Journal of Engineering and Applied Sciences 14 (Special Issue 1): 3938-3941, 2019
ISSN: 1816-949X

Security Enhancement for IoT Information System Connected with 5G

Hyeong-Do Im and Dea-Woo Park
Department of Convergence Science Technology, Hoseo Graduate School of Venture, Asan, Korea

Abstract: Recently, high-speed, high-quality real-time service platforms are changing due to the development of ICT (Information and Communication Technology) convergence technologies such as IoT (Internet of Things) and blockchain based on 5G (5 Generation) mobile communication. As the communication system is expanded to 5G, the technology and services of the 4th Industrial Revolution are reflected by the expansion to cyber system connected with IoT. However, the methods and technologies that can be dealt with are still insufficient. In this study, we study security extension analysis of information system. ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27001 analysis, 5G mobile communication security analysis, IoT security analysis, service vulnerability monitoring and minimization of external network exposure. In particular, IoT-based services utilize the default account to study home router DDoS (Distributed Denial of Service) attack, smart home appliance malicious code attack, malicious code infection due to vehicle IP exposure and 0-day attack on OS (Operating System) and firmware. The research of this study will be the basic data to counter the cybersecurity threat to the IoT system connected with the new 5G.

Key words: 5G, IoT, ISMS, security audit, information security, system

INTRODUCTION

The technology of ICBM (Internet of things, Cloud, Big data, Mobile) which is important technology of present value creation is rapidly developing. In addition, according to changes in important 5G communication, IoT, AI (Artificial Intelligence), AR (Augmented Reality) and VR (Virtual Reality) technology and service environment that will lead the fourth industrial revolution, It affects people's lives and is reflected in the cyber world connected with the real world. With the progress of the fourth business revolution technology, the service platform including 5G expansion, IoT expansion and information system expansion are evolving into high-speed and high-quality service converged in the real world due to rapid intelligent revolution and technology improvement. In this 'smart environment', cybersecurity threats are expected due to new types of services such as IoT system connected with 5G communication which is the basic infrastructure, due to expansion of related technologies. Actual security threats are caused by cybersecurity incidents. Therefore, the government and major private companies utilize security management audit criteria through ISMS (Information Security Management System) and ISO 27001 regulations. Recently, the expansion of 5G and IoT dramatically increases the integrity and security but the aspect.

In this study, we propose a part that needs to be improved for securing security through system expansion through 5G, IoT, security analysis of information system. ISO/IEC 27001 analysis, 5G mobile communication security analysis, IoT security analysis, service vulnerability monitoring and minimization of external network exposure (Jeong, 2015). Especially, IoT-based service researches home router DDoS attack, smart home appliance malicious code attack, malicious code infection by vehicle IP exposure, ROOT authorization by unauthorized access, zero-day attack on OS and firmware. This research will be the basis for securing the security (confidentiality, integrity, availability, non-repudiation, certification, etc.,) according to the expansion of the cyber system in the future.

Literature review

5G mobile communication: As shown in Table 1, the first generation of mobile communication systems in Korea started in 1988, followed by the third generation, 4G LTE-A (long term evolution-advanced), in 2006 and 5G, a 5th generation mobile network, in 2020 (Kim *et al*., 2017). The core services of 5G mobile communications are to implement four key technologies: 1000 times faster transmission speed, 1000 times less response time, 1000 times more device acceptance technology and 1000 times more energy efficiency (Park, 2015). Currently, Korea's 5G

Corresponding Author: Dea-Woo Park, Department of Convergence Science Technology, Hoseo Graduate School of Venture, Asan, Korea

Table 1: 5G development and domestic commercialization

Division	Core services	Domestic commercialization
1st generation	Voice	1988 year
2nd generation	SMS (short message)	1996 year
3rd generation	Data+Video call+USIM	2006 year
4th generation	High speed video+Network game	2011 year
5th generation	Realistic media+Intelligent service	After 2020

Table 2: IoT information system security requirements (ITU-T)

Division	Contents
General	
Device	Establish access rights, authentication, device integrity verification, access control, data confidentiality and integrity verification
Network	Establishing and authenticating access rights, ensuring confidentiality and integrity of data and signals
Service	Establishing access rights, authentication, data confidentiality, integrity, privacy assurance, performing security audits, anti-virus installation
Additional	Apply security requirements applicable to special situations such as mobile payment

status and activities plan to commercialize 5G Fixed Wireless Access (FWA) network in 2017 and actively promote various global cooperation for 5G standardization and service technology expansion.

IoT information system: The three major technologies used in the IoT are sensing technology that obtains information from objects of type and environment, wired/wireless communication and network infrastructure technology that supports things to connect to the internet and various service fields and forms and service interface technology that fuses various technologies for processing and processing information. The development of IoT information system technology accelerates computing power and networking in all things and devices and serves as a catalyst for creating a convergent smart ICT environment. According to the dissertation of Master's degree by Han (2015), the effect of IoT in everyday life is getting bigger and it is argued that security review is needed to create a fused smart ict environment. In particular as many intelligent terminals are connected to the internet and expanding into two-way communication environments, security breaches increase. Therefore as shown in Table 2, the security requirements presented by the International Telecommunications Union-Telecommunication (ITU-T) are generally divided into devices, networks, services and additions as follows (Kim, 2016).

Expansion of security analysis of information systems

ISO/IEC 27001 analysis: ISO/IEC 27001 is used to regulate requirements for documenting, establishing and implementing information security management systems as well as security management regulations and certification screening criteria according to the needs of individual organizations. ISO/IEC 27002 is an implementation guideline for information security management and can only be used as a reference item for each control item rather than an audit. According to the Kim (2012) Master's thesis, to establish security management items through ISMS and IT audits including ISO 27001. ISO/IEC 27001 (ISMS) is a five-step process for establishing and operating an information security management system (establishment of information protection policy, scope of information protection management system, risk management, implementation and follow-up), documentation, control and records control. Information security measures should be structured and implemented in accordance with the characteristics and environment of the organization and systematically managed, maintained and implemented. However, ISO/IEC 27001 has been revised to 2.0. However, similar to domestic K-ISMS, institutional benefits and effective aspects are lacking. Therefore, the government and private corporations have chosen the security supervision as the second choice but the security supervision and information protection activities are limited to the degree of correcting and correcting the problems through the establishment of the information security. Figure 1 compares the domains of ISO/IEC 27001: 2005 and ISO/IEC27001:2013.

5G mobile communication security analysis: The focus is on the pin-tech industry which combines finance and technology using Information and Communication Technology (ICT) and the wireless communications sector has greatly improved convenience and security. In recent mobile communication environments, mobile services are being implemented in new forms of converged applications such as block chain technology. As a result of the transition to LTE 5G due to the stagnation of LTE after 3Q 2016, a variety of services have been tried in mobile environments where ICT technology has converged. However, quality assurance and security aspects due to communication and system expansion in terms of services experienced by the users are pointed out as the limit. Thus, the security threats to 5G communication and mobile communication applications as shown in Table 3 are based on the Top 10 mobile risks announced by the OWASP foundation, from mobile threat 1 unsafe data storage to mobile threat 10 sensitive information.

IoT security analysis: IoT services such as organic communication and network technology, IoT device control technology and applications including operating

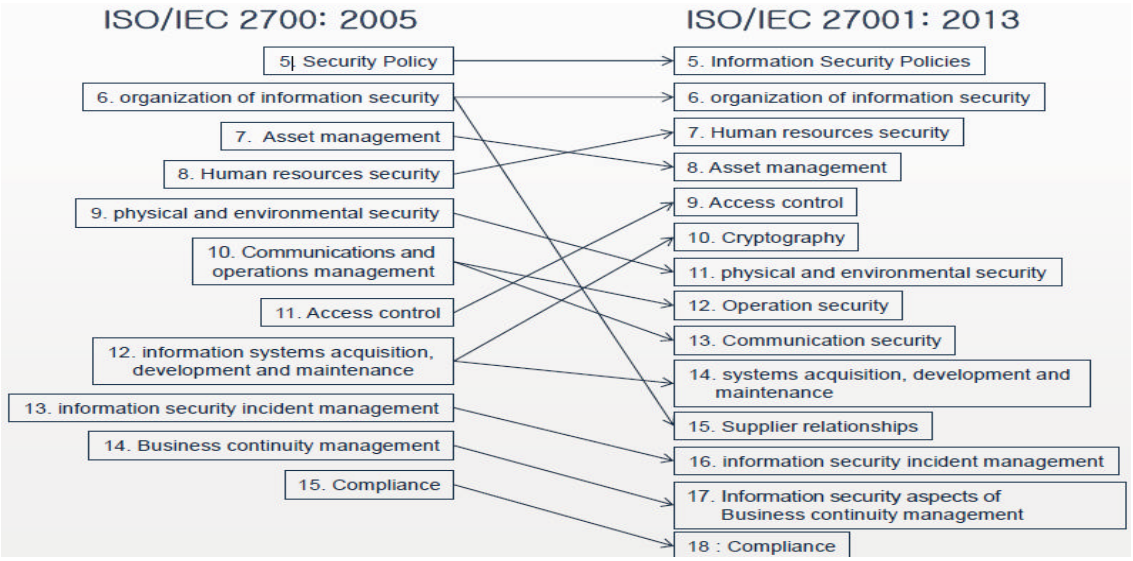

Fig. 1: Compare domains in ISO/IEC 27001:2005 and ISO/IEC27001:2013 (Kim, 2016)

Table 3: OWASP top 10 mobile risks

Variables	OWASP top 10 mobile risks
M1	Insecure data storage
M2	Weak server side controls
M3	Insufficient transport, layer protection
M4	Client side injection
M5	Poor authorization and authentication
M6	Improper session handling
M7	Security decisions via. untrusted inputs
M8	Side channel data leakage
M9	Broken cryptography
M10	Sensitive Information

system are implemented in various technologies. However, due to the development of ICT technology, IoT convergence service is experiencing big and small privacy invasion and property loss including security threat including system error, data forgery, authentication obstruction, DB confidentiality and integrity damage, personal information infringement. A variety of complex devices have been introduced, including wearable devices which utilize the miniaturization and low power of the device throughout IoT. However, security technology is not applied to handsets and management, measures and countermeasure technologies for continuous security enhancement such as service vulnerability monitoring and minimization of exposure of devices and external networks are very weak reality. The network sector connected to IoT also needs to be prepared to cope with new security threats by referring to cases of accidents such as packet sniffing, spoofing, hijacking, illegal APs as a normal AP and collecting personal information.

Security enhancement plan of information systems confidentiality, integrity, availability, non-repudiation, authentication enhancement of information cyber systems: It is divided into the information construction process considering the complexity of the information system and the post-development operation and maintenance. Inspection items are classified into three categories: policy compliance, management organization, human resources security, operational security, development and maintenance, information security incident management, physical environment security, application control, communication and operation management, access control, it is based on the results of detailed configuration of authentication and rights management, harmful software control, network security, encryption, security setting and log management, technical vulnerability management, software security patch update, etc.

5G mobile communication security enhancement: 5G mobile communications refers to the OWASP Top10 mobile risk category to determine security through insecure data storage, weak server-side controls, lack of transport layer protection, client-side injection, incorrect authentication and authentication, inappropriate session handling. The details of mobile communication security are examined through the detailed check items to expand mobile communication security based on the details such as data leakage, side channel data leakage, broken encryption and sensitive information leakage. Regardless of the various smartphone platforms, this focuses on risk areas throughout the mobile telecommunication expansion rather than individual vulnerabilities and establishes plans based on the results.

IoT security enhancement: In case of IoT service, various IoT devices are included and IoT security examination is performed on healthcare services closely related to life in

terms of inspection efficiency. IoT device (terminal), application/firmware, service platform, product design and production, operation management. The target is set as a sensor terminal for healthcare device components, a device ID, a platform for managing user accounts and a device terminal. The check items are checked through items such as authentication and authorization management, whether encryption is used, network security, security settings and log management, application/firmware management, technical security, device error handling and security measures are established based on the results. It exploits vulnerability in various ways such as DDoS attack of home router, smart home appliance malicious code attack, malicious code infection by vehicle IP exposure, ROOT right gain by unauthorized access, 0-day attack on OS and firmware in IoT-based service and to prepare for thorough response from new security threats.

CONCLUSION

The 5G, IoT and system aspects are very difficult to guarantee security because the various requirements are identified from the user's point of view and the expansion of the platform and devices that make up the service evolve dramatically. In particular, there is a growing need for securing security through the convergence of ICBM which is a key technology for creating value. If you overlook this environment, you could cause a huge loss of property and damage to users. In this study, we examined the various types of threats related to the security enhancement of IoT and information systems connected with 5G. To minimize these threats and to enhance stable operation and efficient service in the future, we reviewed the security extension and strengthened the security architecture against expansion of each component. The improvement of security system of information system is required due to 4th industrial revolution technology development such as 5G extension, IoT extension and ICBM.

RECOMMENDATION

Future research will need to develop and apply a security assurance model for 5G, IoT and information system security and operational management.

REFERENCES

Han, J.J., 2015. The IoT security architecture and checklists study for IoT security review. Masters Thesis, Graduate School of Information Financial Information Privacy and Security, Yonsei University, Seoul, South Korea.

Jeong, S.H., 2015. A study on the implementation of healthcare technology using 5th generation mobile communication technology and wearable devices in hyper-connectivity era. Masters Thesis, Graduate School of Convergence Engineering, Korea Dankook University, Yongin, South Korea.

Kim, D.H., 2016. A study on the establishment of cybersecurity governance in the converged. PhD Thesis, Graduate School of Information Security, Korea University, Seoul, South Korea.

Kim, H.J., Y.S. Park, S.G. Ryu, G.E. Lee and S.J. Lee *et al.*, 2017. Koreas development strategy through 5G network global status analysis. J. Convergence Culture Technol., 3: 43-48.

Kim, Y.M., 2012. A study of the information systems audit techniques for enhancing security. Masters Thesis, Graduate School of Information Communication, Korea Konkuk University, Seoul, South Korea.

Park, S.H., 2015. Domestic 5G mobile communication technology development prospect and policy issue. Korea Sci. Technol. Inf. Res., 1: 34-41.