IoT Hacking Attacks and Countermeasure

Sunghyuck Hong, Jungsoo Han, Guijung Kim

Abstract: ***IoT (Internet of Things) means the technology of connecting to the Internet by adding communication functions to all objects. IoT is physical constraints and limited resources which means are a vulnerability for hacking attacks. Therefore, IoT needs countermeasures of the hacking attack. These IoT devices are becoming a target of hacking. Hacking attacks on IoT devices are causing privacy and personal information leakage, and hacked devices are also used for DDoS(Distributed DoS) attacks. To overcome IoT physical constraints, various methods on each sensor in a wireless sensor networks are proposed. We analyzed various characteristics of sensor nodes and listed pros & cons. In addition, countermeasures on each IoT attacks were suggested. By analyzing such cases of hacking damage, I have identified the common weaknesses of IoT devices and looked for countermeasures. Therefore, it contributes to secure communication over a wireless sensor networks.***

Keywords : Internet of Things , malware attack , network security, network vulnerability, hacking attack

I. INTRODUCTION

A. IoT (Internet of Things)

IoT (Internet of Things) refers to the technology of connecting to the Internet by adding communication functions to various objects in the vicinity. Here, various things mean many things, such as household appliances, convenience facilities in public places, and equipment carried by individuals. A variety of IoT devices ranging from Internet-connected refrigerators, surveillance cameras installed in the home, guidance systems at bus stops, to direct production using Arduino or Raspberry Pi, have. The IoT device market is getting bigger. Cisco Systems estimates that the number of objects connected to the Internet will reach 27 billion in 2021 [1]. Figure 1 shows growth rate on IoT based electric devices.

Fig. 1. Cisco Systems. Global Device/Connection Growth

Revised Manuscript Received on September 25, 2019

Sunghyuck Hong, Baekseok University, Div. of ICT, 31065, Republic of Korea. Email: sunghyuck.hong@gmail.com

Jungsoo Han, Baekseok University, Div. of ICT, 31065, Republic of Korea. Email: jhan@bu.ac.kr

Guijung Kim, Baekseok University, Div. of ICT, 31065, Republic of Korea. Email: gjkim@bu.ac.kr

In addition, IDC's IoT market report estimates global spending on IoT in 2017 will increase by 16.7% to the US $ 800 billion, and it is expected to reach the US $ 1.4 trillion by 2021 [2].

B. IoT device security vulnerability

Based on the embedded system, each object is connected to the Internet and has its own Internet Protocol address (IP). These objects are connected to the Internet so that users can easily operate remotely. While various sensors are installed and objects that can acquire data from or interact with the surrounding environment are useful, they may be subject to hacking attacks and cause harm to users. Particularly, miniaturized IoT devices are relatively vulnerable because they operate with limited computing performance due to their characteristics, which sacrifices the security part that requires many operations and processes for convenient access and quick response.

II. RELATED RESEARCH

A. Damage Case of IoT hacking attacks

The most basic security issue for IoT devices is found on the Insecam site. This site allows you to view shooting scenes for devices with networked camera capabilities. Without any consent of the device user, it is possible to view the scene being shot and to use the function such as turning the screen. The devices that are provided with images on this site are generated when the user uses the basic state without setting any security after purchase. IoT devices with well-known passwords or access privilege settings can be accessed from outside without much difficulty. It is a basic but dangerous security issue because it is possible to have Insecam site as well as any knowledge of the network.

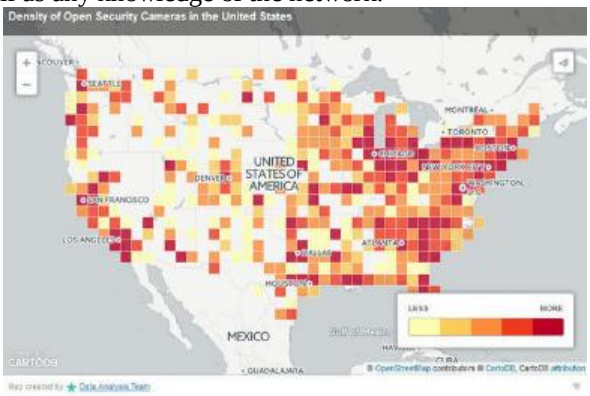

Fig. 2.Open Security Cameras in the United States.

Even if the user is not aware, there are cases of similar damage by the seller of the product. SecureView, a monitoring camera distributed

by TRENDnet in the US in 2013, released with an insufficient level of the security system. As a result, there were over 700 images leaked by hacking and TRENDnet was sanctioned by the Federal Trade Commission [3].

B. Massive damage cases of IoT hacking attacks

In the US, Domain Name System (DNS) service provider received a DDoS attack in 2016 causing more than 1200 domains to fail to access the service. Web services from Amazon, GitHub, Netflix, and many other companies using DNS's services were not accessible, and three DDoS attacks included more than 500,000 IoT devices. The IoT devices used in the attack were infected with malware called Mirai. Mirai has infected Linux-based devices connected to the network, mainly IP cameras and home routers. An infected device is a remotely controlled Bot that becomes part of a Botnet used for large network attacks [4].

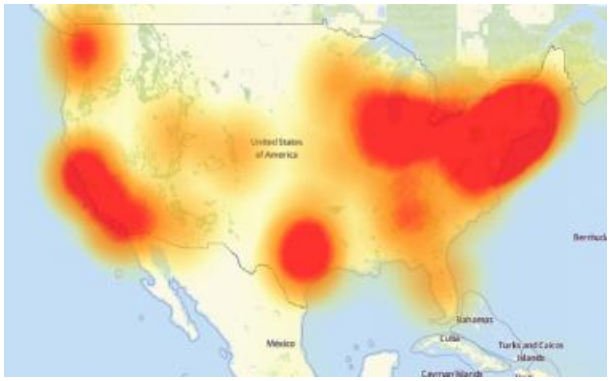

Fig. 3. Mirai malware BotNet IoT Devices Map.

The damage caused by these malware infections is even more dangerous because it increases the risk of infecting other devices on the network where the infected device is running, and in fact, increasing the number of infected devices. In addition, after the source code of Mirai malware has been released, many malware variants have been introduced and the risk is increasing [5].

C. Examples of damage expected from IoT hacking attack

There is a lot of predictable damage from malfunction through radio interference, packet or encryption key capture through data communication analysis of IoT device. The various IoT devices in the house are connected to one network, so once the security problem occurs, the entire IoT device becomes vulnerable. Door locks, gas breakers, and other devices connected to the network are directly linked to safety issues, and the digitization of the vehicle, which has recently undergone much research, also poses a high risk of theft or accidental safety during operation. When a medical device is hacked, it is also dangerous to change the dosage. Most of the damages listed above, such as traffic jams by hacking road traffic signs, hacking of home temperature controllers, have already been shown in many white hackers and security conferences [6]. Table 1 describes that each IoT areas has its own vulnerabilities. IoT with camera has private a video footage problem. Traffic has a possible traffic jam or signal manipulation. Smart car has a brake malfunction. Medical equipment is connected on network and controlled by a operating system which can be hacked. Home network can be manipulated by remote access.

Table- I: Risk of IoT hacking

Field	Risk
IoT with Cam	Private video footage
Traffic	Traffic jam, Signal manipulation
Smart Car	Brake operation, unlock
Medical Equipment	Drug dose manipulation
Home Network	Additional infection in the network, DDoS, Spamming

D. ZigBee security analysis

ZigBee is a technology standard for low-power, low-power devices to send and receive data. It is widely used among devices in a home network unit.

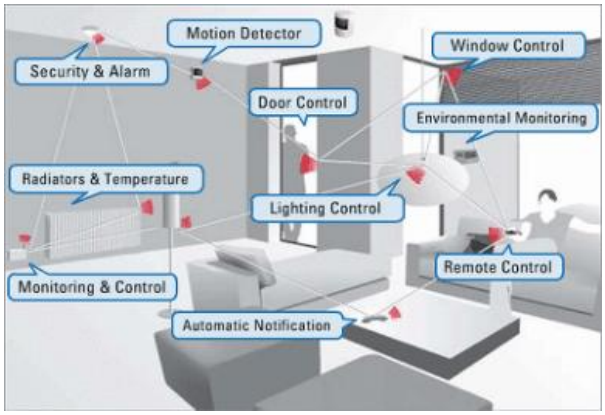

Fig. 4. ZigBee Home Network.

However, low-performance devices are relatively vulnerable to security because they cannot apply high-level encryption technologies. It is also a problem that the encryption level is low and it is difficult to apply the latest techniques, but there are unencrypted sections in the authentication process in particular. This occurs in the pairing process between ZigBee devices and is found in most ZigBee enabled devices. Since there is no way to increase security for the general user, there is no way for the manufacturer to be more concerned about security. As a primary complement, there is an additional authentication procedure in addition to the authentication of the non-encrypted section used for pairing, in addition to the actual command/data transmission. However, the perfect countermeasures will complement ZigBee's technical weaknesses and lead to the standardization of low-power security communication technology [7].

E. Detailed analysis of Mirai malware operation

IoT devices, which are targets of Mirai malware, run on the Linux-based operating systems that run on a variety of hardware. Cross compiled malware to run in these various environments of Linux operating system will attack most IoT devices. Most vulnerable IoT devices are vulnerabilities in the configuration of administrative accounts. These vulnerable devices are infected

with malware, infecting another vulnerable device, securing a large number of Bot devices, and configuring a Botnet to collect DDoS attacks. Mirai malware launches the attack on port 23 of random IP by executing scan function at first run. This attack is an attempt to connect a plurality of IoT devices by randomly assigning the default setting ID / Password to the target device. If the connection to the target device is successful, inject Mirai malware and repeat it to find another target. By repeating this process, a number of malware-infected Bots can be obtained a Botnet and a set of Bots. They can issue a DDoS command through the C&C server.

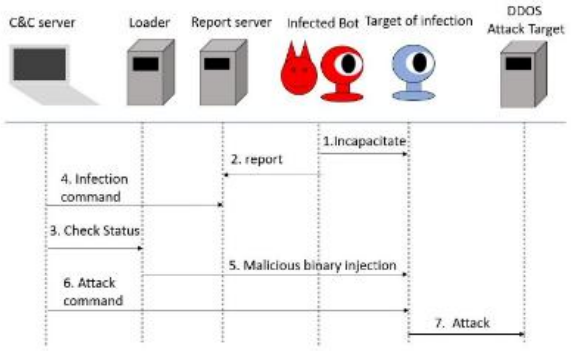

Fig. 5.Mirai malware. Infection and Attack method.

Malicious code attacks such as Mirai malware can be prevented by simple precautionary measures. It is possible to block a lot by blocking the port 23 which is mainly used for malware distribution and changing the default ID / Password. However, there are many variants of Mirai malware with source code released, so be careful and always keep the firmware of the device up to date [8].

F. Attitude in Preparation for IoT hacking attack

In the case of ordinary users, it is difficult to realize a high level of security enhancement because of lack of expertise. However, if you purchase and use IoT devices, you can minimize the damage with simple instructions. If you lack expertise, you will not be able to buy used IoT devices at all. In particular, the main goal of the aforementioned Mirai malware is to keep the default password among the IoT devices on the network.IoT providers should provide initial security configuration guidelines for users. It is also a good idea to encourage them to change their administrative passwords when they are first used. It should be based on a design that emphasizes the security of products and services. It is necessary to prevent unauthorized ports and to block unauthorized access. Firmware should be updated frequently to cope with the latest malware.

TCG (Trusted Computing Group) created and distributed security technology standards for IoT platform. For service development, providers should adhere to this to ensure the secure security of their devices. The basic security functions are as follows [9],[10]. Table 2 shows risk of IoT hacking list which has 10 possible vulnerabilities.

Table- II: TCG – IoT Secure Use Case

1. Establishing and Protecting Device Identity
IoT devices should have the ability to perform mutual authentication with IoT services or with other IoT devices.
2. Protection Against Malware Infection
IoT devices should be able to resist malware infections, Both volatile and persistent. If a malware infection takes place, these devices should minimize the impact and enable recovery.
3. Protecting Against Hardware Tampering
Some kinds of IoT devices need to protect themselves against hardware tampering.
4. Confidentiality, Integrity, and Availability of Data at Rest
Confidential data stored on an IoT device should be protected.
5. Reselling or Decommissioning a Device
Before a device is resold or decommissioned, any sensitive data belonging to the previous owner should be securely erased. Then the device can be securely transferred to a new owner or prepared for disassembly and recycling.
6. Meeting Cryptographic Protocol Requirements
All IoT devices are in some way connected to a network that may not be trustworthy. Cryptographic protocols ensure the security of communications over that network and should be supported.
7. Supporting Multiple Models of Provisioning
IoT technologies must support practical, common methods of provisioning credentials, policies, and anything else needed to make an IoT device functional for the customer.
8. Maintaining Audit Logs
Secure logging is essential to maintaining accountability and enabling forensic analysis.
9. Remote Manageability
Most IoT devices need secure remote management capabilities. Requiring physical access to manage an IoT device won't scale to a large number of devices.
10. Securing Legacy Hardware
The world is currently full of legacy devices that do not support these use cases. Fortunately, the security of these devices can be improved using gateway devices that handle the security for them.

In addition, service providers must provide not only the provision of devices but also the overall management of the consumer. Supply management, manufacturing, assembly, installation, security setting, firmware update, and post-management.

G. The Direction of IoT-related laws

As the IoT environment grows, the relevant legislation needs to be revised and initiated. In the United States, on 1 August 2017, some Senators initiated legislation that stipulates the essential requirements for devices with Internet connectivity. The contents of the bill were as follows.

1) Provide written certification that the product does not contain any known security vulnerabilities.
2) Use software and components that can be updated and patched.
3) Refrain from using hard-coded credentials or passwords.
4) Notify the purchasing agency if any defects are discovered.
5) Update software or replace components that create vulnerabilities.

Repair new security vulnerabilities in a timely manner. These measures will recognize the importance of security from the planning and development stage of IoT and monitor the vulnerability continuously after the service so that it will be able to prevent a lot of cases from the past[11].

III. CONCLUSION

IoT is a field that will attract a lot of attention in the future because many devices connected to the network exchange information, improve the convenience of life, and have good marketability. As a result, IoT devices are increasing in number. The function is also sophisticated and complex, and new technologies are used. Security issues will become even more intense as many devices have diverse sensors, more communications, and the collection and movement of large amounts of data. The severity of damage caused by the hacking of IoT devices is already well known. There is a whole range of threats from personal information leaks to monetary, material damage and major accidents. The threat of information security will grow along with the growing scope of the industry across the industry. If you do not consider security or ignore security by prioritizing performance and functionality, the amount of damage will increase exponentially. Not only the primary hacking damage but also the secondary damage caused by it are already shown. On the top of that, this is not the answer to regulating the spread of IoT devices and distancing them. First of all, users of IoT devices should start with care about their own device management and care about their information security. And service providers must know precisely the data access range and network configuration of each IoT device and establish security measures. While it cannot completely block all attacks and threats, within a realistic scope, organizations will need to standardize security technologies and establish standards that ensure minimum security of IoT devices in the country by law. In Korea, there is no integrated legislation related to IoT. However, there is protection through personal information protection law and location information law. In order to develop IoT related services, enhance competitiveness and ensure stability, the integrated legislation related to IoT should be enacted at the government level.

ACKNOWLEDGMENT

This research was supported by 2019 Baekseok University fund.

REFERENCES

1. J. Guo, Y. Peng, X. Peng, Q. Chen, J. Yu and Y. Dai, "Traffic forecasting for mobile networks with multiplicative seasonal ARIMA models" 2009 9th International Conference on Electronic Measurement & Instruments, Beijing. 2009. https://doi.org/10.1109/ICEMI.2009.5274287
2. S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce" 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida. 2015. https://doi.org/10.1109/ICGCIoT.2015.7380718
3. J. Habibi, D. Midi, A. Mudgerikar and E. Bertino, "Heimdall: Mitigating the Internet of Insecure Things" in IEEE Internet of Things Journal,vol.4 no.4, 2017, pp.968-978. https://doi.org/10.1109/JIOT.2017.2704093
4. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets" in Computer., vol.50 no.7 ,2017, pp. 80-84. https://doi.org/10.1109/MC.2017.201
5. T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari and E. Magesh, "Mitigating Mirai Malware Spreading in IoT Environment" 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018. https://doi.org/10.1109/ICACCI.2018.8554643
6. S. Sezer, "T1C: IoT Security: - Threats, Security Challenges and IoT Security Research and Technology Trends" 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA. 2018. https://doi.org/10.1109/SOCC.2018.8618571
7. W. Razouk, "Zigbee Security within the Framework of IoT" 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue. 2014. https://doi.org/10.1109/SOCA.2014.57.
8. H. Sinanović and S. Mrdovic, "Analysis of Mirai malicious software" 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, 2017. https://doi.org/10.23919/SOFTCOM.2017.8115504
9. D. Minoli, K. Sohraby and J. Kouns, "IoT security (IoTSec) considerations, requirements, and architectures" 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas NV .2017. https://doi.org/10.1109/CCNC.2017.7983271
10. P. McNeil, "Secure IoT deployment in the cement industry" 2017 IEEE-IAS/PCA Cement Industry Technical Conference, Calgary, AB. 2017. https://doi.org/10.1109/CITCON.2017.7951862
11. F. Rahman, M. Farmani, M. Tehranipoor and Y. Jin, "Hardware-Assisted Cybersecurity for IoT Devices" 2017 18th International Workshop on Microprocessor and SOC Test and Verification (MTV), Austin, TX. 2017. https://doi.org/10.1109/MTV.2017.16

AUTHORS PROFILE

Sam 'Sunghyuck' Hong received his B.A. degree from Myongji University, Korea in 1995. After graduation, he worked at Hyosung Inc. in Seoul, Korea from 1995 to 1999 as a computer programmer and ERP consultant. He received a Ph.D. degree from Texas Tech University in August, 2007 major in Computer Science.

After graduation, he worked at International affairs in Texas Tech University as a senior programmer/analyst from 2007 to 2012, and his jobs were development of ASP.NET web applications and maintenance of PC/Server.

Currently, he is an associate professor in Division of Information & Communication at Baekseok University, and he is a member of editorial board in the Journal of Korean Society for Internet Information (KSII) Transactions on Internet and Information Systems. His current research interests include Blockchain, Secure Crypto-currency, Secure Mobile Networks, Secure Wireless Sensor Networks, Key Management, Networks Security, Information Security, Embedded Networked Systems, Embedded Software, Wireless LAN, Distributed Systems, Computer Networks, Hybrid Wireless Network Architecture Design, and Mobility Design/Modeling/Simulation.

He published 53 referred journals papers and 28 referred conference papers which are related to Blockchain and Secure protocols since 2004. Total research grants is $928,578 from 2013 to present. Contact email is shong@bu.ac.kr. Mailing address is Munam-ro 76, Dongnam-Gu, Chenan, Chungnam, Republic of Korea, 31065.

Jung-Soo Han received a BS, an MS, and a PhD in Computer Engineering from Kyung Hee University, Republic of Korea. Since 2001, he has been a Professor in the Division of Information & Communication Technology, Baekseok University, Cheonan City, Chungnam, Republic of Korea. In 2014, he researched Convergence IT and Creative Education Methodology at California State University Fullerton as an Exchange Professor. His research topics include Data Mining, Contents Planning, 3D Modeling and CBD, Telemedicine, Knowledge-based Decision Support Systems, Intelligent Systems, Convergence, HCI, and Recommendation Systems. He has edited books on computer science and convergence technology. He serves as Executive Editing Director of the International Conference on Convergence Content (ICCC), as General Co-Chair of the International Conference on Digital Policy & Management (ICPDM), as General Co-Chair for steering committees of the International Conference on Convergence Technology (ICCT), as Workshop Chair of the International Conference on Information Science and Application 2013, as Workshop Chair of the 2nd International Conference on IT Convergence and Security 2012, as Vice President of the Korea Contents Association, as Vice President and a member of the Editorial Committee of the Society of Digital Policy & Management, and as Vice President of the Editorial Committee of the Korea Contents Association.

GuiJung Kim received the B.S. degree and the M.S. degree in computer engineering from Hannam university, Republic of Korea, and the Ph.D. degree in computer engineering from Kyunghee university, Republic of Korea in 2003. Since 2001, she has been a professor in department of Biomedical Engineering, Konyang University, Chungnam, Republic of Korea. Since 2017, has been a Professor in the Division of Information & Communication Technology, Baekseok University, Cheonan City, Chungnam, Republic of Korea. Her main research interests include Medical Information System and 3D e-Learning, security programing, Big data, Intelligent Systems, Convergence System. She has edited books on computer science and convergence technology.