International Journal of Innovative Research in Technology & Science
ISSN: 2321-1156 Volume VII, Issue IV, July 2019

THE DESIGN CONSIDERATIONS FOR SECURITY ANALYZING TECHNOLOGY IN EKM SYSTEM OF IOT

Eun Young Choi, Korea Internet & Security Agency; Haeryong Park, Korea Internet & Security Agency

Abstract

The Internet of Things (IoT) is high world-wide, and developments of various technologies to establish the IoT environment have been ongoing. In particular, massive IoT devices will be in our midst because the 5G technology that the world is paying attention to is about to be realized. Hence, security technologies should be introduced to secure safety for the IoT environment since it c

an be the target of hacking or cyber intrusion. The encryption technology can be applied to security, and encryption key management is crucial since the core of the encryption technology is the safety of the encryption key. In this paper, we review the security vulnerability of IoT and recommendation/standard related to the encryption key. Then, we propose the factors to be considered in relation to the design of the technology to analyze the safety of efficient IoT EKM(Encryption Key Management) needed to construct a safe IoT environment.

I. Introduction

According to Gartner, the number of IoT devices excluding PC, tablet, and smartphone is expected to reach 20.8 billion by 2020 due to the development of smart IoT such as self-driving and smart factory [1]. As a complex object composed of a wide range of technologies and protocols, the IoT environment has an organic relationship wherein the IoT sensors/devices, gateways, middleware platforms, service platforms, and IoT services are interlinked and interactive. Moreover, since all devices are connected to the Internet, they are exposed to risks such as information leak by unauthorized users and system damage; information leak in particular can lead to privacy violation.

Various security technologies such as data encryption and access control have already been applied to enhance security for implementing safe Internet-based services and infrastructure. Organizations like NIST and ISO/IEC have issued various recommendations (drafts) and standards related to implementing and managing the encryption key management system safely [7-10,14-16,18,19]. Enterprises are adopting not only the recommendations to enhance security but also the security certification system that analyzes the safety of IT and certifies it depending on whether it meets the certification criteria. Despite the recognition of the necessity of the technology to analyze the security vulnerability in the IoT environment, however, technology development is inadequate with regard to the safety of efficiency encryption key management in particular.

This paper is consisted as follows. In Section 2, we describe the security vulnerability in the IoT environment and review the technologies such as the encryption technology needed for security. In Section 3, we describe the recommendations/standard issued by NIST and ISO/IEC related to encryption key management and also survey the currently existing security certification systems. In Section 4, we propose the factors to be considered in relation to the design of the technology to analyze the safety of efficient IoT encryption key management needed to construct a safe IoT environment. Finally, we conclude in Section 5.

II. Security Vulnerability and Response Technology in IoT

In this section, we describe security vulnerability and response technology in the IoT environment.

2.1 Security vulnerability of IoT

The IoT environment has not only physical components but also a wide range of technical factors such as communication/network technology, data mining technology, and service interface technology. Therefore, various security vulnerabilities can exist in areas where components are connected. Moreover, new security vulnerabilities can arise in each component given the connection to security vulnerabilities that are not present. In Table 1, we check the security vulnerabilities and attack types that occur widely in the IT sector. Although the same vulnerabilities in the existing IT environment are also present in the IoT environment, it is difficult to cope with such security vulnerabilities [23].

2.2 Technology to cope with IoT security vulnerability

In this section, we review measures to solve the privacy problems and security vulnerabilities in the device, protocol, platform, and service sectors as the technologies for coping with the IoT security vulnerabilities mentioned above.

2.2.1 Privacy protection technology

In a typical IT environment, there are various privacy protection measures such as cryptographic techniques and access control and permission control techniques. Cryptographic techniques include encryption of the database, confidentiality of information during IoT, and encryption key management technique needed for the techniques. Moreover, access control and permission control can minimize the privacy infringement of information through the role-based access control

technique or attribute-based access control technology that authenticates and approves according to the permission in the IoT component or service.

Table 1. Security Vulnerabilities and Attack Types in IoT

Security Vulnerabilities and Attack Types	Attack Targets in the IoT Environment
Worm and virus	IoT communication/network, device, gateway, platform, and application service
DoS/distributed DoS	IoT communication network
Unauthorized access	IoT device, gateway, platform, and application service
System OS not patched/OS security vulnerability	IoT device, gateway, platform, and application service
Inappropriate use of antivirus software	IoT platform and application service
Inappropriate use of firewall	IoT communication/network
Unauthorized service access	IoT application service
Protocol security vulnerability	IoT communication/network
Access by unauthorized user	IoT application service
Cloning attack	IoT device and gateway
Unauthorized I/O access	IoT device, gateway, platform, and application service
Inappropriate system log record	IoT platform and application service
Configuration error	IoT device, gateway, platform, and application service
Confidentiality/Integrity attack	IoT communication/network, device, gateway, platform, and application service
Unsafe password	IoT application service
Unprotected firmware	IoT device and gateway
Privacy infringement	IoT platform and application service

2.2.2 Light security and authentication technology in devices

Confidentiality, integrity, and authentication between devices are necessary for the communication between devices for IoT device security. In the existing PC/server environment, encryption technologies such as AES [6] and SHA-2 [13] can support confidentiality, integrity, and authentication. Note, however, that there is a limit in applying the existing encryption system in the IoT environment because of the calculation, storage, and communication capability owing to the low power and lightweight characteristics of IoT devices.

Light encryption systems such as PRESENT [3] and LEA [11] have recently been introduced to reflect such environmental factors. Wi-Fi [22], ZigBee [24], DASH-7 [7], and Bluetooth [2] are the device communication technologies that are applicable in IoT environments.

o Wi-Fi : It provides data integrity through data confidentiality and MAC with WPA (Wi-Fi Protected Access). It mostly uses AES-CCMP (AEC-Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) to provide confidentiality and integrity by generating the encryption and integrity check code using the counter mode and CBC mode.

o ZigBee : The communication protocol using the physical layer and data link layer of 802.15.4 supports confidentiality and integrity by using the AES-CCM version, which extends the AES-CCM defined in 802.15.4.

o DASH-7 : It defines the mutual authentication protocol and frame protection technique using various encryption algorithms and describes the method of using the key distributed in advance for mutual authentication and public key such as AES, SHA, RSA, and ECC.

o Bluetooth : The Bluetooth specification has evolved through the first-generation BR (Basic Rate), second-generation EDR (Enhanced Data Rate), third-generation HS (High Speed), and 4.0 LE (Low Energy) as the most recent one. The first and second generations use the stream cipher called E0 for encryption and the E1 algorithm based on SAFER+ encryption during the authentication process.

2.2.3 IoT Platform/Service security technology

Unlike the existing PC/server environment, the IoT platform must consider the communication among many nodes and node clustering problems as security matters. It must provide a safe security platform among all devices that can communicate with a specific platform. In addition, it must make sure that there are no safety problems while allowing users to use services anytime, anywhere through safe ID management and web service security such as CoAP [21] and DTLS [20] from the service aspect.

III. Analysis of recommendation/standard and security certification scheme related to EKM

In this section, we first analyze the standard and recommendation related to EKM(Encryption Key Management) in the IT environment by ISO/IEC and NIST. And then, we review the currently existing security certification systems.

3.1 ISO/IEC standard encryption key in each step

The ISO/IEC 11770 standard is organized into Parts 1 through 6, and 11770-1 [9] classifies the encryption key into three states: Pending-Active, Active, and Post-Active. The Pending-Active step refers to the state wherein the key is generated but not used right away, the Active step means the state wherein the key is generated and used for data encryption or

decryption, and the Post-Active step pertains to the key used only for decryption or validation.

3.2 EKM steps recommended by NIST

The NIST SP 800-57[14,17,18] recommendation classifies the encryption keys according to type (symmetric, asymmetric cryptography, etc.) and purposes (data encryption, signature, etc.) and presents the key operation period according to type. It presents the key circulation cycle and defines the process in four phases according to the key state and state switch as follows.

o Operational Phase: The keys are not yet generated or enabled since the keying materials are not normally usable.

o Operational Phase: The keying materials are usable, and the keys are enabled for normal use. The keys can be used to protect the processes or the key and the process.

o Post-Operational phase: The keying materials are no longer used normally but are accessible. The keying materials are usable only in some situations, and the key is disabled or compromised.

o Destroyed Phase: The keys are no longer usable, and all records of their existence may have been deleted. Although the key is disabled or compromised, the key attributes (key name, type, and encryption cycle) may be available.

Also, the United States and European countries operate security certification schemes that define the criteria for the safety of the information protection systems that provide security functions such as confidentiality and integrity and guarantee the safety of the systems depending on whether they meet the criteria. They can be summarized as follows:

Table 2. CMVP Validation Criteria [12]

Inspection Item	Key Inspected Items
1. Encryption module statement	7
2. Encryption module port/interface	2
3. Role, service, and certification	18
4. Finite state model	2
5. Operating environment	14
6. Encryption key management	26
7. Self-test	21
8. Design guarantee	5
9. Other responses to attack	1
Total	96

(1) CMVP(Cryptographic Module Validation Program)

CMVP is the system for evaluating the cryptographic modules jointly developed by NIST (National Institute of Standards and Technology) in the United States and CSE (Communications Security Establishment) in Canada to validate the safety of cryptographic modules [25].

It assigns Levels 1-4 after the validation, and the validated modules are registered in the "List of Validated FIPS 140-2 Modules." As shown in Table 2, the inspection consists of 96 items in 9 areas. Since CMVP evaluates the actual security modules, it includes the security technology and symmetric key/hash-based authentication technology. Studies show that 70% of IoT devices transfer data over non-encrypted networks. Therefore, appropriate encryption technology is needed to protect IoT device objects, which in turn requires safety analysis technology.

(2) TCSEC (Trusted Computer System Evaluation Criteria)

TCSEC was adopted as the standard for the evaluation of information protection systems in the United States, becoming the role model for other evaluation criteria since it was the world's first security system evaluation criteria [27]. TCSEC has requirements in four categories to evaluate each security classification. The evaluated system must meet the requirement in each category to receive the security classification of D, C, B, or A.

The evaluation requirement of TCSEC consists of the security policy, responsibility, guarantee, and documentation. As shown in Table 3, TCSEC can classify the systems into four classes -- D, C, B, and A -- and they can be further segmented into D, C1, C2, B1, B2, B3, and A1. Class A means the highest security level, whereas class D means the lowest.

Table 3. Evaluation Criteria for Each Class of TCSEC

Classification	Description
D	Minimal protection
C1	Discretionary information protection
C2	Controlled access protection
B1	Labeled security
B2	Structured information protection
B3	Security domain
A1	Verified design

(3) ITSEC (Information Technology Security Evaluation criteria)

Although developed in the United States, ITSEC was used to evaluate the information protection systems in Europe [26]. Some European countries recognized the need for the criteria and method of evaluating information protection systems, and ITSEC was adopted as the standard in Europe. Unlike TCSEC, ITSEC sought to evaluate all information protection products with a single set of criteria. The developers can set the security functions considering the environments where the products are used or use the security functions defined by ITSEC or ZSIEC in Germany. The products are evaluated only in terms of the guarantee.

The evaluation criteria are based on the functions. The security policy states how the security system manages and protects the needed information, and the theoretical basis of the

product provides information on how the product fulfills the purpose of system security.

Like TCSEC, ITSEC can be characterized by assigning the weight factor for each security class. Moreover, it focused more on the environment than the technology or domain. It can additionally analyze the environment that can provide IoT device service to deduce the security certification items. Note, however, that the security certification has a limitation, i.e., there is no significant distinction in classes E1 through E6 as they have different weight factors only.

IV. Design Considerations for the technology for analyzing safe EKM

It is necessary to manage safely the encryption key, which plays an important role in the safety of the encryption algorithm. The factors to consider for the safety of the encryption key differ according to the state change such as generation and storage and use cycle. Organizations like ISO/IEC and NIST have already presented the criteria for encryption key management in IT environments, with the encryption key circulation cycle and state change to manage encryption keys defined as shown in Figure 1 based on them [5]. They can be summarized as follows:

1. Preparatory step to generate the encryption key (Pending-Active): The state for generating the key to share or the secret parameter

2. Step to use the encryption key for data encryption or decryption (Active): The step for sharing or distributing the generated key so that the same key is shared can include the storage process in the Pending Active and Active steps.

3. Step for no longer using the encryption key for decryption and validation (Post-Active): When renewing the expired key like the certificate, the process is switched to the preparatory key generation step so that a new key can be generated and used. It permanently disposes of keys that are no longer used. Based on the encryption key state transition and lifecycle, we define that the basic characteristics of the encryption key include the key type, key cycle, key storage, and key damage, and it is necessary to analyze each of them and to manage the key safely for each lifecycle step.

The encryption key analysis factors based on the basic characteristics of the encryption key can be summarized as follows:

o Key type : The key type can differ according to the algorithm and usage, and the suitable key length and related information must be selected to realize security strengthening according to the purpose and algorithm of the key.

o Key Cycle : It is determined differently according to the operating environment and whether the symmetric key or asymmetric key is used. The key cycle can be divided into the transmitter user agency that can apply the encryption method to the data and the receiver use period to process the protected information.

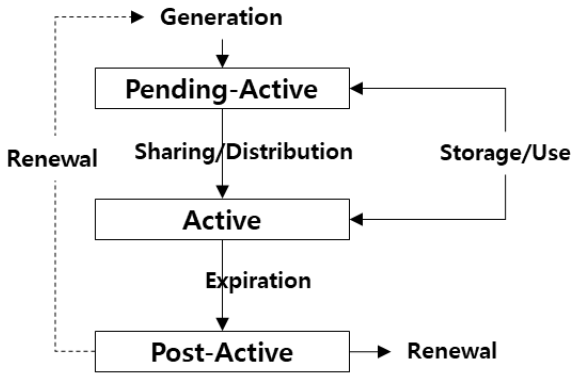

Figure 1. Encryption Key Life Cycle and State Transition [5]

o Key damage : Safety cannot be guaranteed when the key is damaged even if the safe encryption algorithm is used. The key must be disabled when it is damaged. In case of a need to continue processing the generated encryption statement or signature, the decision must be made considering the possible risks and the key management policy of the system.

Moreover, the factors for analyzing the encryption key management of each lifecycle step, in addition to the basic characteristics of the encryption key, can be summarized as follows:

o Key Generation : Since the encryption key is the critical safety factor for using the encryption algorithm, it must be generated in a safe manner. A random number generator must be used to ensure the cryptographic safety of the encryption key, and the generated key must be validated in terms of safety.

o Key Derivation : Key derivation refers to the generation of a new key using the shared secret value (encryption key, password, PIN, etc.). It is similar to key generation, and the encryption key must be derived safely since the secret value can affect the derived key.

o Key Injection : Key injection involves retrieving the key or random number safely generated outside when it is difficult for the object requiring the encryption key to generate the key or random number. It must validate whether the injected key or random number was generated safely and inject it into the object requiring such safely. The key or random number retrieved from outside must be injected in a safe manner, and

the random number must be deleted after key generation if a random number is injected to generate a key.

o Key Distribution : Key distribution means an object transferring the encryption key to other authenticated object(s). The distribution method depends on the key type (symmetric key or asymmetric key). The key distribution process must ensure confidentiality and integrity and validate that the key is distributed correctly.

o Key Agreement : Key agreement involves two or more mutually authenticated objects jointly generating the required key to share it. Since key sharing includes key generation, it is necessary to check if the key is generated in a safe manner and to validate the data exchanged between the objects since multiple objects are involved.

o Key Cancellation : Key cancellation means terminating the operation to stop using the key for various reasons (expiration of key cycle, key damage, etc.). When a key is canceled, its use must be terminated immediately; a canceled key must be neither reusable nor recoverable. In other words, an expired key must no longer be used.

Table 4. Safety Items that can be used for tooling

Type	Factor	Safety Items That Can Be Used for Tooling
Basic key characteristics	Key type	Key length and security strengthening of related information
	Key cycle	Comparison of key cycle for transmission and receipt
	Key damage	Reuse and deletion of damaged key
Actions for each lifecycle	Key generation	Use of safe random number generator
	Key derivation	Use of safe key derivation function
		Effect of damaged key on the derived key
	Key distribution	Validation of correct transmission
	Key agreement	Sharing of the key only with the authenticated object
	Key deletion	Zeroing or input of trash value after deletion

o Key Deletion : Deletion refers to deleting the key that is no longer needed for any purpose. It is necessary to delete the key permanently to prevent its use for unauthorized purposes, and the key information (purpose, cycle, etc.) must also be deleted. Moreover, a deleted key must be neither recoverable nor reusable.

In other words, the encryption key has two analysis factors in their basic characteristics and one in each lifecycle step, and safety analysis is possible by checking if the encryption key is safely generated and used for each factor. Some of these factors are included in the analysis criteria of CMVP in the United States as mentioned above, but the analysis is mostly performed manually; thus requiring a long time.

It is necessary to make the tool for the safety analysis factors that can be automated in order to develop the technology for analyzing the criteria efficiently. Table 4. Shows those that can be automated among the abovementioned factors for the analysis of encryption key management. Tooling the items that can be automated for the safety analysis of encryption key management can reduce the time to analyze safety and ensure accuracy.

V. Conclusion

In this paper, we reviewed the security vulnerabilities of IoT and the standards and recommendations for safe encryption key management. And we studied the characteristic of the encryption key and items that must be checked for each key management step and deduced the factors needed to analyze key management based on them. Moreover, we mentioned the matters that must be considered for efficient safety analysis technology based on these factors. This study is applicable to the technology for analyzing the safety of the encryption key in not only light IoT products but also server/PC environments. Its benefits include the reduction of time needed for the analysis.

Acknowledgments

This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00267, Development of Automatic Security Analysis Techniques for Lightweight Cryptographic Mechanisms)

References

[1] Gamter, Inc, http://www.gartner.com /newsroom/ id/3165317.
[2] Bluetooth, http://www.bluetooth.org.
[3] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher", CHES 07, pp. 405-466, 2007.
[4] K. Cameron, The Laws of Identity, http://www. Identtyblog.com/?page_id=354, May 2005.
[5] Eun Young Choi and Haeryong Park, " A study on Encryption Key Management Technology in a Light IoT Device Environment", IJIRTS 2017.
[6] J. Daemen, V. Rijmen, "AES proposal: Rijndael", NIST AES Proposal, 1998.
[7] DASH7 Alliance, http://www.dash7.org

[8] CRYPTREC, List Guide 2010(Key management), 2012.
[9] ISO/IEC 11770-1, Information technology-Security techniques-Key management, 2010.
[10] ISO/IEC 11770-3, Information technology-Security techniques-Key management-Part 3: Mechanisms using asymmetric techniques, 2015.
[11] National Security Research Institute,"LEA", 2013.
[12] NIST, FIPS 140-2, "Security Requirements for cryptographic modules, 2001.
[13] NIST, FIPS PUB 180-4 Secure Hash Standard, 2012.
[14] NIST SP 800-57, Recommendation for Key management- Part 1: General (Revision 3), 2012.
[15] NIST SP 800-130, Framework for Designing Cryptographic Key Management Systems, NIST, 2013.
[16] NISTIR 7628, Guidelines for Smart Grid Cybersecurity, NIST, 2014.
[17] NIST SP 800-57, Recommendation for Key management- Part 2: Best Practices for Key Management Organazation, MIST, 2016.
[18] NIST SP 800-57, Recommendation for Key management- Part 3: Application-Specific Key Management Guidance, NIST, 2017.
[19] OASIS, Key Management Interoperability Protocol Specification Version 1.2, 2015.
[20] E. Rescorla, N. Modadugu, "Datagram transport layer security", 2006.
[21] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol(coap)", 2013.
[22] Wi-Fi Alliance, http://www.wi-fi.org
[23] A. Wright, "Cyber security for the power grid: cyber security issues & Securing control systems", ACM CCS, Nov, 2009.
[24] ZigBee Alliance, http://www.zigbee.org
[25] CMVP, https://www.nist.gov/programs-projects/cryptographic-module-validation-program-cmvp
[26] ITSEC. "Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria" (PDF), 1991.
[27] TCSEC , Department of Defense Standard, Trusted Computer System Evaluation Criteria, 1985.

Biographies

EUNYOUNG CHOI received the B.S. degree in Mathematics from Korea University, Korea in 2001, the M.S degree in Information Security from Korea University, Korea, in 2003, and the Ph.D. degree in Information Security from Korea University, Korea, 2009, respectively. Currently, She is a general researcher at Korea Internet & Security Agency in Korea. Her research areas include mobile security, cyber financial security, cryptography and information security. Dr. Eunyoung Choi may be reached at bluecey@kisa.or.kr

HAERYONG PARK received the B.S. degree from Chonnam National University in 1999, Chonnam, Korea, , the M.S. degree from Seoul University in 2001, Seoul, Korea, and the Ph.D. degree from Chonnam National University in 2006,Chonnam, Korea. Currently, he is a general researcher at Korea Internet & Security Agency in Korea. His research areas include cryptographic algorithm design & analysis , cyber balckbox technology development and cloud service security. Dr. Haeryong Park may be reached at hrpark@kisa.or.kr.