International Journal of Smart Home
Vol. 9, No. 10, (2015), pp. 63-68
http://dx.doi.org/10.14257/ijsh.2015.9.10.07

Study on the Vulnerability Level of Physical Security And Application of the IP-Based Devices

Kwang-Hyuk Park[1], Il-Kyeun Ra[2] and Chang-Soo Kim[3]*

[1]*Interdisciplinary Program of Information Systems, Pukyong National University, 608-737, Republic of Korea*
[2]*Department of Computer Science and Engineering, University of Colorado Denver, Denver, CO 80203, United States of America*
[3]*Department of IT Convergence and Application Engineering, Pukyong National University, 608-737, Republic of Korea*
Email: rhkdgur@hanmail.net, ilkyeun.ra@ucdenver.edu, cskim@pknu.ac.kr

Abstract

The various IP-based devices (Sensor network devices, CCTV, etc.) are provided with a specific purpose, recently, IP-based IoT (Internet of Things) devices of collecting information were studied intensively. However, these IoT devices have vulnerability of security because of CPU processing power and small storage capacity. In this paper, we analyze vulnerability of security with the classification of IoT devices and investigate the practice. And we look at the issues of vulnerability of physical security based on results of analysis. Based on this, it provides a baseline about standards of the security level of IP-based devices. Also, looking for the target and studying the ways to take advantage of this standard.

Keywords: *IoT devices, IP exposure, Measures, Security*

1. Introduction

As the increase in number of IoT devices, international standards are prepared, and network security protocol is developed as well. Despite such efforts, users are often using the initial ID and PW that was set in the factory. This situation can be easily obtained by malicious people to have access to the rights and the device. When using the engine to search for IoT devices, a number of devices list can be obtained that it can be exploited only by the keyword search. In this situation, the security of the device does not have an indicator to measure how dangerous it is even less sensitive to the risk. This vicious cycle becomes even more neglected in security management. In this paper, a non-professional point of view, the general users to access, easy to understand indicator made about the security vulnerability as an easy reference level. And after collecting actual data, by giving a rating to create statistics, we want to inform the readers, whether vulnerable or not, as to what extent the current security is at [1].

2. Security Threat of the Device

Through IoT devices, we can include location information of the user, which means that that much information is transmitted and is generated, to compromise the security of the IoT devices by people for trying to benefit by attacking the device elements has also been discovered. The era has come to a number of information, including the user's location information, is generated and transmitted in the IoT devices.

These people get their profits by breaching the IoT devices and these kinds of threats to the security are found. There are many factors considered here and we investigated the four elements that can be found most often [2].

ISSN: 1975-4094 IJSH

2.1. Exposure of IP

It is very difficult to prevent the IP address getting exposed. However, the beginning of every malicious attempt is to access an exposed IP address. There are several ways to hide the IP; commonly used method is to bypass using a proxy server and using a VPN. However, these methods have fatal disadvantages such as slowing internet speed and weakening security system. There is a need in developing other alternative technology [3-5].

2.2. Information Exposure of Device

A screen requesting an ID and PW attempts to access your IP address.. Abundant information is contained on this screen. Although many use initial ID and PW of device, the access is not easy if they are unable to get the initial ID and PW. However, if relevant information, such as model name of device, manufacturer and type of device, is shown on screen, acquisition of the initial ID and PW will become easier with simple internet search.

2.3. Initial ID/PW Management

To use original initial ID and PW is dangerous. There was a case of a Russian hacker who had made seventy thousands IP Cameras which was using initial ID and PW public to the world. However, despite the reality where there are existing cases that alerted society like with another case of hacking three thousands cameras by the same individual, still many are using initial ID and PW. To change initial ID/PW will enhance security system to be sufficiently safe. Creation of a complicated combination of password as much as possible will be a shortcut to safety as well [6].

2.4. Concealment of Access Port

Even if IP is known, if the access port is not open when access is allowed through assigned port, access is denied. One can deteriorate imprudent access by setting access to be denied without assignment of port for one cannot easily identify open port, unless port scan is performed additionally.

3. Vulnerability Level Setting, Actual Application Statistics and Suggestion of Solution

3.1. Vulnerability Level Setting

Vulnerability level is assigned in accordance with the degree of risk based on the standard of security threats shown above. With the safest rating as A and the most dangerous rating as D, there are four ratings of A, B, C, D. As shown in illustration 1, colors of green, yellow, orange and red are assigned in order from A rating icon. The shape of icon is inspired by shape of a lock that is mostly known as a symbol of security.

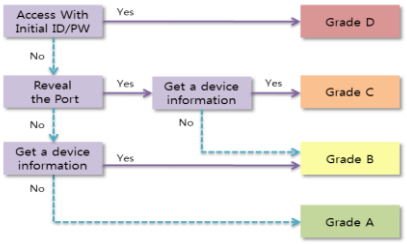

Figure 1. The Progresses of Leveling

3.1.1. Grade A to D: Though exposure of IP is inevitable, the log-in page must not be shown when user entered the wrong Port while accessing the concerned IP. There is no information relevant to device on log-in page with an ID and PW set by a user, and that is all that is necessary. Rating B is assigned when access to log-in page is allowed without entering the port number or log-in page which includes information such as the type of device, model name or manufacturer amongst devices with the same condition as A rating device. Because there arises a tendency to use words set to be used for the name of device as access ID, B rating is given also when the name of the device is exposed.

Rating C is assigned when user can access to log-in page without entering port number and information about concerned device is shown on log-in page. Even if user was able to manage initial ID and PW, it will not be a problem for an expert hacker to acquire admin authority for C rating devices.

Rating D is assigned if user uses initial ID and PW or if anyone can acquire admin authority without any attempt to do so. There are actual cases rarely; and these cases are mostly dangerous for possible manipulation or change of data of concerned devices. The device of such rating can be abused whenever one has intention to do so at no cost.

3.2. Classification of Actual Rating Application and Statistics

As a result to access 158 IP devices around the world through random search, 33 devices were revealed to belong to rating D. There were also rating C 42 devices. Please refer to Figure 2 and 3 for details.

Figure 2. The Number of Devices to Each Grade

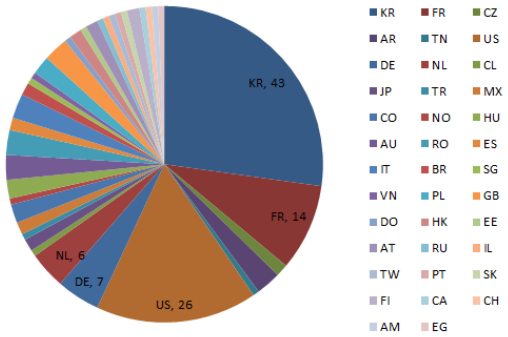

Figure 3. Nationality Statistics on the Target Device

3.3. Alternative Security Suggestions

3.3.1. Introduction of White-List Obligation for IoT Devices: By introduction of White-list, as a counterpart of Black-List, a method which only allows access to devices with permit that is available through registration beforehand is obliged. There is a

disadvantage on a new device registration with low accessibility, it will not be a big problem due to the nature of loT equipment that usually accesses devices that are often used. It provides a chance to enter ID and PW only to the users in accordance with characteristics in a list such as Mac Address or IP[7].

3.3.2. Exposure Minimization of Equipment Information: It is highly recommended not to give any information about a device before accessing the log-in page. When the types of device, name of model or manufacturer are exposed, the device itself provides a great hint to know its initial ID and PW. It can be said that exposure of device will be minimized as well if exposure of information is minimized for initial information is easily found by keyword search of loT equipment search engine.

4. Target and Using Ways

The criteria to gauge the level of IP-based security devices are now clearly in need throughout our community. But there's no clear answer for the specific agent, place and way to use it.

There is no meaning if no one will use the security level in accordance to the criteria laid elements of vulnerability, not knowing the purpose and plan. We will find out who can take advantage of the security level of an IP-based device, and look for the specific use to explore ways and the benefits for each target.

4.1. Ensuring Mandatory through Regulations Established

Even simple to identify vulnerabilities of IP-based devices provide a convenient basis, without any compulsion would not have expected this to be easy to adopt which is made for real use. After initiative and modifications are made in the legislation related to security based on these standards, if it can be somewhat of a regulation on measures to reinforce the vulnerable elements to point out in this paper, like the security threats, we will be able to respond to it more efficiently.

If you are on the login page of the security threats related to information disclosure and in regulating the establishing of initial ID / PW on the device, threats B and C are both fundamentally removed. Unless a hacker with superior technology, people in general are a big help to be able to prevent illegal access, IP-based security enhancement device.

4.1.1. Legislation Initiative Process and Contents: As you can see in Figure 4 below, in accordance with the established legislative plan of the National Assembly or government initiative of Proposition undergoing a review, to the National Assembly through a vote of the State Council, it is followed by an announcement received with the signature of the President. If this legislation is to establish a planning department in consultation with the authorities, and then would be submitted to Parliament through political consultations [8]

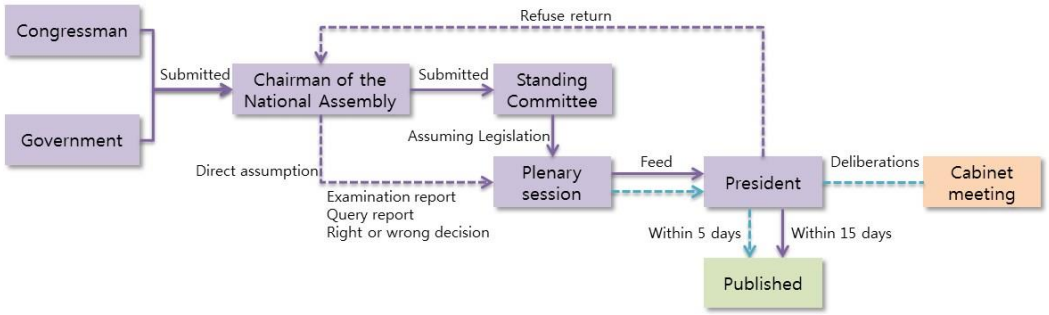

Figure 4. Legislation Initiative Process

Manufacturers of IP-based device after passage of the legislation are obliged to use the initial page information with minimal exposure of the device, uniform set of initial password and username will also take steps such as changing.

4.1.2. Security-Related Legislation is currently in Effect: Currently, the laws enforced in relation to the information security are as follows:

- Personal Information Protection Act
- Electronic Banking Transactions Act
- Information Network Act
- Credit Information Act

Most contents are related to the protection of the law and it can be seen on their data and personal information are not laws or regulations containing additional information about the security of the device itself. As mentioned in 4.1.1., if you raise the minimum set of required security from the device manufacturing steps, which are quite simple, majority will be safe than Class B devices[9].

4.2. Information and Guidance Led by the Government's Office

After the graded security threats level, where substantially responsible for management will be the appropriate government offices. Although the legal system is not substantially prepared through the legislature, if the instructions are enforced under the leadership of the responsible ministries, then there will be a significant effect.

4.3. Voluntary used by enterprise

Without external administration and law, the change in its own perception of the company producing the product is important. Why bother going through the legislative procedure even if it's compulsory, if you are aware of the fact that only a very small effort to help improve the security of IP-based devices reflects the production process, procedures and greater efforts will be greatly helpful in improving security without rating.

4.4. Self-Checking of Individual Users

Check the security efforts of individuals to try their IP-based devices using security indicators, it is to some extent determined whether the situation is dangerous and this is the most important part rather than the appropriate response.

5. Conclusion

Four factors that threaten IoT device security were discussed and four security threat levels were defined corresponding to these four factors. Actual access test was performed targeting IoT devices around the world randomly and each level was assigned. As a result, it has proven the vulnerability of security in general. This research also discussed the alternative suggestions which manufacturers can utilize instead of users to dissolve such unsatisfactory security factors. So be prepared to learn a subject about security clearance standards, it sought to take advantage of the specific measures for each target. Researchers hoped this research to be helpful for future study or research regarding IoT device security.

References

[1] D. Gessner, A. Olivereau, A. Salinas Segura and A. Serbanati, "Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things", IEEE Conference on Trust, Security and Privacy, **(2012)**.
[2] S. K. Hynix, "Official Blog Column "Threatening presence of Smartphones and wearable devices, the device hacking", http://skhynix.tistory.com/1185, **(2015)**.
[3] Korea Information Security Agency (KISA), "Cases of exploitation of a proxy program for bypass connect to online games", KrCERT-IN-2006-02, **(2006)**.
[4] Korea Information Security Agency (KISA), "After setup Virtual Private Network, Waypoint exploitation of damage cases", KrCERT-IN-2011-001, **(2011)**.
[5] Journal of the Korea Institute of Information and Communication Engineering (JKIICE), "Analysis of Global Research Trend on Information Security", vol. 19, no. 5, **(2015)**, pp. 1110-1116.
[6] dailysecu.com, "CCTV SCADA", http://www.dailysecu.com/news_view.php?article_id=5517, **(2013)**.
[7] H. Yoo, J. –H. Yun and T. Shon, "Whitelist-Based Anomaly Detection for Industrial Control System Security", Journal of the Korea Communication Sciences '13-08, vol. 38B, no. 08, 2013.
[8] Legislative Office web-page, "Government guidance legislative process",
[9] http://www.moleg.go.kr/lawinfo/governmentLegislation/process/processSchedule, **(2015)**.
[10] Kim and J. Law Firm, "Information security laws and current issues",
[11] https://www.raonsecure.com/data/thanksletter/20130905/01_raonsecure2013seminar_kimchang.pdf, **(2013)**.

Authors

Kwnag-Hyuk Park, He received his B.S. degree in Urban Engineering from Hongik University in Korea in 2014. He is taking his master's degree at Pukyong National University. His current research interests are disaster prevention, Internet of Things, GIS and security of IP exposure.

Il-Kyeun Ra, He holds a Ph.D. degree in Computer and Information Science from Syracuse University in 2001, M.S. degree in Computer Science from University of Colorado Boulder, and B.S. degree and M.S. degree in Computer Science from Sogang University. He was a Research Staff Member at the LG Information and Communications Research Center. He joined the department of Computer Science and Engineering at the University of Colorado Denver 2001. His main research interests include computer networks, developing adaptive distributed system software and high speed communication system software to support High Performance Distributed Computing Applications.

Chang-Soo Kim, He received a B.S degree in Computer Science from Ulsan University, Korea, in 1979, and an M.S. degree in Computer Engineering and Ph.D. degree in Computer Engineering from Chungang University, Korea, in 1984 and 1991 respectively. He has been a professor at the department of IT Convergence and Application Engineering, Pukyong National University, Korea, since 1992. His research interests are operation system, LBS/GIS, WSN and urban disaster prevention system.

