Journal of Digital Contents Society Vol. 17 No. 6 Dec. 2016(pp. 499-507)
https://doi.org/10.9728/dcs.2016.17.6.499

A Study on Security Vulnerability Management in Electric Power Industry IoT

Sang-Gi Lee*, Sei-Yoon Lee**, Jeong-Chul Kim***

Abstract

The era of IoT, which figures exchanging data from the internet between things is coming. Recently, former electric power energy policy paradigm, namely Supply side paradigm, is changing, because electric power energy consumption is rapidly increasing. As new paradigm for this limit, convergence of existing electric power grid and ICT(Information and Communication Technology) will accelerate intellectualization of electric power device, its operation system. This change brought opened electric power grid. Consequently, attacks to the national electric power grid are increasing. On this paper, we will analyze security threats of existing IoT, discuss security weakness on electric power industry IoT and suggest needed security requirements, security technology.

Keywords : Electric Power Industry, Vulnerability, Security, Cyber Security, Threat

전력 산업 IoT에서의 보안 취약점 관리에 관한 연구

이상기*, 이세윤**, 김정출***

요 약

사물 간의 인터넷을 통하여 정보를 주고받는 사물인터넷 시대가 열리고 있다. 최근 전력 수요가 급증하면서 기존 공급 위주의 전력에너지 정책 패러다임이 변화하고 있다. 사물인터넷 기술이 발전함에 따라 기존 전력망에 ICT를 융합시켜, 전력 디바이스 및 운영 시스템의 지능화를 가속화시킬 것이다. 전력망에 사물인터넷이 접목되어 개방화함에 따라 국가 전력망에 대한 사이버 위협 및 공격에 대한 우려가 증대되고 있다. 본 논문에서는 기존 사물인터넷에서의 보안 위협을 분석하고 전력산업 사물인터넷에서의 보안 취약점과 보안 요구사항 및 보안 기술을 제시하고자 한다.

키워드 : 전력 산업, 취약성, 보안, 사이버 보안, 위협

1. Introduction

Recently, IoT(Internet of Things) connected by internet are figured by approximately 10 billion, in the year of 2020, the figure will be reached to 50 billion. Thanks to openness of IoT, there is a prospect that connection between different kinds of products, networks, applications will be accelerated, accordingly security threats will be increased[1].

In spite of IoT's merits, in the year of 2015, the figure of control system violation will be reached to 295 cases, increasing by 20% as compared with the former year. In the last

※ Corresponding Author : Sang-Gi Lee
Received : November 25, 2016
Revised : December 18, 2016
Accepted : Decembe 30, 2016

* Kyonggi University Computer Science
email: leesg6102@kyonggi.ac.kr
** Korea University Law
email: edouardm@hanmail.net
*** Kookmin University Electrical Engineering & Computer Science
email: kjc5443@gmail.com

▣ This research was supported by Korea Electric Power Corporation through Korea Electrical Engineering & Science Research Institute. (grant number : R15XA03-65)

year, the most frequently attacked part is major manufacturing industries, and energy, water supply, drainage facility are followed about attack figures. This attack figure is reached to 486, remarkably increased when compared to 231 in 2014[2]. ICS(Industrial Control System) attack can shake industries or national system on the whole, can bring a considerable impact on national major infrastructure. National infrastructure means fundamental system needed for national function implement, such as electric power, water resources, gas transport network. Scott Borg, the head chief of the U.S. Cyber Consequence Unit, said that if one-third network of the U.S. electric power network is blacked out, there will be damages 40-50 times greater than a large hurricane like Hurricane Katrina. Moreover, unlike in former electric power grid, in electric power industry IoT, as data technology is converged by electric power grid, the electric power grid can be controlled by outside invaders by communications network. Even, what was worse, in national emergency situation, national overall system may be incapacitated. On this paper, we will find out how formerly many people discussed IoT security threat could be applied to electric power industry IoT. Based on this, we will analyze security weakness of electric power industry IoT. Eventually using these analysis, we will establish security solution on electric power industry IoT[3].

This paper is composed like this. Firstly, we will find out the formerly many people discussed kinds and examples security threat of IoT in chapter II. Secondly, we also find out weaknesses of electric power industry IoT in chapter III. Thirdly, we will discuss security requirements and technology of electric power industry IoT in chapter IV. Lastly, we will command the direction of available further studies.

2. Formerly discussed security threats of IoT

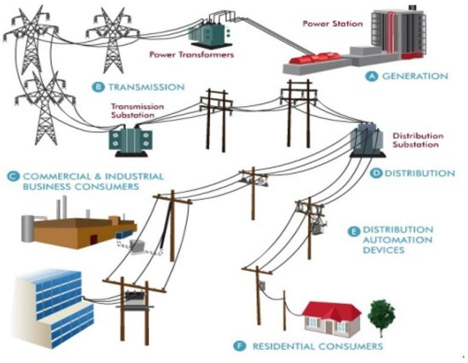
IoT means an environment building intellectual relationship by wire-wireless network connection from various kinds of things with sensors and communication functions. IoT connects all the things like humans, products, spaces and data. And nowadays IoT is rising up as new power of economic growth, is applied to various industries, and is applied to major social infrastructure.

Recently by IoT platform openness, the connection of networks, applications, different devices is accelerating. Despite of this merit, various security threats are mentioned as (Figure 1). IoT security threats are fatal like threating human's life, and countermeasure is unable or expensive. There can be security threats interrupting normal service offer, use, 'violating, commonly said, three elements of data security, like Confidentiality, Integrity, Availability'.

In IoT, it is hard to strengthen overall security of many interconnected devices, for limits of time, memory, process, energy consumption, etc. The elements of IoT security threats are representative as Confidentiality/Integrity attack, privacy invasion, manipulation/extortion of data. Next, we will find out the representative security threats and examples.

2.1 Security threats on devices

At present, PCs, mobiles are connected by networks, and security is implemented by individual level in vaccine, etc., or by group level in IPS. Of course, enclosed-type devices, medical devices, automobiles, etc., are not connected to networks, but individually used. The devices with limits of CPU efficiency, consuming electric power, memory volume, etc.,



(Figure 1) Electric power industry elements concerned with security threats

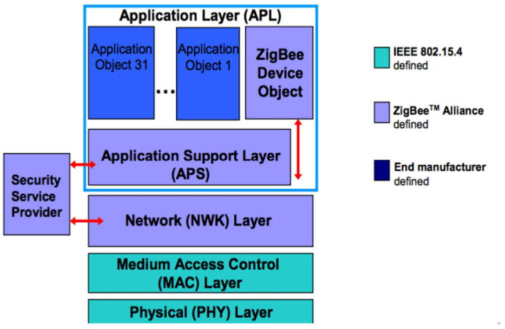
have trouble with being applied by existing code technology. Especially in low specification devices, it is hard to enhance efficiency and security level.

Also, as the functions and kinds have become various, it is getting hard for the devices to be applied for security. Therefore, managing and monitoring of the devices has come to be not easy. From this kind of poor managing, monitoring, abnormal manipulating of information's input node, tag has become possible, and unauthorized user's illegal approach has become possible.

In Russia, some spy microchips, used in hacking of spreading malignant code, spam, by connecting wireless network, were detected in made-in-China irons, kettles. Discovered spy microchips were tiny and cheap, so those could be put in many devices easily. About this, people presume that China criminal group organizationally put spy chips into various kinds of home appliances for large scale hacking[4].

2.2 Security threats on networks

On IoT network, there are security threats in the field of domain like RFID/USN, ZigBee, Wi-Fi, 3G/LTE. Concretely, network security threats include data forgery, authentication interruption, data confidentiality/integrity invasion, data loss, denial of service. Especially on wireless network, it is not only hard to maintain security level, as interworking between different wireless networks like ZigBee, Wi-Fi, Bluetooth, etc., but also device authentication is provided limitedly for device communication. Also, security on interworking between different networks includes risks in authentication limits, occurring communication delay. As on data server, server is vulnerable to illegal network eavesdropping, attack to directory server, and illegal data stealing on data server. And sensor network is vulnerable in security of physical position, accession, based on sensor network intrinsic features. Network traffic attack can cause zombie PCs via cloud services, infecting various devices with infection codes, and bring network degradation by thing's infected robot's network traffic sudden increase attack(DDoS).



(Figure 2) Security in the ZigBee stack block

At present, Europe has introduced an intellectual greenhouse service, so called 'Smart farm', remote-controlling inside temperature, humidity, water supply, drainage, fertilizing by smartphone IoT. An attempt to hack remote-controlling system maliciously and incapacitate temperature, humidity system, was exposed. If this attempt was succeeded, the farm would have damaged[5].

For IoT network security, authentication, security communication, access control between devices are not only needed for integrated networking between different functional IoT devices, but also network monitoring, managing skill are needed for prevent traffic sudden increase attack(DDoS). In the case of sensor network, a sensor-receiving-data encryption module, which can be supported by security service provider as (Figure 2). Also, both security technology for interworking between different networks and security technology application for large scale devices, networks, are needed.

2.3 Security threats on platform/service

In case of IoT platform, there can be a security threats such as malicious data on transmission between devices and services via open platform, individual data loss from illegal management of malfunction data and collected data. In case of IoT service, when malicious data is intruded via a middle ware, fatal attack to a device's operating system, hardware resources can be occurred. In case of IoT application, there are security threats not only like data-falsification, data-confidentiality, data-integrity, privacy-invasion, but also like user identity data loss, tracing users from centralized control of data by an IoT device.

There is a case in which a hacker attacked U.S. central traffic-control system and left a massage, "Watch out dinosaurs ahead", on traffic signs. This is the representative case about data forgery. When it comes to the situation that important information should be reached to people, but it did not, there can be a big accident. This event brought people, who believe a national system deeply, big confusion[6].

For IoT platform/service security, firstly, depended on its kind, we need an unrelated platform to be offered. Secondly, we need mutual authentication, limitation of an unauthorized access, key management technology, and technology for anonymity for preventing privacy invasion. For application security, we need its own specially prepared proper security technology, because of its natures of low-electric power, lightweight.

3. Security threats in electric power industry IoT

Recently electric power industry is figured as a highly intellectual, automatized electric power management system converged with information communication technology. Unlike the former electric power system, mutual relationship with other systems is more important, openness to other systems is more possible. This change brought us security threat increase. These security threats in electric power industry system may menace national fundamental, necessary systems like electric power, water resources, gas transport network

On March, 2008, there was an accident that the U.S. Georgia Hatchee nuclear plant was stopped for system software update. This kind of accident can bring us enormous economic damage[7].

On April, 2009, the U.S. national security officer said that cyber spy embedded malicious program to destroy electric power system by intruding the U.S. electric power system. This spy from China or Russia wanted to manipulate all the U.S. electric power system needed, going around in this system[8].

In electric power industry, the types of security threats are the same as followed.

3.1 Security threats via devices

If security in an electric power industry IoT device is not considered, this device security can be easily threatened by attackers. In case of a smart meter, which installed on a house's outside wall, an attacker can easily manipulate or destroy the device with poor physical security. Moreover, via this device, the attacker can get into the system of an electric power industry management center.

3.2 Security threats via networks

While the former electric power grid was managed as closed grid, nowadays electric power industry has converged with IoT, and worm infection, virus infection, a hacker's intrusion are possible. With this phenomenon applied to electric power grid, security threats are gotten worse. A Smart meter, which is used to find out electric power transmission, supply, is the subject to be intruded the easiest. And when this meter is attacked, huge confusion can be occurred. In case of HAN(Home Area Network), it has various security vulnerabilities, with connecting different wire, wireless networks, like financial data stealing, privacy invasion with regard to a user.

3.3 Security threats via software

When it comes to the situation that electric power grid is converged with IoT, the software in major system can be threatened. To offer various services in electric power industry IoT, software should be properly updated. If each software has problem on stability or security weaknesses, attackers can use this, consequently attacking electric power managing system or threating electric power industry networks by making and spreading a malignant code.

4. Management of security weakness in eletric power industry IoT

As we discussed above, a smart meter, a data collector, a data collecting sensor, a wind power station and a solar power station can be threatened in security. And these transmit or receive important data in electric power industry, such as electric power supply demand state, electric power facility state, electric power facility control. Most of electric power industry IoT have many lightweight, low-electric power devices, so it is hard to apply general code algorithm because of limits of function, cost. Consequently, these kinds of electric power industry IoT have lower security level. For this limit, attackers can intrude connected network more easily, and finally threaten the security of all the electric power industry. To overcome this. there are several approaches for lightweight cryptography algorithms as <Table. 1>.

Even worse, if there are not user authentication as <Table. 2>, access control system, this situation can be linked to blocking out. Electric power by an attacker, and can be

PRESENT[16]	- The block length is 64bit and two key lengths of 80 and 128 bits are supported.(Figure 3)
KATAN, TANTAN[17]	- The structure of the KATAN and the KTANTAN ciphers is loaded into two registers, several bits are taken from the registers and enter two nonlinear Boolean functions.(Figure 4)
HummingBrid[18]	- An encryption algorithm with a 128-bit secret key and a 64-bit initialization vector.
HIGHT[19]	- A new block cipher HIGHT with 64-bit block length and 128-bit key length.(Figure 5) - Ubiquitous computing device such as a sensor in USN or RFID tag.
Photon[20]	- An AES-like primitive as internal unkeyed permutation - The most compact hash function (about 1120 GE for 64bit collision resistance security)

<Table 1> Lightweight Cryptography

ID/PW	- Special application, protocol needed for ID/PW Authentication between an administrator and a device. Account data priorly shared.
Certificate	- PKI based device authentication used. As electronic signature, Verification algorithm for device authentication, figure over RSA(2,048 bit), hash function SHA-2(256 bit) used.
SIM	- Authentication way using USIM or UICC geared in device.

<Table 2> Authentication ways between devices

linked to financial damage like electric power price manipulation. For the worst, this can be related to large scale attacks to electric power grid, like worm, virus, DDoS. Next, we will discuss security requirements in electric power industry IoT, and present available security technology.

4.1 Device Security

4.1.1 Security requirement

Electric power industry IoT devices are converged with wire, wireless service, smart gears. The devices are originally lightweight gear, and need a low-electric power encryption module. Also a security module is needed for IoT platform's management system. In case of a drone, a sensor, a sensor node is so small that CPU, computing ability are restrained, therefore various customized device security technologies are needed.

4.1.2 Security techonology

Traditional security system, which can be used to electric power industry IoT, commonly use AES[9] and DES[10] for offering confidentiality, and use hash function like SHA-1, SHA-2[11], MD5[12], and recently established as standard, SHA-3[13] for offering integrity, and use PKI based on RSA[14] for offering authentication function. On the ITU-T's Framework[15], which defines IoT's structure on the aspect of web, well for the most, defines divided non-constrained devices with sufficient resources, constrained devices with insufficient resources in terms of calculation or electric power.

One of the most essential elements composing IoT, a constrained device has a limit on using traditional encryption system, in terms of calculation, storage and communication capacity.

In electric power industry IoT, when communicating with other devices, whether data was transmitted from an authorized device should be identified, authenticated. Authentication process between devices is implemented via the middleware geared in the device, or in the situation without a middleware, could be implemented via a separate device gateway. Authentication ways include ID/PW, certificate of authentication, SIM

RFID USN [22]	- RFID(Radio Frequency Identifier) based on ISO-18000-7 standard - Wireless network collecting, processing, storage a thing's data, surrounding data by attached tag on the thing
ZigBee [23]	- ZigBee based on IEEE 802.15.4 standard works at network layer, application level - ZigBee divided with low level security SSM (Standard Security Mode) and high level security HSM(High Security Mode)
Wi-Fi [24]	a) WEP - Wireless LAN or Wi-Fi based on IEEE 802.11 standard conducting on data link layer - Stated clearly that WEP(Wired Equivalent Privacy) is a user's authentication protocol on IEEE 802.11 - Fundamental authentication algorithm is RC4 b) WPA, WPA2 - As the user recognition way which make up for a weakness of WEP, using TKIP(Temporal Key Integrity Protocol), AES-CCMP as authentication algorithm
3G/LTE	- 3G mobile communication has closed environment with voice focused - Infected devices' malicious, abnormal traffic flow to 3G/4G network, by mobile malicious code - Impossible for security gears, in existing

	internet environment, to apply 3G/4G network - Continuous study needed, because detect, dealing are difficult to major attacks
Serial	- Security technology not applied to standard - Serial communication data encryption can be used, by string code, symmetric key code

<Table 3> Security technologies matching to electric power indusrty IoT Communication ways

4.2 Network Security

4.2.1 Security requirement

The former network, sensor network are applied to network for electric power industry IoT service. In network, devices and sensors, which are different in communication ways(ZigBee, Bluetooth, Wi-Fi, etc.), security features(code, authentication way, etc.), are mutually connected. In case of wireless communication, figure transmitted by wireless can be exposed to various attacks like node obtainment, denial of service attack, router attack, etc.. So, we need application of a security solution both on gateway and from outside of network. For sensor security, we need network security technologies proper to sensor environment, like lightweight encryption authentication technology, lightweight key management technology, privacy protect technology, sub-channel attack prevention technology.

4.2.2 Security techonology

Control message protection/authentication, need a security protocol AES-CCM, which is based on symmetric key, and a protocol, which is based on hash, MIC. Concerned with device authentication solution, access controlling device can control other devices, services related. In case of wire, wireless environment, there are SCADA technology, Dedicated Security Monitoring/ Managing technology. <Table. 3> shows several security technologies matching to communication ways[21].

4.3 Platform/service Security

4.3.1 Security requirement

In case of IoT platform/service, thorough security authentication is needed, because it is applied to existing smart gears, Also, encryption transmission technology for individual data, access control module should be applied. Device's individual data filtering technology is needed, and safe guide on open platform should be arranged, and mutual authentication, key management between a device and a user are demanded. Specially made security platform, reflecting service feature(home, medicine, transportation, home appliance) and operating-environment (embedded wearable, mobile).

4.3.2 Security techonology

Security on electric power industry IoT platform has a considerable relationship to security technology, model on network. While M2M technology before IoT has a point on secure communication between devices, electric power industry IoT need secure platform technologies between all the devices with internet approachable or able to communicate.

In case of web service, there are three standard, WSDL(Web Service Definition Language), SOAP(Simple Object Access Protocol), UDDI(Universal Discovery and Integration of Business for Web). And in case of platform, symmetric key/hash based authentication/authentication protocol/verification protocol are needed. By platform level device authentication solution based on full PK1, device authentication can be various depending on various devices like PC, smartphone, CCTV, Set-top Box.

5. Conclusion

This paper has handled the former IoT security threats, examples, and furtherly approached electric power industry IoT security threats. And this paper has introduced present security technology available to apply to electric power industry IoT. By this analysis, we have found out security weaknesses, requirements as to electric power industry IoT. Based on this study, future researches will focus on developing of legal and institutional countermeasures against security threats, and developing of an information security management system and an evaluation/assurance schema for electric power industry IoT.

References

[1] https://isms.islearning.kr/mik_lib/file_down.php?bf_idx=16

[2] https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[3] Jin-Young Kim and Sun-Myung Hwang, "Outlook and Challenges of Security System for the Activation of IoT", Korea Computer Congress, Korea Information Science Society, Jeju, 2015, pp. 1037-1039.

[4] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=1&seq=21742

[5] http://kashi.or.kr/board/index.html?action=view&board_id=pds2&seq=13032

[6] http://datanet.co.kr/news/articleView.html?idxno=69 944

[7] http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501858.html

[8] http://online.wsj.com/article/SB123914805204099085.html

[9] J. Daemen, V. Rijmen, "AES proposal: Rijndael", NISTAES Proposal, 1998, pp. 1-45.

[10] NIST, "FIPS PUB 46-3 Data Encryption Standard (DES)", Federal Information Processing Standards Publications, 1999, pp. 1-22.

[11] NIST, "FIPS PUB 180-4 Secure Hash Standard", Federal Information Processing Standards Publications, 2012, pp. 1-39.

[12] IETF, "RFC-1321 The MD5 Message-Digest Algorithm", Network Working Group, 1992, pp. 1-22.

[13] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, "The Keccak reference", round 3 submission to NIST SHA-3, 2011, pp. 1-69.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol.21, No. 2, 1978, pp. 120-126.

[15] ITU-T, "Framework of Web of Things", Inernational Telecommunication Union, 2012, pp. 1-22.

[16] 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", In Proceedings of the International Conferenceon Cryptographic Hardware and Embedded Systems(CHES 07), Vol. 4727, 2007, pp. 405-466.

[17] C. Cannière, O. Dunkelman, M. Knežević, Katan, and Ktantan, "A family of small and efficient hardware-oriented block ciphers", In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 09), Vol. 5747, 2009, pp.272-288.

[18] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm", In Proceedings of the 7th International Conference on RFID Security and Privacy(RFIDSec'11), Vol. 7055, 2011, pp. 19-31.

[19] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim,J. Kim, and S. Chee, "Hight: a new block cipher suitable for low-resource device", In Proceedings of the Internat

ional Conference on Cryptographic Hardware and Embedded Systems(CHES 06), Vol. 4269, 2006, pp. 46-59.

[20] J. Guo, T. Peyrin, and A. Poschmann, "The photon family of lightweight hash functions", in Crypto2011, Lncs, Vol. 6841, 2011, pp. 222-239.

[21] A. Bogdanov, M. Knežević, G. Leander, D. Toz,K. Varici, I. Verbauwhede, and Spongent: "The design space of lightweight cryptographic hashing", http://sites.google.com/site/spongenthash, 2012.

[22] Donghee Kim, Seokung Yoon, Yongpil Lee, "Security for the IoT Service", The Korean Institute of Communications and Information Sciences, Vol.30, No.8, 2013, pp.53-59.

[23] http://www.zigbee.org

[24] http://www.wi-fi.org

Sang-Gi Lee

1988 : Yonsei University (M.S Degree).
2000 : Daejeon University (Ph.D Degree).
1983~1995 : KEPCO Human Resource Development Institute for Electric Power and Information Communications Education (Associate Professor).
1995~1997 : KEPRI Electric Power and Information Communications Research (Senior Researcher).
2005~2008 : KEPCO PI & Sales SI (Vice president).
2009~2010 : KEPCO ICT Planning & Inforamion Operation (CIO).
2013~now : Kyonggi University Computer Science (Associate Professor).
Research Interests : S/W Science Technology, Ubiquitous Computing (IoT/AI/Big Data), Information Protection & Security Management.

Sei-Yoon Lee

2009 : Korea University (M.S Degree).
2012~2014 : Korea Research Institute of Intellectual Property (Researcher).
2014~now : Korea University (Ph.D Degree Candidate).
Research Interests : Intellectual Property Law & Policy, Information Protection, Security Management.

Jeong-Chul Kim

2010~now : Kookmin University Electrical Engineering & Computer Science (B.S. Degree Candidate)
Research Interests : Information Protection & Security Management, Internet of Things.