International Journal of Control and Automation
Vol. 10, No. 2 (2017), pp.35-44
http//dx.doi.org/10.14257/ijca.2017.10.2.04

A Method for Overcoming Security Vulnerability of DR Service Network

June-Kyoung Lee[1*] and Kyoung-Hak Lee[2]

[1]Naonworks, Seoul 152-775, Korea
[2]IACF, Kwangwoon University, Seoul 139-701, Korea
[1]darkelan@naonworks.com, [2]goldbug@kw.ac.kr

Abstract

Recently, various methods for efficient power consumption for managing power demand, which has increased rapidly, have been proposed. The most typical way, are expanding smart grid-based demand response services. In this paper, we analyze the security vulnerabilities of the protocol openADR the core protocols of the power demand response services. Using the open source of the most generally used to have openADR protocol in the current demand response system, to construct a demand response service network. Analyze the vulnerabilities of various attacks in real demand response service network and similar environment presented a scheme that can overcome the vulnerability.

Keywords*: Smart Grid, DR (Demand Response), Security, openADR(open Automated Demand Response), VTN(Virtual Top Node), VEN(Virtual End Node)*

1. Introduction

What is a smart grid technology that combines information and communication technologies (ICT: Information & Communication Technology) in the electricity transmission, distribution and the development process. By electric providers and consumers to interact with each other, the pursuit of intelligent and sophisticated power grid, to provide high quality power service, the energy utilization efficiency can be maximized.

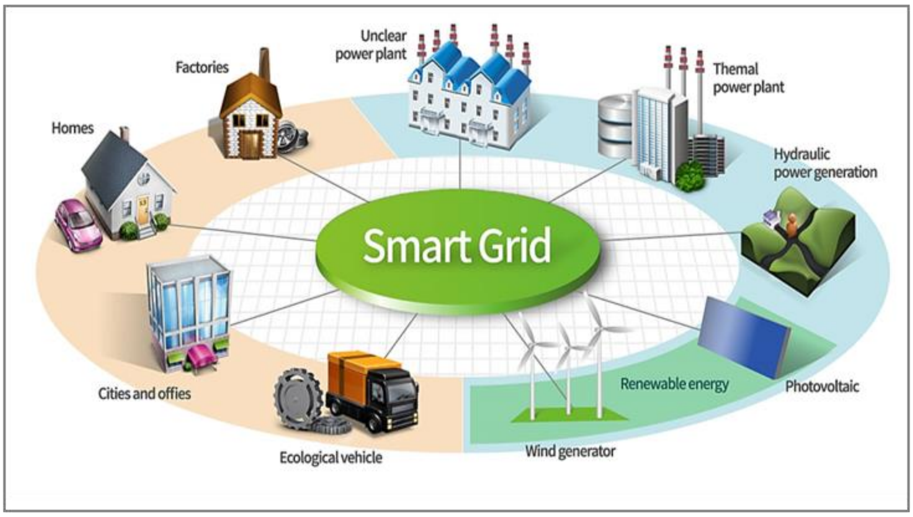


Figure 1. Smart Grid Overview

Smart Grid era previous existing power supply systems have been organized around electrical power supplier. [1, 2, 3, 4] Power consumer has used the power to pay the cost

*Corresponding Author : June-Kyoung Lee

of power supplied by the power provider. As a result, even if excess or deficiency of the electric power is generated, the problem occurs that there’s no active approach to this. For example, if the air conditioning usage of the summer has been rapidly increasing, and there’s insufficient power, then large-scale power outage can frequently occur. On the contrary, night-time electricity consumption is relatively small, as it was prone to discard waste excess power.

Therefore, in the smart grid network, it solves the power of the excess or deficiency in question, in order to balance the consumption and supply of electrical energy, power demand response(DR: Demand Response) system is presented. DR management system is a power system consisting of a large power exchanges, electricity demand management operators, electric power consumers. The power DR system: if power is insufficient, the consumer reduces the power consumption. This power management system provides a financial benefit to consumers due to a more stable power supply.

In these Internet-based smart grid power demand management network, in order to streamline and optimize the use and supply of electrical energy between the power demand management systems, DR technology is being used. openADR (open Automated Demand Response) 2.0 protocol is growing in important technology as the standard protocol of open automated DR system to be able to deliver a DR signal to the provider and the system provider and the user. Therefore, the power DR system, is necessary to communicate openADR 2.0 protocol between power DR systems, power demand management operators, and electric power consumers. However, communication between each of these configurations can be exposed to the hacker, in this case, there is a variety of security issues, and the potential that can be transmitted, such as a bad electrical usage such as reduction request. Currently, the security products of domestic and foreign demand for power management, a situation there is no choice other than Web firewall, which is a state in which the security threat is still present for the vulnerability of openADR 2.0 protocol. If the demand management business DR business is enabled to target each household that has been further activated than it is now, the occurrence of a variety of security vulnerabilities of problems and security incidents have been foreseen. Such a situation, power demand management of a national backbone resources, if they occur security issues, are inherent risks that can develop into serious social problems, such as people's anxiety construction. [5, 6]

In this paper, in Chapter 2, we discussed the openADR concepts and openADR security standard as a smart energy international standard protocol for the savings and automation of power demand management of the current energy. In addition, Chapter 3, using the most widely used openADR 2.0 base EPRI open source in the world, was to analyze the vulnerability of potential attacks that occur at the time of implementation of openADR system. Finally, Chapter 4 summarizes the results of a study about a scheme that can protect the vulnerable attack analyzed in Chapter 3. Finally, in Chapter 5, we summarize the results of this paper.

2. openADR

2.1. Overview

DR is one method for constructing a stable power network. It corresponds to the increased power demand and peak load, by adjusting the power consumption in response to a request of the electric charges and the providers of consumer side, makes use of this technique to ensure the stability and reliability of the electric power system.[8] To enable the services of the reaction of these demands, it is a necessary data format standardized communication method. [7, 8, 9, 10]

It means openADR and open automated DR, refers to a standard communication protocol applied to intelligent DR. This protocol is, the development of commercial openADR system, test, and in order to support the deployment, developed in openADR Alliance [11], which was established in the center of the industry participants in 2010, demand is based on the sustainability and reliability reaction which is a standard protocol. openADR is supporting the new automated DR away from the traditional passive DR as an international standard. Although there is openADR1.0 and openADR 2.0a / b, current openADR1.0 is partially used, a situation where openADR 2.0 is mainly used. openADR 2.0a, resources are limited and intended for DR system for performing a simple DR application, whereas it only supports the Simple EiEvent service, openADR 2.0b, and some of the DR. If you are a DR system for running applications and target EiEvent, EiReport, EiRegisterParty, and supports EiOpt service. openADR 2.0 standard has been developed to 2.0b version of the initial device that has been refined through the version of 2.0a of the target.

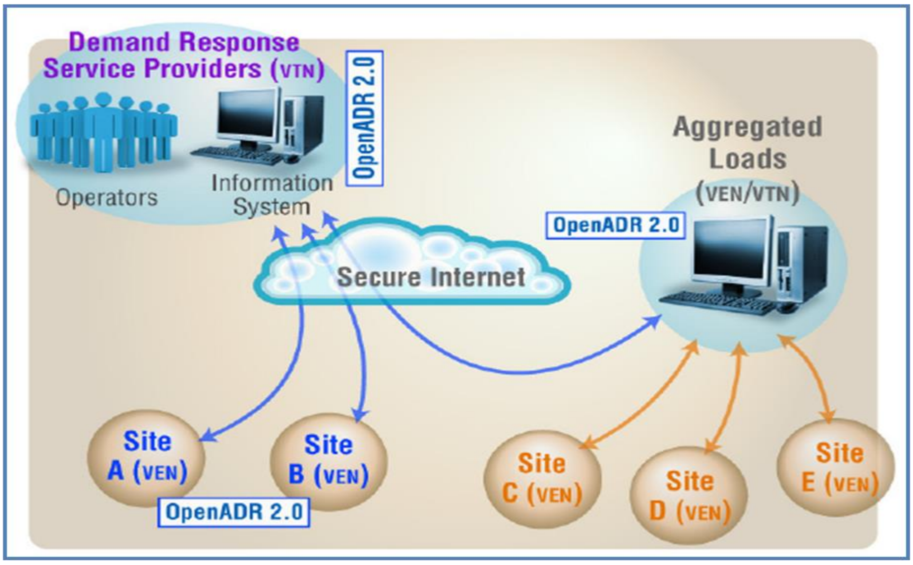


Figure 2. Possible relationships of VTN and VEN [14]

As can be seen in [Figure 2], Major nodes and devices are provided in openADR 2.0b to respond to the significant operation in the server to provide information VTN (Virtual Top Node) and information VEN (Virtual End It is divided into node). In addition, for the mutual exchange of information between the VTN and VEN, you are using an existing open standard (HTTP, XMPP). These standards are basically provided EiEvent services for simple VEN control, EiReport service for power consumption Report, EiRegisterParty services for VEN registration, the EiOpt service is a kind of scheduling service. Also, to provide a flow of mutually complementary DR events between the VTN and VEN now supports data transfer of PULL system with HTTP PUSH that was used in the 2.0a version. [12, 13, 14]

Features of openADR provides a standardized way for the energy supply and system administrators to transmit a DR signal using a common language across all IP-based communication networks that exists, such as the internet. Also it has a feature that the automated DR events by the end user to be automatically started by the reception of an external signal. openADR can come to power suppliers have the same effect as reliability, predictability for consumers, increased consistency, DR programs increased participation, increased customer service. The consumer perspective can bring the effects of energy savings, increase energy efficiency, energy management device according to a DR program participation costs. In addition, the manufacturer of the device it is possible to produce an effect of complexity of relief and quick and easy installation and operation, it has grown as a core technology in the power demand management service network.

2.2. Security

Security protocol for openADR is defined mainly using the Transport Layer Security protocol method using TLS (Transport Layer Security) as suggested in the published standards organizations. VTN and VEN are the use of TLS for encryption, there is a security problem related to certificates and encryption algorithm. TLS is a standardized protocol, which is the SSL (Secure Socket Layer) protocol, in the IETF TSL working group. SSL protocol is an industry standard protocol for securely sending and receiving data between the World Wide Web browser and a web server. It is also possible to implement the XML Security in openADR security if necessary.

However, in addition to the current transport layer security method, the development of the corresponding security technology for this and openADR protocol terms and services of vulnerability analysis is the initial stage. In addition, power demand management system that is currently in operation, with security as a concern, there is no other choice but to utilize the web firewall. However, even if the web application firewall is operating, the security threat to openADR protocol-related vulnerabilities still exists. In the future, if the demand management business is activated through a national DR business, the occurrence of a variety of security vulnerabilities of issues and cases such as the following have been foreseen.

(1) Loss of power system control by cyber attack
(2) Leakage of personal information by hacking of transfer data
(3) The threat of consumer power usage restrictions due to abnormal external control
(4) National disaster situation occurs such as the black-out

As described above, the power demand management network, because it treats the electricity is a sensitive national backbone resources as national security facilities, not only the economic damage in the event security problems, serious, such as public anxiety construction is inherent risk that can be developed into a social problem.

3. Security Vulnerability Analysis in DR Network

We use the EPRI open source, which is the most reliable and widely used for openADR vulnerability analysis configure demand management network system consisting of VEN and VTN[15]. openADR was analyzed for the attack vulnerability of openADR divided into parameters modulation attack and services flow tampering.

3.1 The Configuration of the Vulnerability Analysis System

Using the EPRI open source for vulnerability analysis of the various attacks, we configure the demand management network in conjunction with the VTN and VEN system that implements the openADR 2.0b protocol. Thus, by dividing into two types constructed similarly to the actual power demand management network was analyzed for vulnerability attack. For vulnerability analysis of the attack, to change the EPRI open source to the actual VEN system that has been made using the EPRI open source, made the VTN system was created attacker linked on. The configuration network was analyzed for vulnerabilities on various attacks that may be possessed by the VEN system.

To change the EPRI open source to the actual VTN system that has been made using the EPRI open source, made the VEN system was created attacker linked on. This configuration network was analyzed for vulnerabilities on various attacks that may be possessed by the VTN system. [16, 17]

3.2 Parameter Modulation Vulnerability Analysis

In the method for vulnerability analysis of parameters modulation of openADR, parameter values modulation (case1), parameter type modulation (case2), was subjected to attack separately in the process of the parameter buffer overflow modulation (case3).

The parameter value modulation method, were performed for the case of out of the range of values defined by openADR protocol standard. It was also performed for the case to respond with Response with modulated value or ID of Request values. Parameter type of modulation method was carried out vulnerability analysis by modulating the type of each parameter that is defined in the openADR protocol standard such as an integer; float, double, string, Parameter buffer overflow modulation method was performed modulated to exceed the maximum value that can be held by the parameter type such as the maximum value of the integer, the maximum value of the double , the maximum length of string (the buffer).

<Table1> is a table summarizing the results of an analysis of the parameter modulation vulnerability for each Ei Register Party, EiOpt, EiEvent, Ei Report Service provided by openADR. Depending on the service, to distinguish payload types possible the Message, running case1 from case3 attack above, it summarizes the analytical results. In addition, for a variety of parameters of the payload portion of the oadrDistributeEvent in EiEvent service a variety of parameters exist, and more fragmented, a summary of the analysis result of the execution of the attack in <Table2>. The results of vulnerability analysis for the parameters modulation attacks openADR, as if they were displayed in the <Table2> and <Table1>, most of the parameters showed a parameter value, type, weak results in overflow modulation attack. <Table1> and <Table2> in the "○" displayed items can attack, in other words indicating that the vulnerability exists. openADR system under attack was not detected by the parameter modification. As a result, system malfunction has occurred or a situation where the process is down.

Table 1. Vulnerability Analysis Results of openADR Parameter

Service	Message	case1	case2	case3
EiEvent	oadrDistributeEvent/oadrCreatedEvent/ oadrRequestEvent/oadrResponse	○	○	○
EiRegisterParty	oadrQueryRegistration/ oadrCreatedPartyRegistration/ oadrCreatePartyRegistration/ oadrCancelPartyRegistration/ oadrCanceledPartyRegistration	○	○	○
	oadrRequestReregistration	X	X	X
EiOpt	oadrCreateOpt/oadrCreatedOpt/oadrCancelOpt/ oadrCanceledOpt	○	○	○
EiReport	oadrRegisterReport/oadrRegisteredReport/ oadrCreateReport/oadrCreatedReport/ oadrUpdateReport/oadrUpdatedReport/ oadrCancelReport/	○	○	○
	oadrCanceledReport	X	X	X

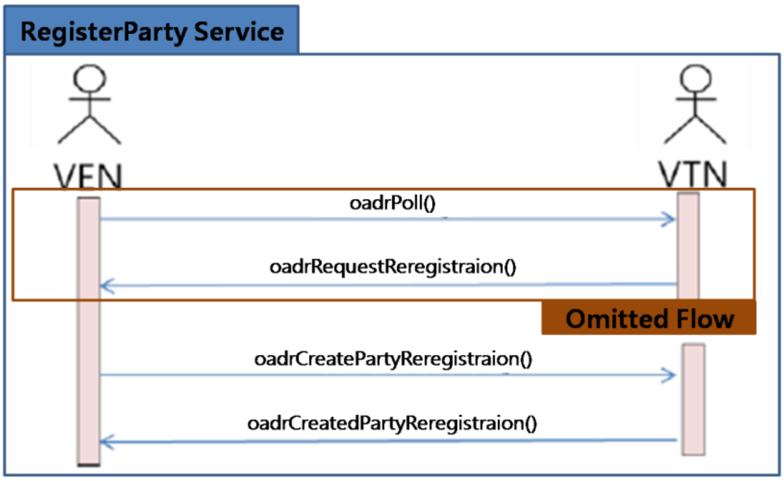
Table 2. Vulnerability Analysis Results of oadrDistributeEvent Parameter

Service(payload)	Message	case1	case2	case3
EiEvent (oadrDistributeEvent)	requestID/vtnID/ venID/eventID/ signalID/groupID/ marketContext/ testEvent/ vtnComment/ duration/ startafter/signalName/ resourceID/ responseCode/ text	○	○	○
	modificationNumber/ priority responseDescription	○	X	○
	createdDateTime/ date-time/ value	○	X	X
	eventStatus/ signalType/ partyID oadrResponseRequired/	X	X	X

3.3 Service Flow of Vulnerability

For vulnerability analysis of openADR service flow, and attack using the other terminal or hacked VEN and VTN system on the VEN and VTN system during normal operation. In order to analyze the vulnerability, omitting some Transaction in the Transaction required for each RegisterParty, Event, Report service, tried to attack how to change the Transaction of the order.

In [Figure.3], it was omitted Transaction flow to "oadrRequestReregistration" Response to "oadrPoll" Request between the VEN and VTN in RegisterParty(EiRegisterParty) service. After this, it is determined that the VEN registration Requset "oadrCreatePartyRegistration" a normal message, VTN was able to check the security of vulnerability to respond in a normal registration confirmation response "oadrCreatedPartyRegistration".


RegisterParty Service
VEN
VTN
oadrPoll()
oadrRequestReregistraion()
Omitted Flow
oadrCreatePartyReregistraion()
oadrCreatedPartyReregistraion()

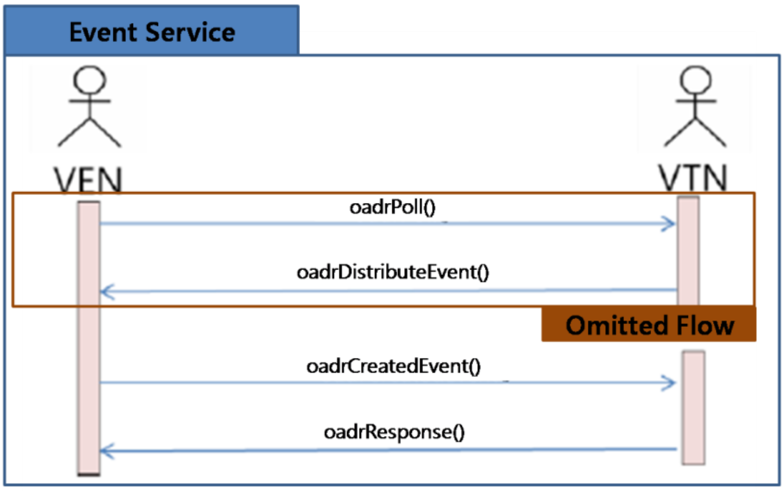
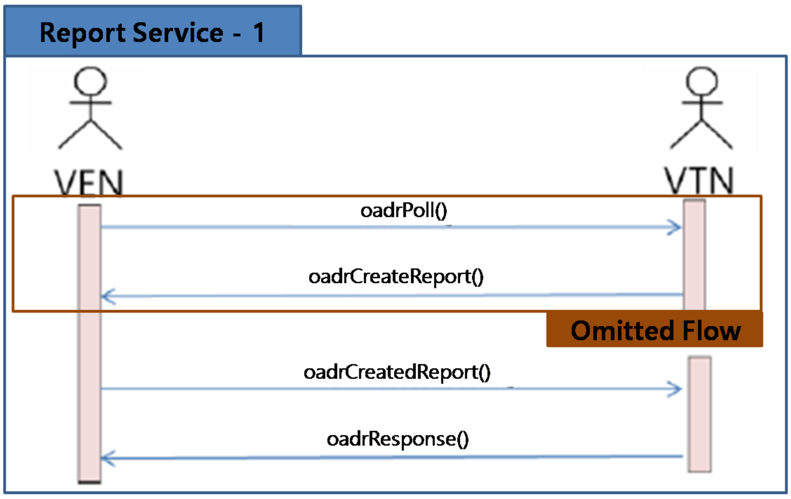


Figure 3. Vulnerability Analysis of Service Flow Modification Attack (case 1)

At [Figure. 3], it was omitted Transaction flow to "oadrDistributeEvent" Response to "oadrPoll" Request between the VEN and OTN in the Event (UiEvent) service. After this, a little modulation of the Event Request of VEN, "the transmission of oadrCreadtedEvent" message, VTN server, usually the Event acknowledgment "were able to confirm the vulnerability to respond with oadrResponse".Depending on the value of parameter "oadrCreadtedEvent" message, in Event services, in both cases the generation and cancellation of the Event is partitioned, it was possible to verify the vulnerability.



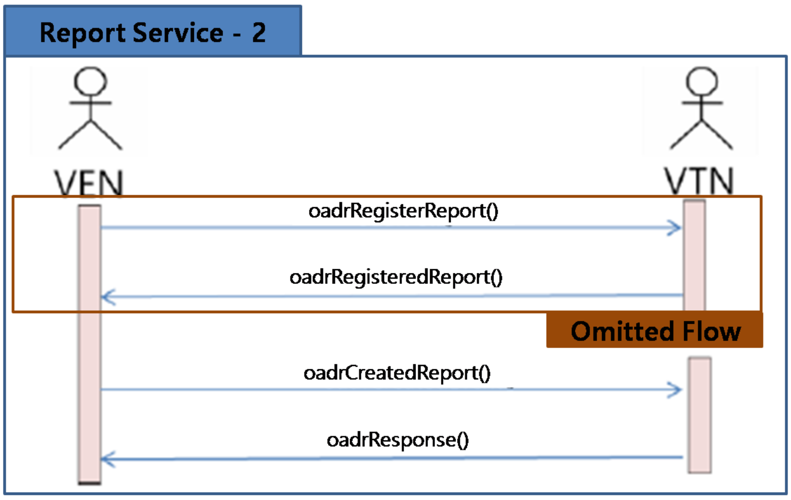


Figure 4. Vulnerability Analysis of Service Flow Modification Attack(case 2)

In [Figure. 4], it was omitted Transaction flow to "oadrCreateReport" Response to "oadrPoll" Request between the VEN and OTN in the Report (Ei Report) services. After this, it was possible to confirm the vulnerability to respond with recognized by VTN the Report Request "oadrCreadtedReport" of VEN to normal Request Report acknowledgment "oadrResponse ". In [Figure 4], it was omitted Transaction flow to "oadrRegisteredReport" Response to "oadrRegisterReport" Request between the VEN and OTN in the Report (Ei Report) services. After this, it was possible to confirm the vulnerability to respond with recognized by VTN the Report Request "oadrCreadtedReport" of VEN to normal Request Report acknowledgment "oadrResponse".

4. Method of Overcome Security Vulnerability

In this paper, we propose a security feature that has specialized openADR protocol services to complement the vulnerability of openADR attacks that were analyzed in Chapter 3 in the following manner

4.1 Detection and Block the Function of an Abnormal Message

In order to syntax error is cut off by detecting the abnormal power DR messages to induce such malfunctions in power DR system in the cause, you must be satisfied following requirements. openADR 2.0 b Profile Specification defines the openADR protocol schemas, sample payload, PICS protocol message.

1) openADR 2.0 b Profile Specification must be detected and blocked for power DR message with the header and body that does not match the format specified in the message. Header what essential items does not correspond to the message format are missing or header configuration means, such as if different from openADR protocol.
2) openADR 2.0 b Profile Specification must be detected and blocked power DR message with the specified message is outside the normal range of field values. Field values outside the normal range means the input of invalid numbers or addresses, Buffer Overflow, such as inserting malicious code.
3) openADR 2.0 b Profile Specification must be detected and blocked Power demand response message with a body that does not match the format specified in the message.

4.2 Detection and Block the Function of Abnormal Flow Message

In order to detect and block the normal Flow message it must meet the following requirements.

1) It must detect and block messages transmitted from another subject than the power DR parties.
2) It must detect and block messages that violate the order of dependency in accordance with the power DR agreement.

4.3 Detection and Block the Function of Abnormal Flooding Message

You must be satisfied following the requirements in order to detect and prevent openADR flooding attack.

1) The Flooding attack using conventional EiRegisterParty registration message to comply with openADR terms must be detected and blocked.
2) While the openADR registration is not made, it must be detected and block the Flooding attacks that use other messages.
3) Flooding attacks using the normal EiEvent, Ei Report, EiOpt message openADR to comply with the protocol must be detected and blocked.
4) After sending the EiRegisterParty, EiOpt message to large quantities any user must be interrupted to detect attempts session connection.

4.4 Network Access Control Function

Controls access demand response system that is not applied to the protected power demand response network, in order to separate from the internet, must satisfy following requirements.

1) It must be detected and blocked all access attempts using unregistered electricity demand response system to be protected.
2) Based on departure point / destination IP address., It must be controlled access to the message
3) Based on the starting / destination URL, It must be controlled access to the message.
4) It must provide a function capable of blocking the network communication protocol other than the power demand response protocol.

5. Conclusion

In this paper, the most reliable, were analyzed for vulnerability of the worldwide diffusion to have EPRI open source variety can have the VEN and VTN system was configured using the attack. As a result of the analysis, could be confirmed that the falsification open source openADR parameters have vulnerabilities. It also remains not recognized the anomaly service flow, was confirmed vulnerability normal processing. In this paper, we present the security functions openADR service specialized that the results of these vulnerability analyses can be used to complement the vulnerability of the original to openADR attack.

On the basis of a management network of power demand reaction in the smart grid network to open and two-way communication environment, it can be a variety of security incidents occur. With reference to the results of this paper, security when implementing openADR system to use and EPRI open source, or other open source, which is specialized in openADR standards and services that takes into account the vulnerability of the various attacks technology must be determined without fail.

References

[1] Hyun-Jae Kim, Sung-Han Jo, “A Study on Consumer Protections for the Introduction of Smart Grid”, the Journal of Digital Policy & Management, (2011).

[2] Ji-Hyun Kim, Suk-Jun Lee, Ki-Yoon Kim, Suk-Jae Jeong, “Evaluation and Facilitation of the Korean Smart Grid Market”, the Journal of Digital Policy & Management, (2013).

[3] Hyun-Jae Kim, Chan-Kook Park, “A Study on the Evaluation Criteria for the Performance of Smart Grid Pilot Projects”, the Journal of Digital Policy & Management, (2012).

[4] Hwajeong Seo, Howon Kim, "Network and Data Link Security for DASH7", Journal of Information and Communication Convergence Engineering, (2012).

[5] Hwajeong Seo, Howon Kim, "Zigbee Security Using Attribute-Based Proxy Re-encryption", Journal of Information and Communication Convergence Engineering, (2012).

[6] NIST Cyber Security WG, “smart Grid Cyber Security Strategy and Requirements”, (2010).

[7] Jae Jung Park, “DR (Demand Response) Technology for Smart Grid“, KERI, (2013).

[8] PIER, "Open Automated Demand Response Communications Specification (Ver. 1.0), (2009).

[9] W. M. Taqqali and N. Abdulaziz, “Smart Grid and demand response technology,” EnergyCon 2010 IEEE International, (2010).

[10] Jae Jung Park, DR (Demand Response) Technology for Smart Grid, KERI, (2013).

[11] openADR Alliance Website, http://www.openadr.org

[12] openADR 2.0 Profile Specification A Profile, openADR Alliance, (2011).

[13] Jimyung Kang, Implementation of openADR 2.0a Profile for Demand Response in Smart Grid, KERI, (2013).

[14] openADR 2.0 Profile Specification B Profile, openADR Alliance, (2013).

[15] openADR Open Source Toolkit: Developing Open Source Software for the Smart Grid, Charles McParland, IEEE Power and Energy Society General Meeting, (2011).

[16] Smart Grid Website, http://www.smartgrid.org.

[17] Certified EPRI Open Source openADR 2.0b VEN & VTN Website, http://www.openadr.org

Acknowledgments

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20151220100090).

Authors

June Kyoung, Lee
February 1995: Department of Computer Engineering of In-Ha University (Master of Engineering)
August 2000: LG Information & Communication Co.,Ltd Senior Researcher
July 2007-present: NAONWORKS Co,.Ltd CEO
Interest: Network, Convergence Security
E-Mail: darkelan@naonworks.com

Kyoung Hak, Lee
February 2007: Department of Electronics and Communication engineering of Kwangwoon University Ph.D
Present: Associate Professor of Kwangwoon University
Interest: VR, S/W Platform
E-Mail: goldbug@kw.ac.kr