ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 66, No. 12, pp. 1879~1888, 2017
http://doi.org/10.5370/KIEE.2017.66.12.1879

IoT 제품의 안전 관리를 위한 기술 및 정책적 사후 보안관리 프레임워크

Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management

이 동 혁* · 박 남 제†
Donghyeok Lee · Namje Park

Abstract - The Internet of Things (IoT) environment has been gradually approaching reality, and although it provides great convenience, security threats are increasing accordingly. For the IoT environment to settle safely, careful consideration of information security is necessary. Although many security measures in the design and development stages of IoT products have been studied thus far, apart from them, the establishment of systems and countermeasures for post management after the launch of IoT products is also very important. In the present paper, a technical and policy post-security management framework is proposed to provide secure IoT environments. The proposed framework defines the concrete response procedures of individual entities such as users, manufacturers, and competent authorities in the case of the occurrence of security flaws after launching IoT products, and performs appropriate measures such as software updates and recalls based on an assessment of the risk of security flaws.

Key Words : Security Management Framework, Electrical Safety Management, IoT, Internet of Things, Security Management

1. Introduction

The importance of IoT environments has been greatly magnified recently, and interest in them is high, to the extent that many related products have been actually launched. IoT environments provide great convenience by combining physical environments with the existing IT environments. Therefore, users can enjoy more convenient and comfortable lives through IoT environments[1,2]. However, IoT security should be essentially considered for the IoT environment. At present, although the IoT environment is being actualized, measures for IoT security are not complete. Since the IoT environment may bring about direct physical and material damage that is different from that of the existing IT environment, policy and technical considerations for security are essential.

In the present paper, a security framework that focuses on the post-management of IoT products is proposed to provide such secure IoT environments. Currently, many studies for security are conducted in the design and development stages of IoT products, [3] [4] and safer IoT products can be designed and developed based on these studies. However, the security flaws of IoT products already launched or new security vulnerabilities that may be found after product launching even in products that met security fidelity cannot be certainly known.

In the case of IT software, even if security vulnerabilities are exposed, there will be no problem if the security vulnerabilities are treated with software updates. However, IoT products are characterized by the fact that whether they can be updated or not cannot be identified with certainty. In particular, due to the nature of IoT products, if hardware defects in the products occur, such problems cannot be solved by software updates only and should be solved institutionally with recalls and other necessary measures. Even in cases where a software update is possible, the time to fabricate update patches is required, and the relevant IoT product will operate in an unstable state at least during that time. These characteristics are adding to security threats in the IoT environment. In the present paper, an IoT product post-security management framework is proposed that will enable the maintenance of security of products centered on the time

† Corresponding Author : Dept. of Computer Education, Teachers College, Jeju National University, Korea.
E-mail: namjepark@jejunu.ac.kr
* Elementary Education Research Institute, Dept. of Computer Education, Jeju National University, Korea .
Received : September 29, 2017; Accepted : November 14, 2017

of post-management after the launch of an IoT product according to the security characteristics of IoT environments as such.

2. Related Work

2.1 Necessity of IoT information protection

The importance of information protection cannot be overstated. Thus far, there have been many information protection threats, and the ones that may appear in the existing IT environment can be applied to and occur as they are in the IoT environment[5,6]. That is, various security threats that interfere with the use and provision of normal services by infringing on confidentiality, integrity and availability, the "CIA triad" which can be said to be the three key elements of information security, may appear[7]. In addition, it is expected that not only existing security vulnerabilities, but also various new security vulnerabilities, will appear in the IoT environment. That is, the security accidents occurring in the IoT environment seem to be much larger than existing ones. The IoT environment is characterized by the fact that IT and physical environments are combined, and in this respect, security issues are directly related to physical and material threats[8].

As the various security threats in major IoT areas (home/home electronic appliances, medical, transportation, energy, and manufacturing) are emerging as such, proper post-management systems are necessary so that IoT products and services can cope with security threats in advance. Since IoT products and services have problems, such difficulties or the occurrence of high costs in ex post facto security measures such as maintenance and the application of security updates after production, sales, and development, technological after-sales policies necessary for post-product management and security maintenance are required.

2.2 Trend of IoT security-related studies

2.2.1 GSMA IoT Security Guidelines

In February 2016, the GSMA (Global System for Mobile Telecommunication) released the GSMA IoT Security Guidelines, which are public guidelines for business operators developing new IoT products and services. The major targets are companies and organizations that are planning to develop IoT services, manufacturers that provide IoT devices to support IoT services for IoT service providers, developers who are developing IoT services on behalf of IoT service providers, and business operators that provide network communication services for the provision of IoT services. The purpose of these guidelines is to enable the IoT industry to establish a common understanding of IoT security issues. The guidelines present a methodology for developing secure services to ensure that security best practices are implemented throughout the life cycle of IoT services. In addition, these guidelines provide various recommendations on how to reduce common security threats and vulnerabilities[9].

The GSMA Guidelines consist of four detailed guidelines, as shown in Figure 1. These include CLP.11, a basic guide for the development of safe products for developers of IoT technologies and services, CLP.12 to assess all components of IoT products or services in terms of the service ecosystem, IoT CLP.13 for evaluating the components of IoT services from the point of view of IoT endpoint devices, and finally, CLP.14 for ensuring system security and data privacy for network operators that provide network communication services for providing IoT services.

Fig. 1 GSMA IoT Guidelines Document Structure

2.2.2 OTA IoT Trust Framework

The Online Trust Alliance (OTA) is a nonprofit U.S. Internal Revenue Code No. 501(c)(3) organization that promotes innovation and vitality of the Internet. Here, the IoT Trustworthy Working Group (ITWG) is composed of many vendor-neutral stakeholders in a workgroup established by the OTA in January 2015. Thereafter, the OTA has announced the IoT Trust Framework, which focuses on home automation and connected home products, and wearable technologies for the fields of health and fitness. The full version, released on March 3, 2016, specifies 30 requirements and recommendations.

2.2.3 OWASP Internet of Things Project

The OWASP (The Open Web Application Security Project) Internet of Things Project is one of the OWASP's projects and aims to support security reviews for users in the construction / deployment / evaluation of IoT technology. The "Top 10 IoT Vulnerabilities" summarized by the OWASP

in 2014 sets forth 10 points at which vulnerabilities are likely to occur in the IoT and concretely defines in detail attackers' attack methods, security vulnerabilities, technical impacts, and business impacts. It explains vulnerabilities and attacks with actual examples, and provides guidelines for solving problems.

3. Proposal for Post-Management Framework

3.1 Threats and countermeasures for IoT product post management

3.1.1 Possibility of occurrence of new vulnerabilities after shipment

Even if no security vulnerabilities were found during IoT product testing prior to shipment, new security vulnerabilities may be found afterward. That is, in situations where the product has already been released to the market and the relevant devices are used by many users, if a new security vulnerability is disclosed to many and unspecified persons, all the IoT product users may become the targets of hackers, and such cases may lead to serious problems. However, no institutional countermeasure for such cases has been prepared at present. Although KISA (Korea Internet & Security Agency) currently has a system to reward reporting of new software vulnerabilities, since it is a system that give a reward to the reporter who found a software vulnerability, has no institutional coerciveness and is not actually appropriate for the characteristics of IoT products, it has limitations in that IoT device manufacturers cannot be forced to take immediate action when a security vulnerability has been found in a product. Therefore, an institutional system to force IoT device manufacturers to immediately respond to new vulnerabilities is indispensable.

3.1.2 Ambiguity on department responsible for IoT security accidents

It is not clear which department is fully responsible for IoT product security accidents. This is attributable to the fact that IoT products have the nature of both physical and IT environments at the same time. That is, when a security flaw in an IoT product has occurred, the responsible department may vary depending on the influence of the security flaw. Examples include cases where personal information may be exposed by the hacking to IoT devices, and cases where physical property losses may occur due to the malfunction of IoT smart door lock devices. In these two kinds of cases, although the essence per systems from the security flaws of the IoT device, the form of actual damage due to the relevant flaw varies. In particular, in the case of hacking that causes operations leading to battery fires, etc. or malfunctions of IoT medical devices that would have a fatal influence on human bodies, the flaw should be handled with immediate recalls and the department responsible for product recalls should be responsible for such cases. Policy systems for such cases are not yet clear.

3.1.3 Absence of a system for user recognition of product security flaws

In cases where any security flaw has occurred in an IoT product, continuous use of the product may cause big problems. In particular, if the software cannot be updated immediately, the user will use the IoT device as it is without being aware of the relevant security flaw. That is, a system is necessary that will enable the users of IoT devices to concretely recognize any security flaw when one has occurred, and in particular, the range and kinds of infringement by the relevant security flaw. The user should be enabled to concretely recognize whether a security flaw is minor or a somewhat serious one, such as one that may lead to the exposure of some personal information, and judge whether to immediately stop the use of the product.

3.1.4 Security threats during software updates

If the security vulnerability of a product can be resolved by a software update, it should be made immediately. However, there may be various security threats during software updates. Representative cases include ones where an update file in an inappropriate state is distributed due to the loss of integrity of the update software. In addition, illegal software may be distributed as a result of the malicious intervention of a hacker and modulation attacks may occur in the process of communication.

Above all, installing software after identifying integrity and reliability is most important, and such conditions should be institutionally managed, but no such system has been established yet.

3.1.5 Countermeasures according to threatening elements

The possibility of the occurrence of new security vulnerabilities after product shipment should be always kept in mind and should be continuously monitored to find any vulnerabilities that may occur. That is, a system to monitor and find security vulnerabilities is necessary to take actions

in advance before hackers conduct malicious acts using security vulnerabilities.

In addition, when an IoT security accident has occurred, the responsible department should be clearly determined according to the seriousness and degree of influence of the relevant infringement incident. That is, KISA's Korea Computer Emergency Response Team (KrCERT) will judge the degree of influence using risk analysis. If the seriousness of the situation of the relevant product is minor, the accident can be handled by a recommendation to the manufacturer to correct the problem with a software update, and if the situation involves the exposure of serious security threats, the accident should be handled with a corrective order. On the other hand, if it is difficult to update the software immediately and the device per se malfunctions, causing property/physical problems for the user, the accident should be submitted to the Korea Product Safety Association as a recall accident. The Association may issue a recall recommendation or recall order depending on the severity of the property/physical damage of the product. In addition, in cases where a security flaw has occurred, the user may continue to use the relevant product without being aware of the security flaw. Therefore, a system should be established to enable the user to promptly recognize security flaws. Meanwhile, with regard to security threats during software updates, technical software update systems are being established. The KrCERT judges whether software update files are suitable and reliable and notifies whether IoT device software should be updated t so that the updates can be performed.

Table 1 Security Threats in Post Management and Countermeasures

Security threats in post management	Countermeasure
Occurrence of new vulnerabilities after shipment	Establishment of systems that will enable monitoring of vulnerabilities to take action in advance
Ambiguity of the department responsible for security accidents when they occur	Clarify the department responsible for security accidents depending on the severity and degree of influence

3.2 Proposed Post-management framework

3.2.1 Overview of the framework

Fig. 2 shows the post-management framework for IoT security proposed in this paper. In the framework, users of IoT products, manufacturers of IoT devices, and private and public joint IoT security monitoring groups organically interact to report security flaws in current IoT products, and the competent department receives the reports and judges the processing procedure to handle the flaws with appropriate methods. The handling methods can be software updates, corrective recommendation/orders, or recalls, depending on the severity of the situation, or whether the product can be updated or immediate action can be taken.

3.2.2 Private and public joint IoT security monitoring group

In the present paper, the organization of a group tentatively called a private and public joint IoT security monitoring group will be proposed. This group will be composed of private and public IoT security monitoring group members with the capability to analyze IoT security to play the role of analyzing IoT security vulnerabilities at all times. The group will be composed of citizens with diverse experiences in IoT products and the ability to analyze the IoT security field, experts from academia with expertise in IoT security, experts from enterprises with the ability to analyze hacking and cope with infringement, related government departments, and responsible agencies. Citizens check for product flaws from the viewpoint of users, and the experts from academia and enterprises judge the concrete causes of flaws and the range of influence in relevant cases. The government and agency monitoring group members request cooperation from national/public organizations for the analysis of major security flaw cases.

When an IoT security flaw has been found, the IoT security monitoring group reports the content of the flaw to the competent department, which receives the reports, checks the security flaw, and promotes the finding of new IoT security with rewards.

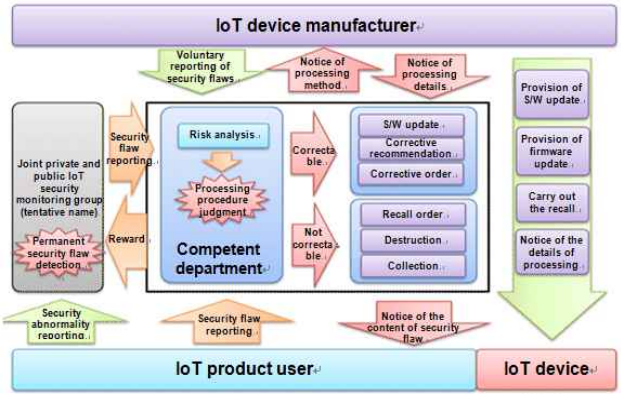

Fig. 2 Post-Security Management Framework

3.2.3 IoT device manufacturer

IoT device manufacturers are responsible for the security flaws of IoT devices. Even if IoT devices pass security flaw tests when quality is inspected, security problems that were not known can be found at any time after the devices are released. Therefore, when any such problem has been found in their products, the manufacturers should voluntarily report the fact to the competent department. Then, the manufacturers should update software and notify the details of processing after completing it.

3.2.4 IoT product user

When any sign of a security problem has been found while an IoT product is used, the user should ask the private and public joint IoT security monitoring group to check it. Meanwhile, if a security flaw is clearly identified by the user, they should report it directly to the competent department, which notifies the IoT device manufacturer of the security flaw and issues a corrective recommendation or orders corrective action. The manufacturer then provides a software update for the IoT device so that security is maintained.

3.2.5 Competent department

The competent department receives reports on IoT security flaws from IoT product users, IoT security monitoring groups, and IoT device manufacturers at all times and analyzes the risks of the relevant problems in the reports to judge how the problems should be handled. The handling methods include immediate correction by the manufacturers with software updates in some cases and the issuance of corrective recommendations or orders according to the severity of the issues so that the manufacturers can take security measures in cases where immediate correction is not easy. Meanwhile, the contents of the security flaws and details of handling are notified to the IoT product users. In cases where correction is not possible, actions such as recall orders, destruction, and collection of products are taken. In cases where the severity of the security flaw of the product is very high, that is, if the user is expected to suffer property or material damage due to an IoT product, the user is recommended to immediately destroy the product, which is then collected by the manufacturer to undergo appropriate procedures such as recalls.

3.3 Policy details

3.3.1 Preparation of vulnerability countermeasure reports

If a new vulnerability has been found in an IoT product, a vulnerability countermeasure report should be written. The report should clearly state the vulnerability, overview, severity, range of influence, anticipated countermeasures against the influence, etc.

When a software (or firmware) security vulnerability has occurred, a general countermeasure is to provide updated software that resolves the vulnerability and recommend the user to apply the update. However, if it is judged that the user cannot immediately apply the update because the provision of the update software takes time, another solution should be prepared immediately. For example, there may be a way to disable certain functions of the product so that the product is not affected by the vulnerability.

3.3.2 Notice to users of the contents of flaws

Vulnerability-related information should immediately be notified to IoT users after it has been prepared. However, before the foregoing, the risk of misuse of the information should be considered. Attention should be paid to the fact that the level of information disclosure should be properly adjusted because it may lead to the exposure of the information to hackers.

In addition, if update software that can be applied to a product is being provided, the users should be recommended to immediately install the software. However, there may be cases where products are used by those who are unfamiliar with IT technology or the update software cannot be easily applied by users. In such cases, the automatic application of the software by remote operation should be considered. Information on the automatic update function should be set forth appropriately in a user manual when the product is shipped so that users can easily understand it. If any function of the product is changed by the update, it should be avoided for as long as possible, and should be applied after the user has agreed to it.

3.3.3 Recall procedures and current issues

In cases where update software cannot be immediately applied to products or a hardware vulnerability has occurred, a recall may have to be carried out depending on the field of the IoT product. In such cases, procedures to collect the product first and carry out update maintenance work are necessary.

Current recalls are based on the Framework Act on Product Safety. Article 5.4 of the Enforcement Decree of the Framework Act on Product Safety specifies major defects as “defects that may cause any death, physical injury, disease, fire, or explosion.” At present, the major grounds for recall

orders of the Korean Agency for Technology and Standards follow the range of the "major defects" specified in Article 5.4 of the Enforcement Decree of the Framework Act on Product Safety. However, one point to note here is that there is no clear legal system for IoT security flaws.

Of course, IoT products per se can sufficiently cause physical and material damage to the user depending on the seriousness of the security flaws of the products. However, issues related to IoT product recalls are that although those parts of IoT products that may directly cause damage to users can be relatively clearly known, those parts that may indirectly cause damage to users cannot be clearly determined. Therefore, IoT security flaw-related details should be concretely specified in the relevant enforcement decree for application.

3.4 Technical issues and countermeasures

Software updates are one of the parts of IoT product post-management that can be regarded as very important in terms of technical aspects. In this section, technical approaches to software updates are discussed and detailed procedures are proposed.

3.4.1 Algorithm selection in advance

In the process of distributing a software update file, it may be tampered with by a hacker attack. Therefore, a file completely different from the one provided by the manufacturer may be delivered to the user. Such problems can cause great security risks. In particular, many of the current IoT products are not designed with a high level of security, and quite a few IoT products are exposed to security threats.

To clearly identify software update files, integrity techniques should first be applied to prevent the forgery problems that can occur in the process of distribution. The present paper proposes to use MAC (Message Authentication Code) as a technical management method in the update file distribution/installation/configuration stages. The difference between MAC and modulation detection code (MDC) is the fact that MAC enables the identification of the integrity of the original message and the source of the message. However, MAC has a shortcoming in that, in order to have such a function, the key should be shared between the sender and recipient in advance. In the case of MDC, hash functions cryptographically corresponding to the original messages are used to ensure the integrity of original messages. However, message senders cannot be identified. In addition, MDC has a shortcoming in that it should be transmitted through safe channels without fail.

Table 2 Fault simulation results

	MDC	MAC
Channel exposure safety	X	O
Sender authentication	X	O
Provision of non-repudiation	X	X
Message integrity	O	O

Table 3 Analysis of Lightweight Encryption Algorithm[11]

Name	ARIA	LEA	HEIGHT
Division	Symmetric key	Symmetric key	Symmetric key
Key length	128 bits	128 bits	64 bits
Structure	Involutional Substitution-Permutation Network	ARX-based Generalized Feistel Network (GFN)	Generalized Feistel transformation structure
Security	Low	High	Low
Security threat	Vulnerable to sub-channel attacks		

Given the update situation for IoT products, MAC is more suitable than MDC because MAC enables the identification of the sources of relevant messages so that when an attack by a hacker has occurred, whether or not MAC has been generated by a legitimate user can be identified. Meanwhile, an ultra-light encryption technology suitable for IoT products is required. [10] Because of the characteristics of IoT devices, encryption/decryption technologies suitable for low power should be applied. Currently, various lightweight encryption technologies have been developed, as shown in the following table. The vulnerable element of sub-channel attacks, which is a threatening element of such algorithms, must be solved.

3.4.2 Procedure for automatic software updates

There are generally two software update methods: manual and automatic. Manual updates are those performed by the user. However, as there are too many devices for which updates should be managed in the IoT environment, it is not desirable for the user to manually update all IoT devices. Therefore, for the security of IoT products, technical measures for real-time automatic updates are necessary.

The abbreviations for the description of the automatic software update procedure proposed in this paper are as shown in Table 5.

Table 4 Abbreviations

Abbreviation	Description
PkgID	Software update package ID
UptID	IDs managed by the update server
VerID	Version ID generated by KrCERT
Data	Actual software update file
H(·)	SHA-1 based hash of a certain value

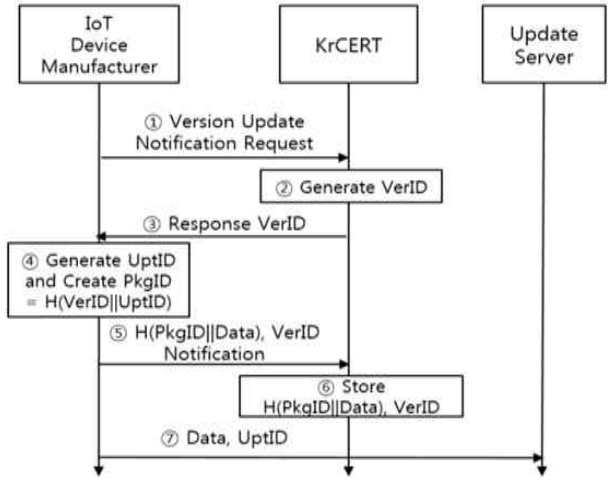

Fig. 3 Software Automatic Update File Registration

In the automatic update process, the loss of the integrity of the update software, malicious changes by hackers in the software being distributed, or forgery attacks in the communication process may occur. Therefore, in the present paper, an automatic update procedure that can prevent problems in the update process is proposed, as shown in Fig. 3 and Fig. 4, as a method to maintain the latest security module. In this case, for secure communication, the communication and security modules between the two devices must have the same latest version, in principle. Accordingly, procedures for updating the software between the two devices to communicate with each other are defined in detail.

Fig. 3 shows the steps for the IoT device manufacturer to register the software in the update server in advance for automatic software updates. The detailed procedure is as follows:

① The IoT device manufacturer informs KrCERT that a new version of the software update is required.
② KrCERT generates an arbitrary VerID, which will be used for mutual authentication with IoT devices.
③ KrCERT informs the VerID to the IoT device manufacturer.
④ The IoT device manufacturer generates an arbitrary UptID and generates a PkgID value through H (VerID ‖ UptID) based on the relevant value.
⑤ The IoT device manufacturer transmits the H (PkgID ‖ Data) value and VerID value to KrCERT.
⑥ KrCERT stores the received values as a pair.
⑦ The IoT device manufacturer transmits the actual update file and the UptID to the update server, and the update server keeps the relevant values as a pair.

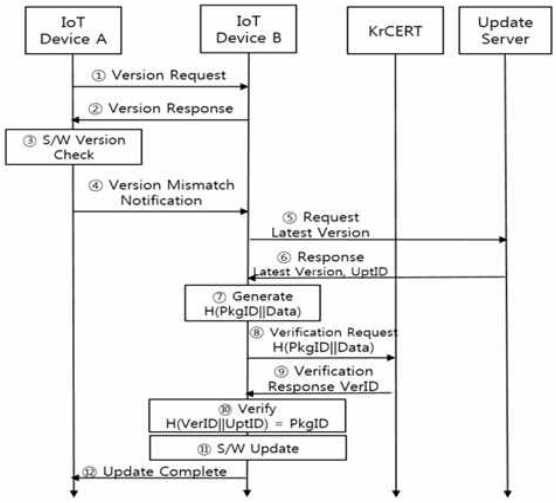

Fig. 4 Software automatic update protocol

Fig. 4 defines a detailed protocol for updating the software into the newest software for communication between the actual IoT devices A and B when the software auto update registration has been completed. The proposed automatic update protocol is as follows.

① IoT device A requests device B for the software version.
② Device B returns the software version.
③ Device A checks the software version. Here, assuming that the software version of the device B is lower and it was identified that an update is required:
④ Device A notifies device B of software version discrepancy.
⑤ Device B requests the latest version from the update server.
⑥ The update server returns to device B with the latest software file and the corresponding UptID.
⑦ Device B generates the H (PkgID ‖ Data) value obtained by hashing the supplied software file and the Pkg ID.
⑧ Device B requests KrCERT to validate the H (PkgID ‖ Data) value.
⑨ KrCERT checks the validity to confirm that there is no abnormality, and returns the fact that there is no abnormality and the VerID.
⑩ Device B judges whether the hash value and PkgID value of the UptID received as set forth under ⑥ and

the VerID received as set forth under ⑨ are identical.
⑪ Device B performs the software update.
⑫ Device B informs device A that the software update has been completed.

When the update method as such is applied, cases where software modulation attacks occur because a certain file in the update server has been damaged or hacking occurred in the update process can be prevented. Meanwhile, since a protocol was configured so that the reliability of the update server with KrCERT was based on the UptID value and VerID value in the present study, and thus the IoT device and KrCERT have a mutual authentication function, server impersonation attacks can be prevented. In addition, in cases where the update file has been changed into data different from the original through various paths such as hacking and packet loss, the hash value H (PkgID ‖ Data) corresponding to the update file will be changed. Since the relevant value is one kept by KrCERT in advance to check validity, and KrCERT compares the H (PkgID‖Data) value and PkgID value generated by the relevant IoT device and delivered to KrCERT with the values registered in advance to judge whether they are identical and informs the IoT device whether the values are suitable, the IoT device can check the reliability of the relevant update file to safely perform the automatic update.

4. Implications

Many security guidelines and frameworks for IoT are currently being proposed. The GSMA guidelines mentioned earlier were written primarily for business operators and developers who provide IoT services. That is, the major targets of the security guidelines and frameworks for IoT are business operators such as enterprises and organizations that plan to develop IoT services, and as major contents, security recommendations for the product design and development stages as methods to reduce security threats and vulnerabilities during IoT product manufacturing are provided. Meanwhile, the OTA IoT Trust Framework focuses on connected home, health, and wearable technologies and provides essential security recommendations for the relevant areas as 30 principles. In addition, the guidelines provided by the OWASP Internet of Things Project provide 10 points where vulnerabilities can easily occur in IoT and mainly describe how to solve related problems.

However, the contents provided by the GSMA, OTA and OWASP commonly mention ways to reduce the vulnerability to security threats during IoT product manufacturing, but do not mention in detail post-management threats and how to deal with problems that may occur. In addition, all three guidelines are characterized by the fact that they mainly deal with technical parts and do not separately mention policy and institutional parts.

That is, most of the IoT-related guidelines published thus far have limitations in that they focus on technical parts. As the IoT environment is spreading rapidly now, policy and institutional discussions to cope with IoT security threats are urgent and indispensable.

The proposed framework focuses on the post management of IoT products and summarizes the overall post-security management of IoT security threats, such as the omnidirectional detection of security threats to IoT products, update / recall policies, and the establishment of IoT security monitoring groups. In this respect, the proposed framework is different from the security guidelines mentioned above. Currently, each department has a framework to deal with risks, but a system for post-security management has not yet been established. In this respect, the present paper concretely established and presented an IoT post-security management system.

5. Conclusion

Although the IoT environment provides great convenience to users, the resultant security threats are also great. Although there are not so many IoT security hacking cases in Korea yet, such threats will gradually increase if various IoT devices such as connected cars are introduced in the future. In addition, although proactive measures are more important for security than anything else, due to the nature of IoT products, post-security management systems should be prepared for products already released and security threats that may occur later. Therefore, in this paper, a post-security management framework for the IoT environment was proposed. This framework is characterized by the fact that it enables IoT product users, manufacturers, and IoT security monitoring groups to cooperate to jointly discover IoT security threats and take appropriate measures when threats have been found.

To this end, the importance of IoT security, actual security breach cases, and IoT security guidelines that have been studied up until recently were examined in Chapter 2. In Chapter 3, a proposed security framework was presented, and in Chapter 4, the implications of the framework were analyzed in comparison with guidelines already proposed. The IoT environment will gradually progress to the settlement stage, and thorough security measures are urgently needed in

relation to it. Since the importance of security in IoT cannot be overemphasized, continuous studies on policy / technical IoT security systems seem to be necessary hereafter too.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2016R1D1A3A03918513).

References

[1] Sungmin Rue, "Survey on the Platform of IoT and Big Data", Korea Institute of Information Technology Magazine, Vol. 13, No. 2, pp. 19-25, Dec. 2015.

[2] Jun Jong Am, Kim Nae Soo, Park Jeong Kil, Park Tae Jun, and Kang Ho Yong, "IoT device products and technology trends", The Journal of The Korean Institute of Communication Sciences, Vol. 31, No. 4, pp. 44-52, Mar. 2014.

[3] Hyun Jung La, Chun Woo Park, and Soo Dong Kim, "A Framework for Effectively Managing Dynamism of IoT Devices", Journal of KISS : Software and Applications Vol. 41, No. 8, pp. 545-556, Aug. 2014.

[4] Kang Nam Hee, "Standard Technology Trends for Internet Security of Things", The Journal of The Korean Institute of Communication Sciences, Vol. 31, No. 9, pp. 40-45, Aug. 2014.

[5] Babar, Sachin, et al., "Proposed security model and threat taxonomy for the Internet of Things (IoT)", In International Conference on Network Security and Applications, pp. 420-429, Jul. 2010.

[6] Zhou, Liang and Han-Chieh Chao, "Multimedia traffic security architecture for the internet of things", IEEE Network 25.3, 2011.

[7] Kang Nam Hee, "Things Internet Convergence Services Security Requirements", The Journal of The Korean Institute of Communication Sciences, Vol. 32, No. 12, pp. 45-50, Nov. 2015.

[8] Kim Dong Hee, Yun Seok Woong, and Lee Yong Pil, "Security for IoT services", The Journal of The Korean Institute of Communication Sciences, Vol. 30, No. 8, pp. 53-59, Jul. 2013.

[9] Park N and Kang N, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle", Sensors, Vol. 16, No. 1, pp. 1-16, 2016.

[10] Kim Seon-Tae, Lim Chae-Deok, Jung Hee-Bum, and Han Dong-Won, "Trend on Lightweight IoT Device Platforms", Korea Institute of Information Technology Magazine, Vol. 13, No. 2, pp. 1-8, Dec. 2015.

[11] Nam-Uk Lee, Seung-Su Yang, Jae-Sung Shim, and Seok-Cheon Park, "Comparative Analysis of Low Power and Lightweight Encryption Algorithm for IoT Security", Proceedings of Korean Society For Internet Information Conference, Vol. 17, No. 2, pp. 249-250, Nov. 2016.

[12] Donghyeok Lee, and Namje Park, "Geocasting- based synchronization of Almanac on the maritime cloud for distributed smart surveillance." The Journal of Supercomputing, Vol. 73, No. 3, Feb. 2016.

[13] Donghyeok Lee, and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 6, Dec. 2016.

[14] Lee D, Park N, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", Personal and Ubiquitous Computing. DOI 101007/s00779-017-1017-1, 2017.

[15] Park N, Hu H, Jin Q, et al., "Security and privacy mechanisms for sensor middleware and application in internet of things (IoT)", Int J Distrib Sens Netw, Article 2965438, 2016.

[16] Park N and Bang H-C, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Security Communication Network, Vol. 9, No. 6, pp. 500-512, 2016.

저 자 소 개

Donghyeok Lee

Mr. Lee received the BSc degree in information industry from dongguk university, Korea, and received his M.S. degrees in E.C.T from dongguk university in 2007, respectively. He is a researcher, STS research center at jeju national university since 2015. Prior to joining the researcher at jeju univ., he had worked as a researcher at KT co. ltd.

for 7 year. And he had an appointment as the researcher of the information security research division of the Electronics and Telecommunication Research Institute for 1 year. He has many talks related in information security technologies, cloud security.

Namje Park

Dr. Part received the BSc degree in information industry from Dongguk University, Korea in 2000, and received his M.E., and Ph.D. degrees in Information Engineering from Sungkyunkwan University in 2003, and 2008 respectively. He is a Professor of Department of Computer Education in Teachers College at Jeju National University since 2010. He has been serving as a Research Scientist of Arizona State University since 2010. Prior to joining the researcher at ASU, he had worked as a post-doc at University of California, Los Angeles for 1 year. And he had an appointment as the senior engineer of the information security research division of the Electronics and Telecommunication Research Institute for 6 years. He is concerned in the information security technology field for the mobile environments, IoT system, Smart Grid, Mobile XML Security, Web Services Security, Ubiquitous computing including RFID/WSN and a variety of cryptographic technologies. He has many talks related in mobile and information security technologies, computer education.