Jeong-Jin Kang
Edward J. Rothwell
Nguyen Nang Dinh
Nguyen Thanh Thuy
Gyoo Seok Choi
Nguyen Ha Nam

Advanced and Applied Convergence Letters AACL 07

Advanced and Applied Convergence

2nd International Joint Conference, IJCC 2016
Hanoi, Vietnam, January 18-22 2016
Revised Selected Papers

IIBC
IPACT

Vulnerability of USB Device Based on IoT

Byungho Park[1], R. Young Chul Kim[2], Dukyun Kim[3], and Sungdeok Cha[3]

[1]*Ministry of National Defense, Seoul, 140-701, Republic of Korea*
[2]*SE Lab, Dept. of CIC(Computer Information Communication), Hongik University, Republic of Korea*
[3]*Graduate School of Information Security, Korea University, Republic of Korea*
[1]*sunsonbob@naver.com*, [2]*bob@hongik.ac.kr*, [3]*kim9069@gmail.com*, [3*]*scha@korea.ac.kr*

Abstract

The rapid development of the Internet and electronic devices can bring a great transformation in our lives. Internet of Things is the network of physical objects or "things" embedded with electronics, softwares, sensors, and connected networks, which enables them to collect and exchange data. Why is IOT security so critical? There are several security risks that occur in the communication process through the connection to the wired and wireless networks for IOT service. In addition, cyber-attacks have been sophisticated, and complicated due to unknown serious vulnerability associated with the IOT spread.

This paper will present the secure vulnerability with USB device based on IOT. If an embedded firm ware of USB were transformed illegally, it would be identified as a mouse, a keyboard, a network card, etc. in a PC. This kind of USB is called Bad USB. Furthermore, it will suggest how to detect Bad USB.

Keywords: *IOT; Malware; BAD USB; Firm ware; Vulnerability;*

1. Introduction

Recently, with the rapid development of smart devices, the connection between people and objects have been possible anywhere any time, and the interest of the Internet of Things (IOT) has been increasing. We can see the IOT device in any place such as CCTVs, IPTVs, refrigerators, home locks, healthcare devices, Z-Wave, ZigBee, etc.

By Wikipedia [1], IOT is the network of physical objects or "things" embedded with electronics, softwares, sensors, and connected networks, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across the existing network infrastructure, creating opportunities for more direct integrations between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefits. Each thing is uniquely identifiable through its embedded computing system and able to interoperate within the existing Internet infrastructure. Experts estimate that the IOT will consist of almost 50 billion objects by 2020.

Concerns have been raised that the Internet of Things is being developed rapidly without appropriate consideration of the profound security challenges involved[2] and the regulatory changes that might be necessary[3]. In addition, cyber-attacks have been sophisticated and complicated due to unknown serious vulnerability associated with the IOT spread.

According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest problem in adopting Internet of Things technology [4]. In particular, as the Internet of Things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat [5].

IOT must be connected with a wire or wireless network between objects, so it can have vulnerability.

Generally speaking, USB short for Universal Serial Bus is not called IOT device because it does not contain an IP or a network function. However, some USBs can get a network function by modifying an

J.J. Kang et al. (Eds.): IJCC 2016, AACL 07, pp. 160~163, 2016

embedded firm ware illegally. Although USB seems to be a mass storage, the modified USB may be considered as a kind of IOT device. If an embedded firm ware of USB were transformed, it would be identified as a mouse, a keyboard, a network card, etc. in a PC. Specially, if a hacker inserted a malicious code in the firm ware of USB, it could destroy a system or steal files. This kind of USB is called Bad USB.

In this paper, we will present the vulnerable security of USB device based on IOT. Especially, we study a bad USB which can change various devices such as a mouse, a keyboard, a network card, and mass storage. Furthermore, it will suggest how to detect the bad USB.

2. Treatment and Measure of Bad USB on IOT

2.1 Security Issues on IOT

Why is IOT security so critical? The cyber-attacks have been sophisticated and complicated due to unknown serious vulnerability associated with the IOT spread. However, despite predicting the rosy growth of the IOT industry, the cases of threatening IOT security have been increasing, which is expected to be a big problem itself in the development of the related markets because of decreased reliabilities in the IOT devices and services.

Hacking targets have been spread to the overall living and industrial aspects, and the extensive areas including power grids, vehicles, health care services, home network systems, etc. have been more likely to be those of malicious hackers. Especially, in health care services, excessive insulin injections to a diabetic patient can result in a sudden shock or death. Also, when power grids or traffic control systems are hacked, they will suffer from great disasters.

2.2 USB & Bad USB

USB has become so commonplace that we rarely worry about its security, and a normal USB has one class such as an external store value 8(Hexa decimal). We will show major USB classes in the following Table [9].

Table 1. Class of USB

Class	Usage	Description	Examples Or exception
03h	Interface	Human interface device	Keyboard, mouse, joystick
06h	Interface	Image	Webcam, scanner
08h	Interface	Mass storage	USB flash drive, memory card reader, digital audio player, digital camera, external drive
0Eh	Interface	Video	Webcam
10h	Interface	Audio/video	Webcam, TV

Generally speaking, USB is not called IOT device because it does not contain an IP or a network function. "Blackhat 2014[10]" Bad USB was introduced on Aug. 7, 2014. Bad USB looks like a regular USB, it can modify the built-in firmware illegally and have multiple classes of USB. However, some USBs can get a network function by modifying an embedded firmware illegally. Although USB seems to be a mass storage, the modified USB may be considered as a kind of IOT device. If an embedded firmware of USB were transformed, it would be identified as a mouse, a keyboard, a network card, etc. in a PC. Specially, if a hacker inserted a malicious code in the firmware of USB, it can destroy a system or steal files. This kind of

USB is called Bad USB.

As an example of Bad USB, it can be disguised with a keyboard of Class 03h, it can enter a command, steal a file, or install a malware in a PC. Also, it is possible to disguise it with a network card, change DNS settings in a computer, redirect traffic, or modify the startup configuration file only to activate viruses when booting a computer, and to make vaccines helpless. In other words, Bad USB can be classified as IOT with a variety of transformations, but it is just a malware to make hacking attempts, and to cause incompetent Malware Detection systems.

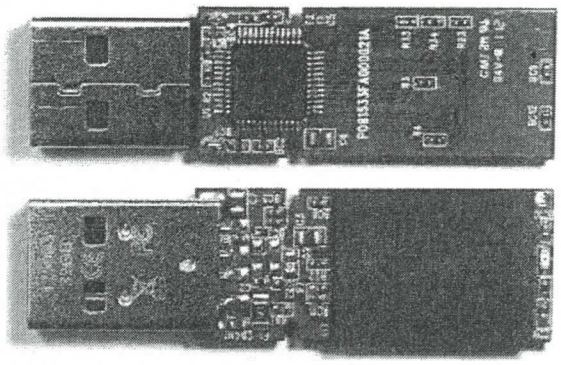

Figure 1. The Structure of general USB

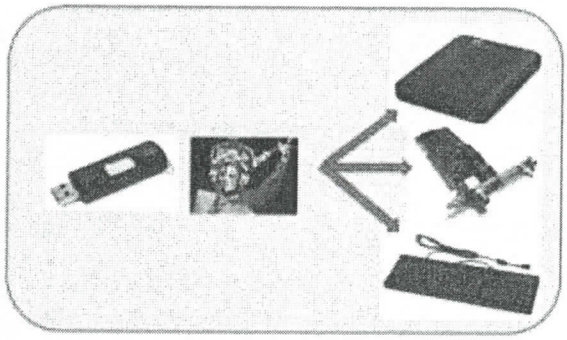

Figure 2. An example of transformation from general USB to Multi Devices

2.3 How to detect Bad USB

USB usually contains two values; Product ID and Vendor ID by 2 bytes, respectively. It is very difficult to fix Bad USB because of its vulnerabilities. We show the list of USB storage which can be converted into Bad USB [11].

Based on a user's testing, the following devices have been found to have a supporting controller:

- Patriot 8GB Supersonic Xpress*
- Kingston Data Traveler 3.0 T111 8GB
- Silicon power marvel M60 64GB
- Patriot Stellar 64 Gb Phison
- Toshiba TransMemory-MX USB 3.0 16GB (May ship with 2307)
- Toshiba TransMemory-MX USB 3.0 8GB
- Kingston Data Traveler G4 64 GB

- Patriot PSF16GXPUSB Supersonic Xpress 16GB
- Silicon Power 32GB Blaze B30 (SP032GBUF3B30V1K)
- Kingston Digital 8GB USB 3.0 Data Traveler (DT100G3/8GB)* - Using PS2251-03

For detecting Bad USB, the computer first investigates a Bad USB list, and in case it turns out to be existing, it continues to check the PID and VID of Bad USB list. So, if possible, it is recommended not to use anything in the above USB list.

3. Conclusion

Recently, with the rapid development of smart devices, the connection between people and objects has been possible anywhere any time, and the interest of IOT has been increasing. IOT is the network of physical objects or "things" embedded with electronics, softwares, sensors, and connected networks, which enables these objects to collect and exchange data. However, despite predicting the rosy growth of the IOT industry, the cases of threatening IOT security have been increasing, which is expected to be a big problem itself in the development of the related markets due to decreased reliabilities in the IOT devices and services.

IOT security is very critical. There are several security risks that occur in the communication process since the connection to the wired and wireless networks for IOT service. In addition, cyber-attacks have been sophisticated and complicated due to unknown serious vulnerability associated with the IOT spread. USB has become so commonplace that we rarely worry about its security. Generally speaking, USB is not called IOT device which does not contain an IP or a network function. Bad USB looks like a regular USB, it can modify the embedded firmware illegally and have multiple classes of USB with a network function. It may be considered as a kind of IOT device. Specially, if a hacker inserted a malicious code in the firmware of USB, it can destroy a system or steal files. This kind of USB is called Bad USB.

This paper presented the vulnerability of USB device based on IOT. Furthermore, it suggested how to detect Bad USB.

References

[1] Internet of Things, *https://en.wikipedia.org/wiki/Internet_of_Things*
[2] Singh Jatinder, Pasquier Thomas, Bacon Jean, Ko Hajoon, Eyers David, "Twenty Cloud Security Considerations for Supporting the Internet of Things," IEEE Internet of Things Journal: 1-1. Doi:10.1109/JIOT.2015.2460333, 2015.
[3] Chris Clearfield, "Why The FTC Can't Regulate The Internet of Things," Forbes. Retrieved 26, June, 2015
[4] BUSINESS INSIDER, We Asked Executives About The Internet Of Things And Their Answers Reveal That Security Remains A Huge Concern, *http://www.businessinsider.com/internet-of-things-survey-and-statistics-2015-1*
[5] Christopher Clearfield "Rethinking Security for the Internet of Things," Harvard Business Review Blog, *https://hbr.org/2013/06/rethinking-security-for-the-in*
[6] Disruptive Technologies Global Trends 2025. National Intelligence Council (NIC), pp. 27, April 2008.
[7] Ackerman, Spencer (15 March 2012). "CIA Chief: We'll Spy on We'll Spy on You Through Your Dishwasher". WIRED. Retrieved 26 June 2015.You Through Your Dishwasher". WIRED. Retrieved 26 June 2015Prudden, J. F., Method and agent for treating inflammatory disorders of the gastrointestinal tract. US Patent 4,006,224, 2007

ISSN 2288-6060

Advanced and Applied Convergence Letters

The AACL series is committed to the publication of proceedings of Advanced and Applied Convergence. Its objective is to publish original researches in various areas of Smart Convergence. This will provide good chances for academia and industry professionals as well as practitioners to share their ideas, problems and solutions relating to the multifaceted aspects.

Research papers were strictly peer-reviewed by program committees to make sure that the papers accepted were high quality and relevant to the current and future issues and trends in Advanced and Applied Smart Convergence.

The scope of AACL includes the entire area of advanced and applied convergence from the current and future trends. The language of publication is English.