ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(20), DOI:10.17485/ijst/2015/v8i20/79292 August 2015 ISSN (Online) : 0974-5645

Design of Prevent Quantification Model for APT Attack in Smart Meter

Donghyun Kim and Seoksoo Kim*

Department of Multimedia, Hannam University, Korea;
sskim0123@naver.com

Abstract

Recently, not only technological engineering techniques as well as social engineering have been applied to target attacks such as APT. The security system to prevent cyber-attack against smart meter must consider the smart meter environment and also apply cognition and behavior pattern of the attacker from both technical and social engineering perspective and quantified prediction of flexible and strategic cyber-attacks should precede it. Therefore, in this paper, a model was designed to quantify APT attack on smart grid in advance.

Keywords: Prevent APT Attack, Quantification Model, Smart Grid, Smart Meter

1. Introduction

Recently, the interest in smart meter, also known as an intelligent electrical grid, has been increasing due to the a result of planned blackout after the nuclear incident in Japan, increasing demand for electricity, spreading a sense of electricity crisis, environmental pollution and aging electricity system. Major countries around the world are actively conducting research to activate smart meter projects using smart grid[1].

Smart meter is the next-generation electrical grid that maximizes energy efficiency through real-time exchange of electricity-related information between the supplier and consumers by applying IT to existing unilateral electrical grid. It enables organic exchange of data between the smart grid center and various components of the smart grid, by changing the existing central communication method based on SCADA (Supervisory Control and Data Acquisition)[2] system to a direct connection based on the 1:N method, applying computer communication protocol and wireless communication technology.

As a result of convergence between various communication technologies and existing SCADA system, it offers more possibilities for convenience and expandability than existing electrical grid system and facilitates development and application of new technologies including remote control and automatic demand forecasting.

The cyber security paradigm in SCADA system applied to conventional electrical grids is designed in an exclusive environment independent from the outside. Conventional electrical grid control system based on this paradigm relies on physical security and does not fully consider software security[3].

However, the smart meter is interconnected with the external network through various routes, which can cause many security loopholes[4].

Recently, not only technological engineering techniques but also social engineering have been applied to target against attacks such as APT (Advanced Persistent Threat)[5]. Major national industry facilities such as the nuclear generating station, internet companies such as Google and Yahoo, as well as security firms such as EMC/RSA have been helplessly attacked, thus the growth of concern and interest in cyber security is rising.

Particularly, Stuxnet attack showed how the control facility can be paralyzed and even physical facility can be destroyed from the digital I&C system infection of the exclusively designed nuclear power system.

To improve security of smart meter against cyber-attacks, it is necessary to fully understand security vulnerabilities of the system and network composed

* Author for correspondence

of smart meter, evaluate the threat and risk of those vulnerabilities and build a response system that provides alarm step-by-step[6].

Security institutions and firms perform evaluation to suggest risk levels regarding worm, virus, security vulnerabilities or hacking methods, and sends alarm or warns users according to the levels.

However, these risk levels are merely based on quantified risk calculation and actual prediction is not possible due to lack of quantified prediction system.

Also, because the main purpose of smart network is to standardize message exchange among different electrical devices to control and automate the components and therefore, show very different characteristics and structure from general computer networks. Moreover, most of the terminal devices of smart grid are in the IED (Intelligent Electronic Devices) form, with significant technological and performance differences from standardized computers and there are various connection forms among the devices by a large scale. For those reasons, the pre-quantified method against cyber-attack is inadequate.

The security system to prevent cyber-attack against smart meter must consider the smart meter network environment and also apply cognition and behavior pattern of the attacker from both technical and social engineering perspective and quantified prediction of flexible and strategic cyber-attacks should precede it.

Therefore, in this paper, among the 6 steps of APT attack, the first step Intelligence Gathering, second Point of Entry and third Command and Control (C&C) communication are defined as smart meter network security steps to prevent cyber-attack in order to prevent social engineering APT attack to smart meter control system and threats to network are classified and quantification model designed.

2. Related Works

2.1 Security Standard of Smart Grid

IEC 62351[7] is a security technology standard designated and distributed by IEC TC57 WG15 for smart grid electrical system management and data communication based on grid standardization roadmap of SG3. So far, IEC 62351 Part1 to Part 8 has been published and currently Part 9-11 is being standardized.

Through guideline interagency report 728 for Smart meter cyber security[8], it describes framework and strategy for cyber security risk management, privacy protection and smart grid logic, interface analysis and AMI (Advanced Metering Infrastructure) security requirements, including security requirements for smart grid.

61850 and GB/T2239[9] is technical specifications related to data modeling, report system, fast transmission of events, group setting, sample data transmission, are defined by the substation automation standard including IEC 61850-9. GB/T2239[10] is a Chinese national standard defined by the State Grid association and contributes to reducing the costs and risk of equipment at the high-voltage substations.

SG17 of ITU-T developed X.1111-X.1114[11], a network security standard that can be used in the home area within the smart grid is working on standardization of security threat, requirements and functional structure in the smart grid service section.

These smart grid security standards do not include prompt measure against vulnerabilities based on evaluation of security threat and ISO/IEC 25408 standard is to show security levels and therefore, is different from security threat evaluation that is to numerically show security threat to the system.

2.2 Common Vulnerability Scoring System

CVSS (Common Vulnerability Scoring System)[12] is an international industry standard that evaluates vulnerabilities of network system environment through objective and formalized procedure based on systematically classified values in complex system environment. CVSS is composed of three metrics.

CVSS must refer to vulnerability database such as CVE (Common Vulnerabilities and Exposures) and NVD (National Vulnerability Database) to express vulnerability in scores. Therefore, it is very difficult to quantify vulnerability through CVSS if there is no basis in the relevant database. However, because network vulnerability is not static and new vulnerabilities can be found, CVSS vulnerability calculation does not provide smooth response to new vulnerabilities and is very difficult to apply due to many differences with general PC-based networks in data, hardware function and protocol.

3. Quantification Model in Smart Meter Security for APT Attack

3.1 Abbreviations and Acronyms

In general, network threats are classified as malicious

codes such as worm and viruses, security vulnerabilities and hacking techniques. Malicious codes are the major cause of cyber-attack and threat to network, and refer to all programs with malicious purpose of installing without the user's consent and threatening the data or system.

In the early days, malicious codes mostly took the form of virus that destroys the system, but, recent attacks use a social engineering technique that arouses users' curiosity and induces their access.

APT attack, which applies a social engineering technique, has high flexibility and strategy and is detected less than 10% depending on the characteristics of the attack.

APT attacker collects information for system invasion and uses the information to form rapport and disguise. Once it is successfully disguised, it performs manipulation that is related to technical threats and social-engineering technique[13].

Figure 1. APT attack process.

The manipulation commands an action to obtain authority from the targeted system (exploit, shell-code).

Malicious codes find other computers in the network and send exploit through the network, attacking vulnerability, transmitting shell-code and obtaining control authority, before self-replication.

Since malicious codes have characteristics like early infection, obtaining system information of the target, and transmission and execution of worm and virus, in the preparation stage, it clearly contains social engineering techniques.

Therefore, in this paper, among elements that can occur in the quantification stage for prevention of APT attack, data collection, rapport, manipulation and derivation were classified as social-engineering threats and exploit and shell code as technical threats to the network and theoretical analysis was performed.

3.2 Classification of Risk Score

Risks for preliminary quantification of APT attack are derived from hazard potential and context frequency based on time characteristic.

Preliminary Risk(R) = Hazard Potential(A) + Context Frequency(B) (1)

Therefore, the overall risk based on hazard potential and context frequency is as follows:

Table 1. Total risk

Context Frequency / Hazard potential	High Score	Middle Score	Low Score
High Score	High Risk	High Risk	Middle Risk
Middle Score	Middle Risk	Middle Risk	Low Risk
Low Score	Low Risk	Low Risk	Low Risk

In this paper, potential threats were listed and context frequency derived according to passage of time. Also, based on risk evaluation standard (ICSS-V) with experts regarding hazard potential and context frequency, quantitative scoring was performed through qualitative analysis.

3.3 Composition of Quantification System

In this paper, according to research on correlation with existing threats, preliminary risk (R), hazard potential (A) and context frequency (B) were established as shown in the following equation, in which I and J represent the number of variable items added or subtracted, k the number of specific threats, and n threats.

Hazard Potential (A) = Score A x 0.25 (2)

Context Frequency (B)=Score B x 0.75 (3)

$$R = \sum_{i=1}^{k} A_i + \sum_{j=1}^{n} B_j \quad (4)$$

In this paper, derived preliminary risk, hazard potential and context frequency was defined as basic quantification system and the algorithm for preliminary threat alarm model has been designed as follows in the following order.

Table 2. Quantitative distribution

Threat Classification	Threat	Details Threat			Hazard Potential (25%)	Context Frequency (75%)
Social Engineering Threat	Information Gathering (4)	Specific Information			2	4
		Basic Information about the System			1	
		Other			1	
	Rapport (10)	Spam			2	10
		Phishing			2	
		File Name			2	
		Direct Contact			2	
		Other			2	
	Deduction (20)	Attack Code Use			2	20
		Remote Available			3	
		Operating System Services			3	
		Application Service			3	
		Account			5	
		Other			4	
	Pretexting (30)	Attack Code Use			5	30
		Remote Available			5	
		Operating System Services			5	
		Application Service			5	
		Account			5	
		Other			5	
Social Engineering Threat + Technical Engineering Threat	Manipulation (36)	Exploit	VIRTUALIZATION	White List Frequency	1	15
				Black List Frequency	4	
				Other Frequency	10	
		Shell code		White List Frequency	1	15
				Black List Frequency	4	
				Other Frequency	10	
		Other		Inclusion of Dormant Code	2	6
				Inclusion of Self-deleting Code	2	
				Inclusion of Device Driver	2	
Total					**Score A**	**Score B**

Algorighm for preliminary threat alarm model.

- Social-engineering-based threats perform characteristic analysis of each specific element.
- Technical threats analyzes only characteristics related to manipulation.
- The social-engineering-based threats that finished characteristic analysis examines hazard potential and context frequency through frequency analysis.
- Technical threats that finished characteristic analysis (manipulation) classify registered and unregistered signatures through virtualization.
- After finishing signature classification, it performs frequency analysis to for the inclusion of code and driver.
- Hazard potential and context frequency of technical threats (manipulation) is analyzed.

- After finishing analysis of hazard potential and context frequency, real-time monitoring is performed based on aggregated preliminary risks.
- If the preliminary risk exceeds a risk level, virtualization analysis is performed to check whether threat is included.
- If a threat element is included, it is registered in DB and the alarm level is determined.
- After the alarm level is determined, preliminary alarm is sent according to the determined level.

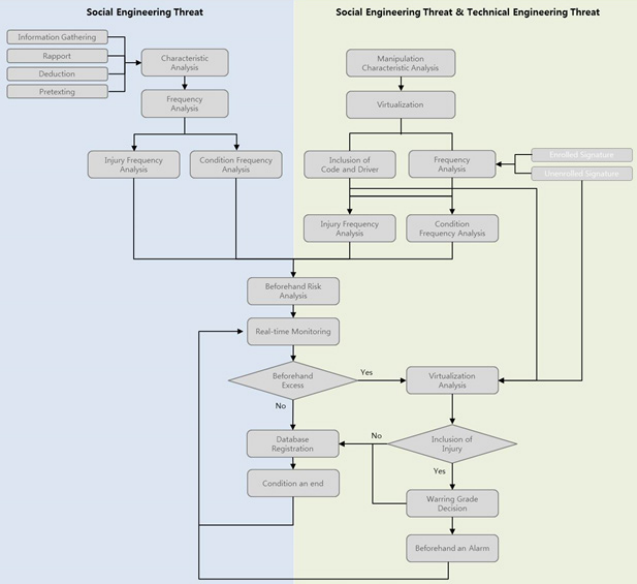

Figure 2. Algorighm for preliminary threat alarm model.

4. Conclusion

In this paper, a model was designed to quantify APT attack on smart meter in advance. The quantification model designed enables new system for realistic security evaluation of networks composed of smart meter. By applying social engineering to security engineering analysis and proposing objective quantification guideline for prevention, instead of relying on subjective opinions of security experts.

Also, using analytic hierarchy process through score allocation and weight calculation for different threats, it can be used as more objective evaluation criteria by verifying and deriving score criteria for different specialized institutions based on consistency ratio, comparative matrix and characteristic value.

However, as it is limited to deduction result, in preliminary quantification, context frequency 1 results in low risk, but if the relevant context frequency 1 is a strategic APT attack that includes both social engineering-based and technical threats, the preliminarily quantified risk can be different from the actual context. To solve this problem, future research may look into detection algorithm that allows strategic APT attack in low context frequency to build more accurate preliminary quantification system.

5. Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2006026).

6. References

1. Amin SM, Wollenberg BF. Toward a smart grid : power delivery for the 21st century. IEEE Power and Energy Magazine. 2005; 3(5):34–41.
2. Lakhoua MN. Application of function analysis on a SCADA system of a thermal power pant. Advances in Electrical and Computer Engineering. 2009; 9(2):90–8.
3. Oman P, Schweitzer E, Roberts J. Safeguarding IEDs, substations, and SCADA systems against electronic intrusions. Proceedings of the 2001 Western Power Delivery Automation Conference; 2001. p. 9–12.
4. McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. IEEE Security and Privacy. 2009; 7(3):75–7.
5. Dell SecureWorks. Anatomy of an Advanced Persistent Threat (APT). 2012.
6. Jongbin K, Seokjun L, Taeshik S. Security threat evaluation for smartgid control system. Journal of The Korea Institute of Information Security and Cryptology. 2013; 23(5):873–83.
7. Power systems management and associated information exchange – data and communications security – part 10: security architecture guidelines. IEC 62351-10; 2012.
8. NIST frameworks and roadmap for smart grid interoperability standards release 2.0. NISTSP 1108; 2012.
9. Communication networks and systems in substations part 7-1: basic communication structure for substation and feeder equipment- principles and models. IEC 61850-7-1; 2011.
10. Chinese national standard, information security technology-basic requirements of GRADE protection of information system security. GB/T22239-2008; 2008.
11. IT SERIES X: Data Networks. Open System Communications And Security. ITU-T; 2007.
12. Mell P, Grance T. Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme. NISTSP 800-51; 2002.
13. Sungmo J. Global network security system to prevent cyber attacks [PhD Thesis]. Hannam University; 2014.