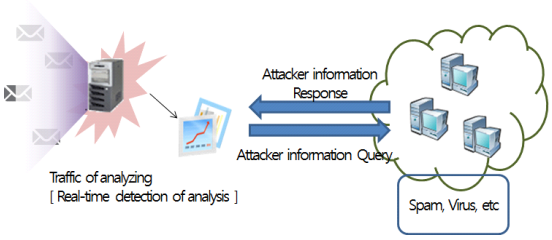

Fig. 7 Zero-day Attack detection defense

By monitoring and analysis in real time by applying accurate repetitive pattern detection technology to network traffic, it is possible to cope with infringement by malicious code and viruses immediately after contact.

Ⅴ. Conclusions

In this paper, we present our results from a study on network system analysis, wired / wireless link system analysis, digital smart device analysis, and a design for the establishment and operation of a secure Smart Work system. We analyzed the cyber-attacks on wired and wireless Smart Work Systems. We analyzed in detail a DoS attack as part of a network attack on the Smart Work System. Based on the results from analysis of these cyber-attacks, a design for cyber security of the Smart Work System was studied and proposed.

To establish and operate a secure Smart Work environment, continuous research is needed to ensure higher reliability by establishing and applying appropriate security measures. This is done by responding to security threats through systematic risk management and analysis of vulnerability.

References

[1] MINISTRY OF PUBLIC ADMINISTRATION AND SECURITY, “Smart Work Promotion Plan,” 2010.

[2] KOREA COMMUNICATIONS COMMISSION, NATIONAL INFORMATION SOCIETY AGENCY, “Smart Work Introduction and Operation Guidebook for Enterprises,” 2011.

[3] J.S. Kim, and K.S. Han “The key technology factors of Smart work and the situations in Korea and overseas,” *The Journal of the Korea Contents Association*, vol. 14, pp. 14-20, March 2016.

[4] S. K. Park, and J. H. Lee, “Smart Work Technology and Standardization Trends,” *TTA Journal*, vol. 136, pp. 79-84, July. 2011.

[5] M. A. Abbas, and J. P. Hong , “Survey on Physical Layer Security in Downlink Networks,” *Journal of Information and Communication Convergence Engineering*, vol. 15, no. 1, pp. 14-20, March 2017.

[6] W. Hyun, and S. K. Kang, “Smart Work Standardization Trends - Focusing on Telepresence,” *Electronic Communications Trend Analysis*, vol. 26, no. 2, pp. 42-49, April 2011.

[7] H.W. Kim “An Analysis of Security Threats and Vulnerabilities for Information Protection in Smartwork Environment,” *In Proceeding of the Korea Contents Association Conference*, pp. 291-292, November 2014.

[8] J.H. Park, “Current Status of ICT Device Authentication Security Technology,” *The Journal of The Korean Institute of Communication Sciences*, vol. 31, no. 5, pp. 20-26, April 2014.

[9] J.H. Kim, and J.K.K im, “An Empirical Study on Interaction between Threats and Efficacy of Security : Focused on the Smart-phone Users,” *The Journal of Internet Electronic Commerce Resarch*, vol. 15, no. 3, pp. 1-17, June. 2015.

[10] H. Y. Lee, J. H. Jung, and K. W, Son, “Smart Work Security Threats and Countermeasures,” *Journal of The Korea Institute of Information Security and Cryptology*, vol. 21, no. 3, pp. 12-21, May 2011.

[11] KOREA INTERNET & SECURITY AGENCY, “Internet & Security Issues,” April. 2012.

[12] H.K. Kim, S.J. Kim, H.K. Lee, and, H.K. Jung, “Light-weight System Design & Implementation for Wireless Intrusion Detection System,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 18, no. 3, pp. 602-608, Mar. 2014.

천재홍(Jae-Hong Cheon)

2007 Department of Information Security at Soongsil University (Master of Engineering)
2018 Acquiring CISA Licenses
2019 Completion of PhD Courses in Convergence Science and Technology at oseo Graduate School of Venture at Hoseo University in South Korea
1997 ~ Present Korea Environment Institute
※ Areas of interface : Hacking, Fornsic, Countermeasure of Infringement Accident, Information Protection, Mobile Security, Cybersecurity, Information Security Equipment, Smartwork

박대우(Dea-Woo Park)

2004 Department of Computer Science at Soongsil University (Doctor of Engineering)
2004 Professor at Soongsil University
2006 Senior Researcher of the Korea Information Security Agency (KISA)
2007- Present Professor in the Hoseo Graduate School of Venture at Hoseo University in South Korea
※ Areas of interest : Hacking, Fornsic, CERT/CC, Responding to an Infringement, e-Discovery, National Cybersecurity, Cyberssecurity, Information Protection, Mobile Communications Security, Convergence Security, IT convergence