ICIC Express Letters
Part B: Applications
Volume **10**, Number **7**, July **2019**

ICIC International ©2019 ISSN 2185-2766
pp. 605–612

STUDY ON THE SYSTEM DEVELOPMENT FOR PORT LOGISTICS SYSTEM DIAGNOSTICS

Young-Tae Park[1], Hyun-Sik Kim[2] and Gyusung Cho[3,*]

[1]Division of International Trade and Distribution
Dongeui University
176, Eomgwangno, Busan jin-gu, Busan 47340, Korea
gregory@deu.ac.kr

[2]School of Mechanical Engineering
[3]Department of Port Logistics System
Tongmyong University
428, Sinseon-ro, Nam-gu, Busan 48520, Korea
hyunskim@tu.ac.kr; *Corresponding author: gscho@tu.ac.kr

Received December 2018; accepted March 2019

Abstract. *A variety of security policies have been enacted on a national level in South Korea; however, investments in security have been lacking due to ineffective legal punishments. Furthermore, South Korea has not created a complete logistics security system that integrates and manages the entire logistics sector. Even though the port logistics information system is a key national information system, there has been insufficient research on diagnosing information security vulnerabilities. As such, in this study research on the development of a vulnerability diagnostics system that automatically performs a series of information security activities such as asset management, vulnerability diagnosis, vulnerability analysis, and action planning for information assets that exist in a port logistics information system was conducted. In addition, this study also proposes a port logistics diagnostics system operating plan for the efficient development of automatic diagnostics scripts using the operating system of servers for a vulnerability diagnosis system, integrated operating platform, and diagnostics system of a port logistics information system.*

Keywords: Port logistics, Logistics information, Diagnostics system, System development

1. **Introduction.** The development of information technology has changed our society into a knowledge and information society, and because of this, knowledge and information can be shared anywhere in the world through the Internet or a similar means [1,2]. As such, the development and sharing of information technology have created an opportunity to transform each country into an information society. As a result, the growth of information technology has created more opportunities to invest for strengthening the competitiveness in information systems of enterprises [3,4]. Currently, many companies are developing a variety of information systems and exerting a great deal of effort to improve their information capabilities, but they have shown insufficient effort and necessary awareness with regard to protecting the important information that is used in these information systems both internally and externally. Port logistics information systems rapidly collect various data and information about the movement of goods in and out of ports, manage the storage and processing of this information, and provide timely relevant information to the users [5-7]. If a security problem occurs at a port container terminal and the terminal operation stops, an unprecedented situation may occur in which the country's imports and exports are paralyzed, so information security in the port logistics industry is as

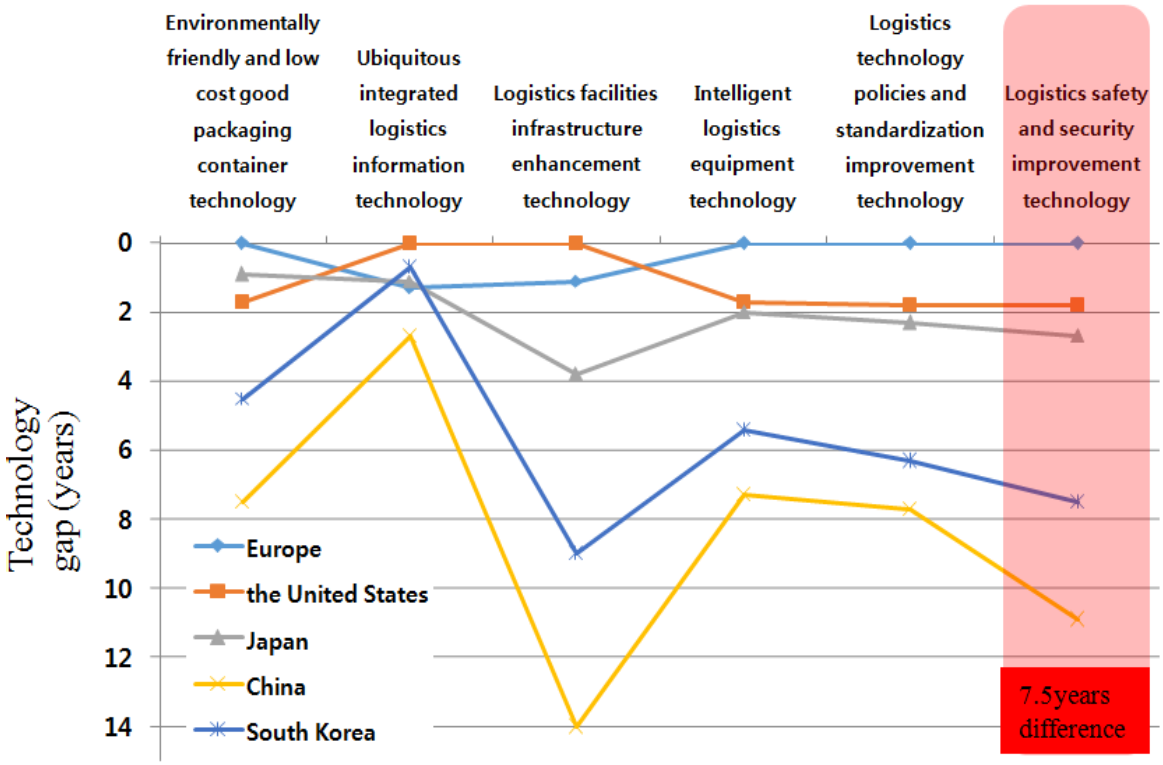
DOI: 10.24507/icicelb.10.07.605

important as it is in any industry. However, current port container terminals are built and operated with a focus on physical security, and the effort put into implementing software-based information security management for port logistics information systems is relatively insufficient. In this study, research was conducted on the development of a vulnerability diagnostics system that automatically performs a series of information security activities such as asset management, vulnerability diagnostics, vulnerability analysis, and action planning for information assets that exist in a port logistics information system in the delivery and delivery of the agent system and inside-servers. Web management of security objectives, entrance, guard, situation room, entrance area, arrange a little bit of patrolling and initial arrangements, gain the continuity of the day and night costs. Prientific security equals. Monitoring and monitoring systems are installed in the Security Situation Room, and 24-hour-monitoring system establishment. In the last security search item, install and operate detector for personal search, installation and utilization of equipment for possible products, operation of applications or biological response equipment, vehicle search for vehicle inspection.

2. **Special Characteristics of Port Logistics Information.** The port logistics information system aims extending a crosscutting concern analysis of the port container terminal center's operating system design by transmitting each piece of information for each class and executing the feedback [8-10]. Currently, port users around the world such as shipping companies and importer/exporters are able to make port usage applications such as ship arrivals and departure reports, goods delivery and sending reports, and port facilities usage reports mainly via the EDI (Electronic Data Interchange) method making reports through computers in VAN (Value Added Network) dedicated network. However, port logistics information systems are being built and operated to allow port usage reports to be made from any location in the world by port users if they have devices that can connect to the Internet. A port logistics system which is Port-MIS (Port Management Information System) is being operated in the Yeongnam, Honam, Gyeongin, and Yeongdong management areas, centered on SP-IDC (Shipping & Port Internet Data Center). Civil petitioners process their various civil complaint tasks using Port-MIS, which is built into SP-IDC, and task managers use the Port-MIS for each management area to process acceptance or approval tasks related to the civil complaint reports [11]. The purpose of Port-MIS is to make port management operations efficient and support policy decisions for scientific port management. For port users, the integrated information system that is installed and operated by the port authority to provide convenience can be considered as the most widely known system. However, there still have been no efforts or technology developments related to information security that consider the specific characteristics of the port logistics field. As shown in Figure 1, there is a more than 7-year gap between South Korea's level of logistics security technology and that of other advanced nations. The government has been enacting policies related to security, but investments in security have been lacking due to light legal punishments, and South Korea has not created a complete logistics security system that integrates and manages the entire logistics sector.

Furthermore, as insufficient systems for information security in the port logistics sector in South Korea exist, the enactment of relevant national laws is currently being reviewed with a focus on specific sectors such as information communications networks.

3. **Hardware Development for Vulnerability Diagnostics System of Port Logistics Information.** As part of this study, it is a research for the development of an operating system which can diagnose port logistics information vulnerabilities, and the hardware systems presented in this study were classified as internal devices and external devices as they were developed.



Source: Current technology levels according to the Korea Institute of S&T Evaluation and Planning National R&D Technology Industry Information Service (NTIS)

FIGURE 1. Current technology status related to port logistics security in South Korea

3.1. **Internal device and external device implementation.** The vulnerability diagnostics hardware system was implemented based on Open Source Hardware (OSHW). OSHW publicly releases the circuit schematic diagrams, related instructions, printed circuit board diagrams, etc., that are used in a variety of hardware, so that anybody can develop the same good or goods that use the public hardware. In OSHW, specific hardware designs are publicly released so that anybody can use them to learn the hardware manufacturing methods, and at the same time, permission is given to modify, distribute, or manufacture the designs. It is possible for anyone to manufacture a totally new form of connected device according to changes in the user's form of operation. Arduino, which was created in Italy in 2005 and is responsible for physical inspections, is currently the most famous and widely used OSHW platform. In the system developed for this study, development tools and circuit schematic diagrams, etc., can be provided in an open source form so that users who have no experience with embedded development can easily use them. Arduino is a microcontroller board with low specifications using an 8-bit AVR CPU; however, this device has been developed so that various sensors for measuring light, temperature, humidity, etc., are easily connected to various actuators such as speakers, LEDs, and motors, as it is equipped with several digital pins and analog pins that can be used by sensors and actuators. In addition, it can combine accessories such as LCD screens, USB adapters, or "shields", which are communication link modules for GSM, wi-fi, Ethernet, etc., and supports a variety of operating systems such as Windows, Mac OS, and Linux. Table 2 shows the major functions of the internal devices and external devices developed in this study.

The internal device performs the role of distinguishing the necessary data from each agent and corresponding port operations information and collecting the basic data that

Table 1. Major legislation related to information security

Category	Legislation name
Safe use of information communications networks and information systems	Framework Act on National Informatization, Act on the Protection of Information and Communications Infrastructure, Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc., Electronic Government Act, Digital Signature Act, National Cyber Security Management Regulation, etc.
Punishment for violations	Act on the Protection of Information and Communications Infrastructure, Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc., Electronic Trade Facilitation Act, criminal code, etc.
Prevention of international theft of state secrets and vital information	Military Secret Protection Act, security operations regulations, military criminal law, Act on Transfer of Technology and Promotion of Commercialization, Act on Promotion of Public-Private Partnership Technology Business, etc.
Creation of information security conditions	Information Protection Industry Promotion Act, Act on the Protection of Information and Communications Infrastructure, National Cyber Security Management Regulation, etc.
Personal information protection	Act on the Protection of Personal Information, Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc., Use and Protection of Credit Information Act, etc.

Source: National Information Security White Paper, National Intelligence Service, 2016.

Table 2. Major functions of internal devices and external devices

Category	Description	Function
Internal device	This provides an independent console and operates independently within a closed network.	- Equipped with Analysis console - One-way outgoing encrypted transmission is available to a specified external device
External device	This communicates with internal devices from the external of a closed network and provides console function.	- Receipt of one-way incoming encrypted communications is available with the specified internal device due to the equipped analysis console.

were diagnosed by the agent. In communication fields, it continuously acts as the connection between the operation network and external networks, and blocks unauthorized access attempts that occur via the external network. The agent is installed in the relevant information system, taking account of the operation environment and operating system that is appropriate for the characteristics of a port logistics information system to perform a normal diagnosis. It is implemented to transmit the diagnostics logs for each piece of information to the internal device. In this study, the port logistics information vulnerability diagnosis performed by the internal devices and external devices is conducted. The software performs the vulnerability analysis based on the agent, receives each piece of information from the internal device, and analyzes the diagnostics results. In the hardware part, the system is operated to collect various diagnostics results that occur in the port logistics information system and to perform logical network separation by installing the

internal and external devices. Communication between closed networks in the port logistics information system and external networks is implemented so that information from the internal device is encrypted and transmitted to the external device via the developed software and hardware system. In the external network, this information becomes the basis for analysis that can be used in the port logistics information system's diagnostics results, which become the basis for risk analysis and finding improvements. The port logistics information vulnerability diagnostics hardware system considered in this study was developed so that the information system had an independent network section that was distinct from the network being operated and a connection with an external network can be available. The hardware system is configured so that communication with the information system is controlled by a Raspberry Pi and communication with physical environment measurement sensors and other devices is performed by the Arduino. Both the internal device and external device were developed using a Raspberry Pi as shown above, and the internal device operates independently within the closed network. A virtual environment system was built to evaluate the vulnerability diagnostics system developed in this study.

3.2. **Analysis console development.** In this study, the analysis console system was developed to perform the functions of receiving the values measured by the agent and providing analysis results. It provides the number of registered information systems, safety index averages, etc., via the logistics information system's status report so that the operator can understand the overall status of the information system. In addition, it provides the status of assets according to information system type in the "Asset List", and it provides asset registration and safety indexes according to each information system. The "Diagnostics Results Report" provides the status of whether there is a vulnerability and the vulnerable point action plan for each control item. It was implemented so that reports could be automatically generated through automatic diagnostics scripts for each server operating system so that the user can easily see the diagnostics results as shown in Figure 2.

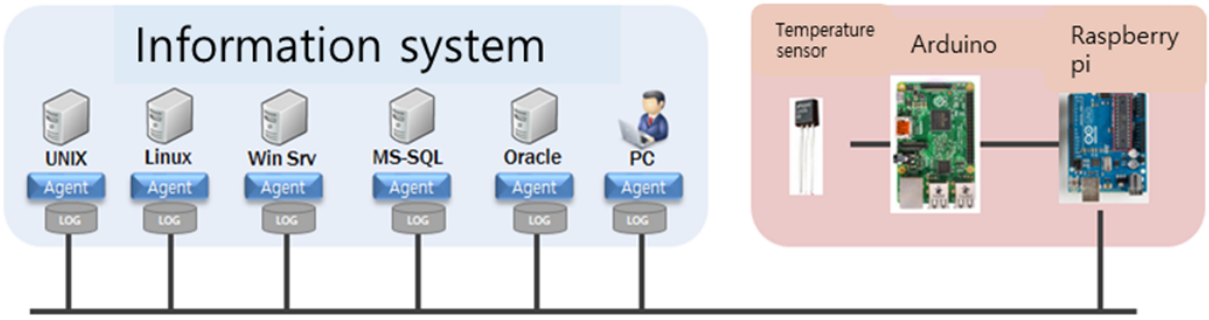


FIGURE 2. Analysis console implementation

3.3. **Performance analysis of vulnerability diagnostics hardware system.** Using the vulnerability diagnostics hardware system developed in this study, the diagnostics results received from each host in the port logistics information system were combined to calculate the current risk, as shown in Figure 3.

The internal device received the transmitted results, added up the received content, and presented it to the console screen as shown in Figure 4.

It was found that when the developed system performed diagnostics in a Windows Server environment, it completed the diagnostics within 10 min, the average time being 5 min and 58 s, as shown in Figure 5.

Area	Diagnostic statistics				Diagnosis Results		
	Overall	Protected	Vulnerable	N/A	Overall Score	Evaluation score	Security level
Account Management	90	89	1	-	780	8	99.0%
Service Management	180	168	2	10	1,600	20	98.8%
Patch Management	10	10	-	-	100	-	100.0%
Log Management	25	24	1	-	210	6	97.1%
Security Management	100	87	3	10	800	26	96.8%
DB Management	5	-	-	5	-	-	N/A
Total	410	378	7	25	3,490	60	98.3%

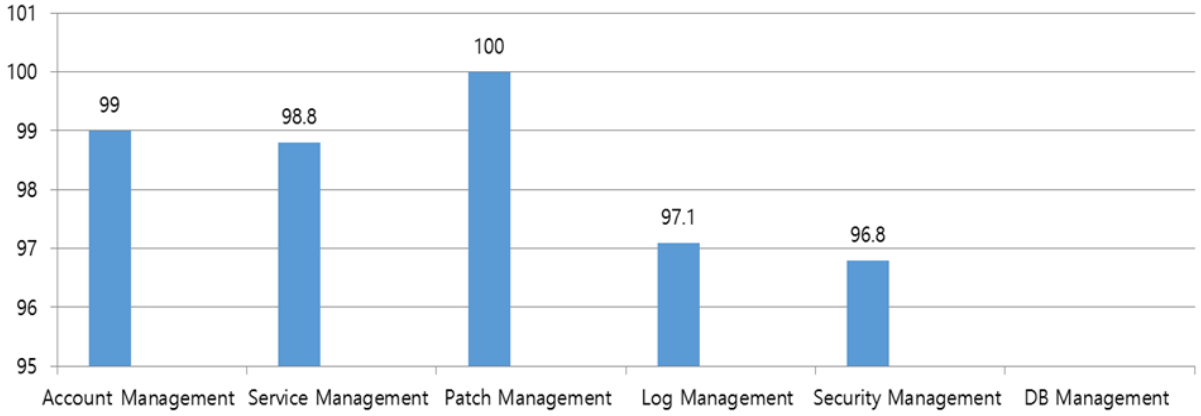


FIGURE 3. Results report provided by the internal device

Host Name	Operating system	Model	IP	Asset Name	Total	Protected	Vulnerable	N/A	Security level	Measurement date	Importance
Use-pacweb 1	Windows Srv 2008 Standard	Hi-Ware HW	192.168.1.20	Internal linkage	82	76	1	5	98.6%	2017-04-06 01:30	2.3.2

FIGURE 4. Vulnerability diagnostics system execution report

4. **Conclusions.** The development and operation of systems for port logistics safety and security can not only advance the port logistics industry to a more systematic and efficient state, but can also become a factor that increases international competitiveness. Particularly in a country like South Korea where dependence on trade via importing and exporting is high, promoting and supporting the port logistics industry is important; however, systematic management of port logistics information has still not been implemented, and the relevant systems require continued development. Therefore, this study has developed an operation system that can diagnose and resolve port logistics information vulnerabilities. The developed system periodically diagnoses vulnerabilities in the server and DBMS, transmits the diagnostics results to an agent that performs analyses. It has implemented functions for logically separating networks during emergencies and storing diagnostics results in order to respond to various disruptions. This is expected to reduce the vulnerabilities in port logistics information systems and consequently strengthen robustness against cyber-attacks and reduce system disruptions due to mistakes and gross negligence by information systems operators. It also makes it possible to continuously monitor the inevitable vulnerabilities that must be accommodated due to the characteristics of application programs and legacy systems. Because it is possible to handle sustained

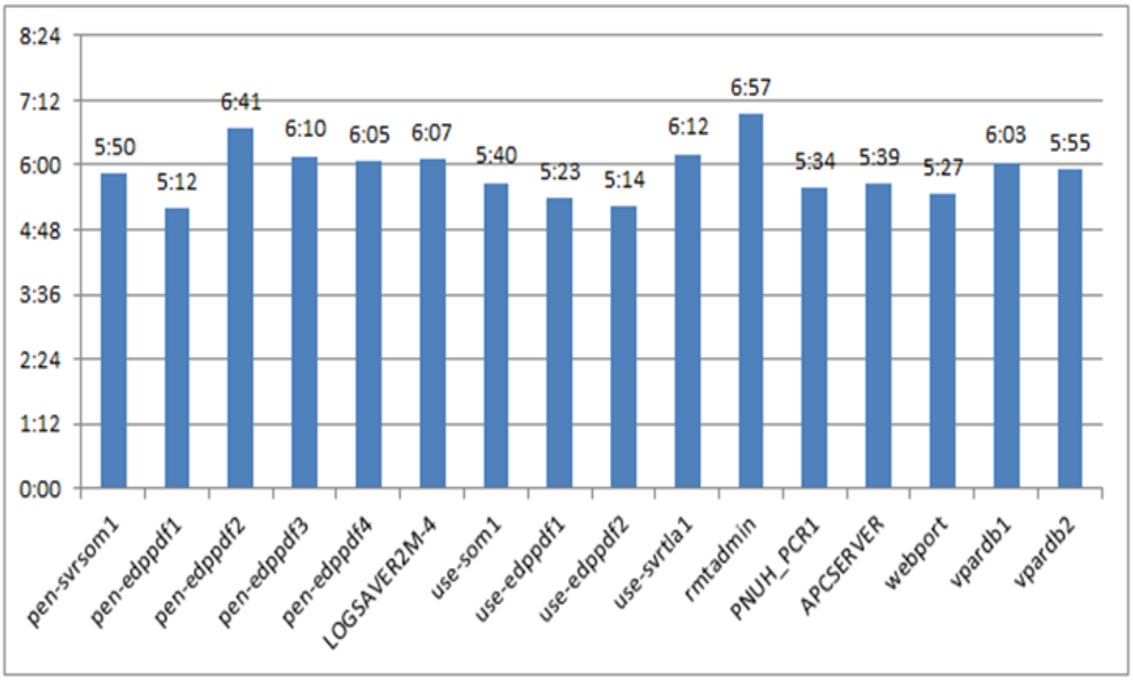


FIGURE 5. Example of diagnostics execution results in a Windows Server system

external attacks, the competitiveness of South Korea can be strengthened by improving the country's port logistics industry capacity and increasing its international standing through an uninterrupted port logistics service. The number of items will be increased by drawing more emphasis on the vulnerability diagnosis item, and the current system will be implemented around diagnosis and monitoring, but will increase maturity as a step of remote action. In addition, it is going to install a function that can statistically derive particular occurrence based on accumulated data on installed environment by installing learning functions such as Deep Learning.

Acknowledgment. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2018R1D1A1B070 44856) and the Tongmyong University Research Grants 2018 (2018A005-1).

REFERENCES

[1] J. M. Bae, S. J. Ko and C. S. Lee, Example of building a global logistics service cost management system through BPR, *International Management Review*, vol.22, no.1, pp.135-164, 2018.

[2] C. S. Lee, Environmental uncertainty, logistics information systems and organizational structures having an impact on logistics performance, *Internet E-Commerce Research*, vol.16, no.4, pp.247-271, 2016.

[3] S. I. Lee, K. Y. Ryu, M. S. Shin and G. S. Cho, Function and service pattern analysis for facilitating the reconfiguration of collaboration systems, *Computers & Industrial Engineering*, vol.62, no.3, pp.794-800, 2012.

[4] G. S. Cho, A simulation modeling approach method focused on the refrigerated warehouses using design of experiment, *IOP Conference Series: Materials Science and Engineering*, vol.229, pp.1-6, 2017.

[5] G. Cho, H. S. Kim and M. Kim, Development of refrigerated warehouses logistics system based on the ISMS, *ICIC Express Letters, Part B: Applications*, vol.8, no.3, pp.633-638, 2017.

[6] S. Michael, Integrating unmanned vehicles in port security operations: An introductory analysis and first applicable frameworks, *Ocean Yearbook Online*, vol.32, no.1, pp.556-583, 2018.

[7] Y. G. Mun, G. G. Park, D. H. Lee and H. H. Yoon, Development of power-driven RFID tag for intelligent logistics tracking system, *Korean Institute of Communication Sciences*, 2015.

[8] H. S. Kim and G. Cho, Study on advanced performance estimation of heterogeneous collaborative network for maritime domain awareness, *ICIC Express Letters, Part B: Applications*, vol.8, no.3, pp.525-530, 2017.
[9] G. S. Cho and H. G. Kim, A method for simulation design of refrigerated warehouses using aspect-oriented modeling approach, *International Journal of Industrial Engineering*, vol.20, no.12, pp.24-35, 2013.
[10] H. S. Oh, Smart factory logistics management system using bluetooth beacon based on indoor location tracking technology, *Journal of the Korean Institute of Information Scientists and Engineers*, vol.19, no.11, pp.2677-2682, 2015.
[11] Korea Association of Marine Industry, *A Study on the Activation Plan for the Hinterland of Busan New Port in the Era of Global Logistics*, 2015.