https://doi.org/10.33778/kcsa.2021.21.1.009

A Study on IoT Devices Vulnerability and Security★

Seung Jae Yoo*

ABSTRACT

Numerous IoT devices are connected to a wireless network environment to collect and transmit data without time and space limitations, but many security vulnerabilities are exposed in these process. But IoT security is not easy to create feasible security standards and device authentication due to differences in the approach or implementation of devices and networks. However, it is clear that the improvement and application of the standard framework for enhancing the security level of the device is the starting point to help the most successful security effect. In this study, we investigate the confidentiality, integrity, availability, and access control implementation plans for IoT devices (which are the basic goals of information security), and standardized security evaluation criteria for IoT devices, and study ways to improve them.

IoT 디바이스 보안위협 및 대응방안 연구

유 승 재*

ABSTRACT

수많은 IoT기기들이 시공간의 제약이 없는 유무선 네트워크 환경으로 연결되어 데이터를 수집 및 전송하는데, 그로 인해 많은 보안상의 취약점이 노출되고 있다, 그러나 IoT 보안은 디바이스와 네트워크의 접근방식이나 구현방식의 차이로 인해 실현가능한 보안표준과 장치인증을 생성하는 것이 쉽지 않다. 디바이스의 보안레벨 강화를 위한 표준 프레임워크의 개선과 적용이 가장 성공적인 보안효과를 거들 수 있는 출발점이라는 것은 분명한 사실이다. 이 연구에서는, IoT 디바이스에 대해 정보보안의 기본 목표인 기밀성, 무결성, 가용성 그리고 접근통제를 확보할 수 있도록 하는 IoT디바이스에 대한 표준화된 보안성 평가기준을 조사하고, 그 개선방안을 연구하고자 한다.

Key words : IoT Security, IoT Certification, Security Evaluation Criteria

접수일(2021년 02월 28일), 게재확정일(2021년 03월 31일)

* 중부대학교 정보보호학과

★ This paper was supported by Joongbu University Research & Development Fund, in 2020

Ⅰ. Introduction

The IoT continues to grow exponentially in terms of its market and workforce, and in terms of scalability, IoT is creating numerous application areas such as smart home, smart city, smart grid, smart retail smart farm, wearable, healthcare, and connected car.

According to Cisco's report, 2018, the number of networking devices worldwide is expected to reach about 28.5 billion by 2022, of which more than half, or 14.6 billion, will be IoT that connects machines to machines.[7]

IoT devices are subdivided into consumer and industrial categories according to their functions and configurations. In the IoT device category, as a simple device, there is a format that does not communicate with a server and is connected to a terminal through a sensor or converter through zigbee, NFC, bluetooth, and RFID methods, and as a more powerful device, there is a device that uses a powerful processor and processes data by directly communicating with a server by means such as DSL , FTTH and WiFi.

Since numerous IoT devices are connected through a wired/wireless network environment, it can be seen that there is almost no time or space limitation for collecting and transmitting data. Due to these environmental factors, there is a concern about exposure of relatively many vulnerabilities in security, and then IoT threats are basically data interception, interception and forgery, and virus worms.

As we know, interference and forgery attacks by DDoS (DoS), viruses, and malicious codes over wired and wireless are routinely attempted steadily.[1][2][20]

And then, if the target of the attack is closely related to human life, such as healthcare wearable devices, smart cars, and household appliances, it may lead to more serious consequences, so a thorough response is required.

However, in terms of building a relatively secure environment, the current security level can be viewed as very insignificant. In particular, the exponential increase of IoT devices makes it very difficult to establish a universal security environment such as device authentication, data encryption, secure channels, and tunneling.

In this study, we investigate the confidentiality, integrity, availability, and access control implementation plans for IoT devices (which are the basic goals of information security), and standardized security evaluation criteria for IoT devices, and study ways to improve them.

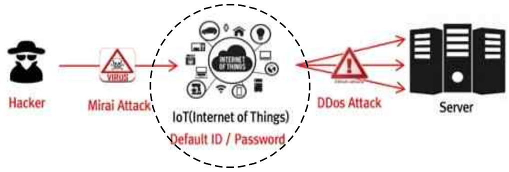
Ⅱ. IoT Vulnerability and Security Product Functions

2.1 IoT Device Vulnerability

As IoT devices are applied to all areas of life, such as personal and major facility access control, social infrastructure management, and agricultural and marine product growth management, It is expected to be managed that everything in our lives is covered through Internet and AI automation. In response to these changes, IoT security establishment Suitable for the environment in the era of the Industry 4.0 is an essential element not only for individuals but also at the corporate and national level.

As mentioned above, IoT devices without adequate security can be a direct criminal pathway. Hacking IoT devices such as IP cameras and stealing or stealing personal information causes privacy or additional crime.

If a malicious firmware upgrade is injected into an IoT device, it can take over the IoT device and form a botnet, causing large-scale DDoS for major infrastructure.



[Fig.1] DDoS attack through wireless router hacking

Looking at the IoT-related attack cases reported so far, it can be seen that mostly fake firmware upgrades, router hacks(as shown in [Fig.1][8]), and CCTV/IP camera hacks. A few related cases are as follows.

In 2019, there was a risk report from Russian white hacker Anna Prosvetova that certain IoT products equipped with the ESP8266 WiFi chipset were exposed online without authentication, and thus fake firmware upgrades were possible.[3]

In 2020, Lennert Woulters, a researcher at the University of KU Leuven in Belgium, reported that a specific model car of T-Company, a global electric vehicle company, had a firmware upgrade risk. He reported that it was possible to steal a vehicle and remotely control it by simply approaching the remote control key and stealing the unlock information and executing a malicious firmware upgrade command.

In SECON & eGISEC 2019, it was announced that digital door locks based on RF communication can be easily hacked through 'Signal Replay Attack' that is a method of attacking by catching the wireless signal generated by the wall pad when opening the door with a transmitter and receiving device and copying and amplifying the wireless signal.[1][2]

According to the Symantec Internet Security Threat Report[20], there are 5,400 Attacks per month on average targeted at IoT devices

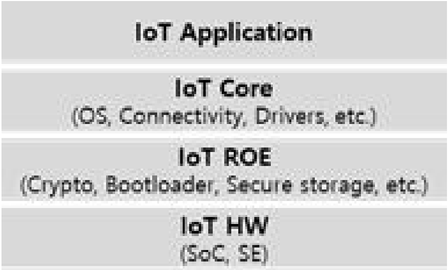
As the risk increases, adoption of IoT devices is rejected or IoT deployment is delayed.

Large-scale DDoS attacks using devices that are vulnerable to security are also possible, and infected devices can form a botnet and be used for various attacks.

IoT devices become zombie by malicious codes such as Satori and Mirai, and can be exploited as a host of malicious code distribution that attacks networks for monetary and profitable crimes and steals personal information.

2.2 IoT Security Products and Functions

In general, IoT products are composed of 4-layers as shown in [Fig.2] due to their structure. For safe IoT device operation, it is required to implement an appropriate security environment for each layer.[9]


IoT Application
IoT Core
(OS, Connectivity, Drivers, etc.)
IoT ROE
(Crypto, Bootloader, Secure storage, etc.)
IoT HW
(SoC, SE)

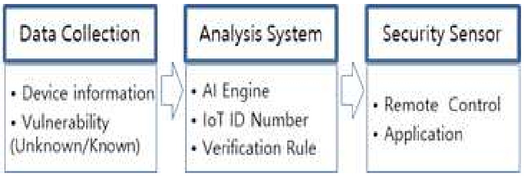
[Fig.2] IoT Device in 4 Layers

Recently, many IoT security solutions and products have been in commercial use, and we look at some of them for their features.

A IoT solution products of N**-company (in Korea) protects various IoT devices such as AP and CCTV connected to the network, and implemented service threats as

[detection] - [blocking] - [response]

when AI machine learning technology was applied for quick and accurate device recognition and behavioral pattern analysis.



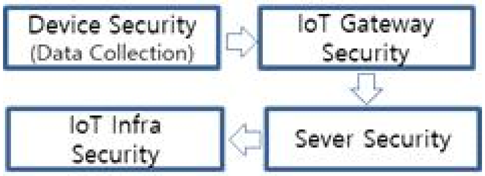
[Fig.3] IoT Care Function[14]

The following are the features of the IoT security product P**IoT Security (P**-company's product).[16]

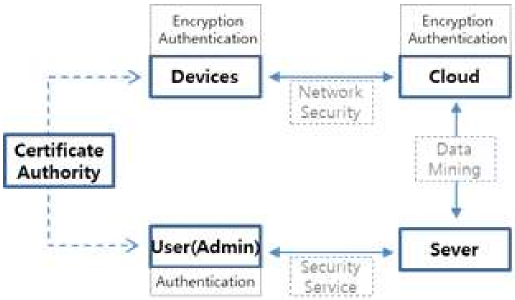
The main technologies to achieve IoT security such as devices, gateways, servers, and infrastructure are as follow;

- encryption including H/W & DB encryption, lightweight encryption module and key management
- network Security including SSL-VPN, APP F/W, data integrity and end-to-end encryption
- authentication for H/W device, PKI device/user and mobile
- security services including monitoring, remote control, abnormal behavior analysis, machine learning

The following two figures are the security configuration in [Fig.4] and main function configuration in [Fig.5] of the IoT product (P**-company).[15][18]



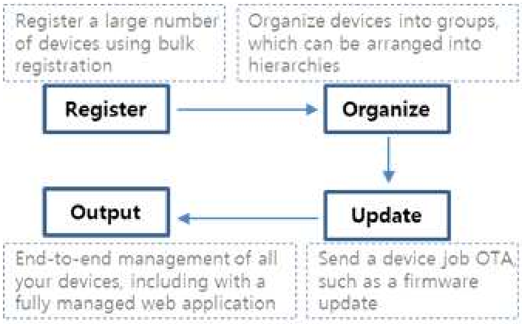
[Fig.4] Security Components



[Fig.5] Main Function Configuration

The following is A** IoT security solution.

Measures to ensure that IoT devices operate correctly and safely include protect access to devices, monitor the condition, detect and remotely solve problems and software and firmware update management, etc.[4]


Register a large number of devices using bulk registration
Organize devices into groups, which can be arranged into hierarchies
Register
Organize
Output
Update
End-to-end management of all your devices, including with a fully managed web application
Send a device job OTA, such as a firmware update

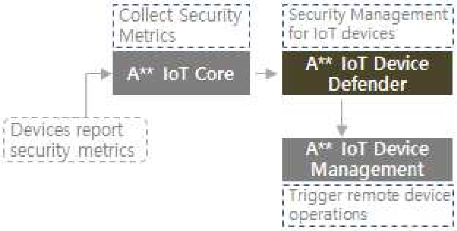
[Fig.6] A**IoT Device Management Configure

As in [Fig.6], A** IoT Core is a IoT device control service which has the following functions to provides convenient and secure data processing in connected devices;[5]

- device connection and management without server management
- connection protocol selection function
- secure device connection and data
- rule-based device data processing and operation

A**IoT Device Defender in [Fig.7] is a well-known IoT device integrated management service that implements the following functions in connection with A** IoT Core and A** IoT Device Management;[6]

- audit function for device-related resources
- monitoring and evaluating data points based on user-defined actions (rules) and reporting anomaly detection alerts
- monitor and identify specified cloud metrics and trigger alarms when anomalies are detected based on machine learning models

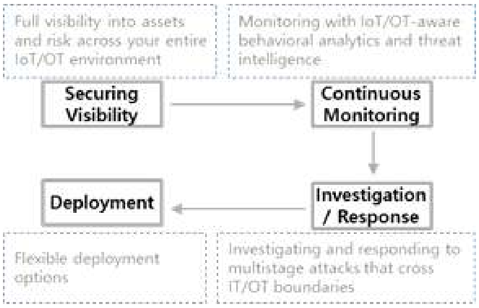

Collect Security Metrics
Security Management for IoT devices
A** IoT Core
A** IoT Device Defender
Devices report security metrics
A** IoT Device Management
Trigger remote device operations

[Fig.7] A** IoT Device Defender Configuration

Microsoft's IoT security strategy is to minimize IoT security issues and protect user, process and data from threats through integrated IoT SIEM, SCAR(Security Coordination, Automation and Response), and XDR (Extended Detection and Response) solutions.[12]

They try to control the risks that exist in the IoT environment by implementing the device enhancement, secure connection, cloud service protection, enhancement of security enforcement capability and reduced complexity.[13]

A** Defender for IoT is a security agent that is constantly searching for assets, performing potential management and new detections for Internet of Things (IoT) and technology (OT) devices. The execution process is shown in [Fig.8].


Full visibility into assets and risk across your entire IoT/OT environment
Monitoring with IoT/OT-aware behavioral analytics and threat intelligence
Securing Visibility
Continuous Monitoring
Deployment
Investigation / Response
Flexible deployment options
Investigating and responding to multistage attacks that cross IT/OT boundaries

[fig.8] A**Defender for IoT Configuration

Ⅲ. IoT Security Technology and Security Evaluation

Cyber-security concern with IoT is based on hijacking attacks on general purpose computers connected to the network.

- Data steal or service interruption through the hijacking of access control.
- IoT infrastructure damage attack that causes data infringement, unstable operation, and physical damage to facilities

Also, the following are pointed out as other IoT security considerations.

- Operational (update and control, etc.) difficulties caused by device heterogeneity
- Problems dealing with lost revenue caused by IoT disconnection
- Vulnerability in security of existing legacy devices that cannot accommodate the security of connected IoT devices

About these security points of view, in [13], it is recommended a three-pronged approach to protect data, devices, and connections;

- Secure provisioning of devices.

- Secure connectivity between devices and the cloud.
- Securing data in the cloud during processing and storage.

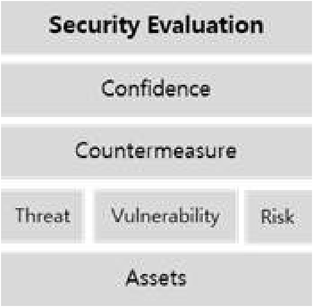
The software that will implement these security functions will have to be structured to perform the following functions.

- Simplify IoT security complexity,
- Monitoring the security management status of connected devices,
- And tracking protection for connected data stores, managers and IoT services, etc.

But it is presumed that devices vulnerable to attack have not been applied with appropriate security standards from the design stage.

Therefore, for commercial IoT devices, it is very important to prepare and control to comply with appropriate certified security standards and requirements according to their functions and application environments

As shown in [Fig.9], security evaluations are performed by CABs in order to provide a certain level of confidence in that the product implements sufficient countermeasures and that these measures are implemented correctly and satisfy the security requirements.[9]



[Fig.9] CASs Security Evaluation

Currently, there are several certification systems for IoT products, and various countries are actively preparing standardized standards.

Here, we will look at KISA's IoT security certification service (IoT-SAP) and PSA Certified, as an IoT device security certification system.

3.1 IoT-SAP

IoT-SAP(KISA's IoT security certification service) is an insurance program that tests whether IoT products and linked mobile apps have a certain level of security and then issues 'Certificates' when meeting standards.

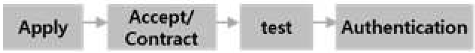
In Korea, since the introduction of this program, 78 IoT products and services have received this certification as of March 2021. (source in [11])

[Table1] IoT product security certification status (as of Mar.2021)

year grade	2021	2020	2019	Total
Lite	8	23	18	49
Basic	1	18	10	29
Standard	0	0	0	0
Total	9	41	29	78

IoT security certification standards are classified into LITE, BASIC, and STANDARD, and as shown in [Table1], various security items are required according to each level.

[Fig.10] indicates the security authentication procedure.



[Fig.10] IoT Authentication Procedure

As shown in the [Table2], the items required for authentication are divided into five types: authentication, password, data protection, platform protection, and physical protection, and are composed of a total of 41 detailed security items. We can see the details on security items in [10].

As a result of such authentication, the effect of voluntary security enhancement and reliability improvement for IoT devices can be expected.

[Table2] IoT security certification requirements for IoT products

Type	Security items	Grade		
		Standard	Basic	Lite
Authen-tication (13)	user authentication	AU1.1-1.8	AU1.1-1.8	AU1.1-1.2
	safe use of authentication information	AU2.1-2.3	AU2.1-2.3	-
	device authentication	AU3.1-3.2	AU3.1	AU3.1
Crypto-graphy (3)	use of safe cryptographic algorithms	CR1.1	CR1.1	CR1.1
	safe key management	CR2.1	-	-
	safe random number generation	CR3.1	-	-
Data Protection (8)	transmission data protection	DP1.1-1.2	DP1.1-1.2	DP1.1
	stored data protection	DP2.1-2.2	DP2.1	DP2.1
	information flow control	DP3.1	-	-
	safe session management	DP4.1-4.2	DP4.1	-
	personal information protection	DP5.1	-	-
Platform Protection (14)	software security	PL1.1-1.4	PL1.1-1.3	PL1.2-1.3
	safe update	PL2.1-2.3	PL2.1-2.2	PL2.1
	security management	PL3.1-3.4	PL3.1-3.3	-
	audit log	PL4.1-4.2	PL4.1	-
	timestamp	PL5.1	-	-
Physical Protection (3)	physical interface protection	PH1.1-1.2	PH1.1-1.2	PH1.2
	defense against tampering	PH2.1	-	-
Number of evaluation items		41	23	10

More notably, in order to obtain this certification, sufficient preparation and review are required for the following matters, and this is recognized as a starting point for building a more secure IoT security environment.

- security measures for each step in the entire process of Design/Development/Distribution and operation management of IoT devices/services
- IoT product/service design considering information protection and privacy enhancement
- appropriate access right management and authentication for IoT service operation, end-to-end communication security, data encryption method
- application of software security technology and hardware security technology with proven stability
- encryption, identification, and access management measures to protect sensitive information

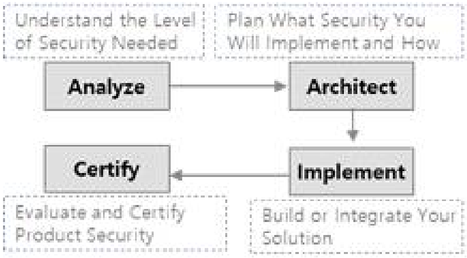
3.2 PSA Certified for IoT

PSA certification is a security framework based on an open source firmware project and matching authentication system to support safe security design for IoT devices.[16]

PSA certification promotes provision of a framework for IoT device protection from analysis to security evaluation and certification

And this framework challenges the solution of the fragmentation problem, which is the limitation of IoT security, and provides standardized resources.

PSA certification consists of the following four-step program[Fig.11] for the security design and development process.[18]


Understand the Level of Security Needed
Plan What Security You Will Implement and How
Analyze
Architect
Certify
Implement
Evaluate and Certify Product Security
Build or Integrate Your Solution

[Fig.11] PSA Security 4-step Framework

The PSA presents the following as standard requirements for the IoT security authentication system;[19]

- Security certification system documents allow use of security level-specific approaches for various IoT product sets
- Starts with security evaluation of the chip and RoT (Root of Trust) and extends to system software and device application code.

Since the introduction of PSA Certified in 2019, 62 IoT products have received this certification as of March 2021.[17]

[Table3] PSA Certified Status(as of Mar.2021)

type / level	Chip	System S/W	Device	Total
Level 3	1	-	-	1
Level 2	9	-	-	9
Level 1	30	15	11	56
Functional	9	8	-	17
Total	49	23	11	83

As shown in above [Table3], since the first PSA Certified program was introduced in 2019, 83 certifications have been awarded for 62 IoT products so far. (The reason why the number of certifications is higher than the number of products is that there are products with multiple levels of duplicate certification.)

For standardized security design for IoT, threat model development functions provided by the PSA authentication framework, appropriately safe chip selection functions, and development simplification functions provided by PSA Functional API are available.

Ⅳ. Conclusions

Even a very simple IoT device can be exploited as an attack target or an attack tool on an Internet network. And IoT security is not easy to create feasible security standards and device authentication due to differences in the approach or implementation of devices and networks. However, it is clear that the improvement and application of the standard framework for enhancing the security level of the device is the starting point to help the most successful security effect.

Therefore, as already mentioned in the previous chapter, many IT leading countries including Korea have developed and operated standardized security standards and certification programs for efficient operation of IoT security.

In addition to this, in order to implement a safer IoT service environment, the development requirements for IoT devices to be introduced in the future should be presented in detail and elaborately step by step, including the following contents, and will have to be continuously updated.

Referring to the IoT development security standards[21] presented by KISA, a more practical proposal is as follows.;

- risk definition and calculation for applications and platforms,
- proper protection of private code signing keys across platform-specific signature generation, use and distribution for embedded device identification and device
- mechanism to establish a so-called trusted (confidentiality and integrity) relationship such as mutual authentication and secure communication between the device and the management server

By sufficiently reflecting the above, appropriate security measures are embedded when designing IOT devices/services, and for this, it is required to apply an intelligent security threat analysis modeling based on AI.

References

[1] Yu W-Y, 'An Analysis of Research Trends in IoT Security, Convergence Security Journal, Vol.18, No.1,pp.61~67, 2018.

[2] Han S-K, Kim M-J, A Design of Technology Element-based Evaluation Model and its Application on Checklist for the IoT Device Security Evaluation, Convergence Security Journal, Vol.18, No.1,pp.49~58, 2018.

[3] https://www.cctvnews.co.kr/news/articleView.html?idxno=201439.

[4] https://aws.amazon.com/ko/iot-device-management/

[5] https://aws.amazon.com/ko/iot-core/

[6] https://aws.amazon.com/ko/iot-device-defender/features/

[7] https://www.cisco.com/c/ko_kr/solutions/internet-of-things/

[8] http://www.ddaily.co.kr/m/m_article/?no=149257

[9] Technical Report:IoT Security Certification Scheme Part-3, Evaluation Methodology v1.2, EURSMART

[10] Internet of Things (IoT) security, Guide to testing and authentication standards, Dec. 2017, KISA

[11] https://www.ksecurity.or.kr/user/extra/kisis/356/iot/iotList/jsp/LayOutPage.do

[12] https://azure.microsoft.com/en-us/overview/iot/security/

[13] https://azure.microsoft.com/en-us/services/azure-defender-for-iot/

[14] https://www.norma.co.kr/iot

[15] https://www.pentasecurity.co.kr/download/#1590053129868-10d07cb4-1dc4

[16] https://www.pentasecurity.co.kr/iot-security/

[17] https://www.psacertified.org/certified-products/

[18] https://www.psacertified.org/blog/four-steps-to-device-security/

[19] https://www.psacertified.org/getting-certified/device-manufacturer/

[20] Internet Security Threat Report, Vol.24, Feb.2019, Symantec

[21] IoT Common Security Guide, IoT Security Alliance, KISA 2016

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교
정보보호학과 교수
email : sjyoo@joongbu.ac.kr