INFORMATION SECURITY MANAGEMENT IN IRANIAN SMART METERING PROJECT (FAHAM)

Meisam Rezaeian
Iran Energy Efficiency Organization (IEEO) – Iran
rezaeian@saba.org.ir

Nader Salek Gilani
Iran Energy Efficiency Organization (IEEO) – Iran
salek@saba.org.ir

Hadi Modaghegh
Iran Energy Efficiency Organization (IEEO) – Iran
modaghegh@saba.org.ir

ABSTRACT

In the recent years with the development of information systems and computer applications, information security has gained special attentions. Due to the implementation of Advanced Metering Infrastructure (AMI) in the near future, the electricity distribution companies will be able to remotely manage and monitor their customers through these systems and also all customers are able to interact with these companies. The main issue is providing security of smart metering system and how to manage and secure data exchange that directly undermine the vital activities of system. Therefore, with reasonable investment in information security and implementing an Information Security Management System (ISMS) with appropriate security mechanisms benefited from increasing system reliability, business continuity, reducing threats and their effects and enhancing customer satisfaction alongside other main benefits of smart metering systems. In this paper we discuss information security issues in smart metering systems including threats, security services and mechanisms to deal with system risks and in particular, the proposed security solutions and schemes in Iranian Smart Metering Project (FAHAM) are presented.

Keywords*—Information Security; Smart Meterig Systems; Information security management System; Risk Management; Security Operations Center; Iranian Smart Metering Project (FAHAM);*

I. INTRODUCTION

Information Security (InfoSec) is called to protect all forms of data (electronic, physical, etc…) against unauthorized access, abuse, disclosure, disruption, modification, recording and destruction. Information security is established with the aim of ensuring continuity of current operations, minimizing the risk, increasing trends and rate of investments.

The history of information security begins with the history of computer security. In World War II, the first mainframe computers were developed to break the security codes. At this time, security requirements are summarized in the protection of places, devices and applications from external threats and this technical perspective of security was raised to the early 1980s [1]. After years it became clear that most of security penetrations occurred according to weaknesses in security management and lack of security training of personnel.

Since the mid-80s to mid-90s, issues related to information security management policies and organizational structures were proposed. These security plans were completed gradually in the mid-90s with combination of the two previous stages and other parameters to implement security policies and mechanisms based on the needs of the organization. This stage includes activities such as the standardization of information security, international licenses and cultural background in the organization and evaluates information security measures permanently and dynamically. This process continues and is being completed [2]. Today, millions of insecure computer networks are connected together via the Internet. With increasing cyber attacks, governments and companies have to protect computer systems in utilities and other vital infrastructures.

The Smart Grid is a next-generation electrical power system that is typified by the increased use of Communications and Information Technology in the generation, delivery and consumption of electrical energy [3]. Smart Grid facilitates control and monitoring of all equipments that can be connected to the grid [4]. Data, commands and requests are exchanged between Central Access System (CAS), smart meters and other smart equipments by Advanced Metering Infrastructure (AMI) at the consumer level in distribution networks. There are security concerns in smart metering systems as well as other information systems. For example, with taking inappropriate security policies and mechanisms, consumption data measured by the meter is tampered or eavesdropped by hackers to discover when consumers are present in their homes. Another issue is cyber attacks to information and telecommunication networks and disconnecting of a large number of consumers and subsequently the energy and load balancing of the whole electrical network is affected. So it seems necessary to take appropriate security mechanisms for dealing with potential security threats of using smart meters.

Section II introduces in Iranian Smart Metering Project (FAHAM). In section II, Information security management system and one of the conventional standards for implementation procedures of this system are described. Also, risk management plan for FAHAM assets and contingency planning for FAHAM services are presented. Section IV describes another most important security control that used for incident security response in Iranian Smart Metering Project (FAHAM) and finally, conclusions is presented.

II. IRANIAN SMART METERING PROJECT (FAHAM)

The deployment of smart grid in Iran started with smart meter rollout and implementation of AMI pilot projects at December 2011. Iranian Smart Metering Plan (FAHAM) was funded by Ministry of Energy (MOE) of Iran and under the supervision of Iran Power Generation, Transmission and Distribution Management Company (TAVANIR). Implementation and development of FAHAM has been assigned to SABA (Iran Energy Efficiency Organization, IEEO) as a project manager from TAVANIR.

In the first phase of this project, about one million smart meters will be installed in five separate areas including central, south east, south west, north west and north east that as shown in Fig. I. Five selected local distribution companies (LDCs) in these areas are Tehran, Bushehr, Ahvaz, Zanjan and Mashhad respectively. At the second phase, implementation and deployment of smart metering includes MDM, system applications and WAN communication infrastructure will be done for all of consumers. Also the specification of data modeling and communication interfaces will be finalized, so the producers will be able to product interoperable smart meters for the utilities individually [5].

Fig. I. Five Areas of FAHAM Project

There are business benefits of AMI implementation in Iran which are mentioned below [6].

- Improvement of customers' energy consumption profile
- Applying energy management by the network operator in normal and critical conditions
- Improving meter readings and billing processes
- Reducing non-technical losses as well as monitoring technical losses in the distribution network
- Improving quality of services and power quality like reducing the duration of outages and number of interruptions.
- Developing distributed generation and clean energy usage
- Possibility of electricity pre-sale and establishing electricity retail markets
- Optimizing operation and maintenance costs
- Providing appropriate management of water and gas meters

III. INFORMATION SECURITY MANAGEMENT

Information is considered as an important and valuable asset to any organization and therefore security mechanisms are necessary to keep them safe and secure. Information Security Management System (ISMS) is a set of policies and planning activities, responsibilities, processes and security mechanisms that are used to manage organization's sensitive data. ISMS provides standards for immunization of cyberspace to establish, implement, operate, monitor, review and improve information security plans that are specified to the organization.[7] By providing the information security management standard in 1995, a systematic approach was formed to immunization of information technology systems. According to this approach, implementation and maintenance of information security management system is a continuous process according to the Deming cycle that consists of four stages including Plan, Do, Check and Act which is known as PDCA cycle.

A. Information security management system standards

The ISO/IEC 27000-series (or ISMS Family of Standards) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS) [8]. ISO/IEC 27005 provides guidelines for information security risk management (ISRM) in an organization, specifically supporting the requirements of an information security management system defined by ISO/IEC 27001. ISO/IEC 27001:2005 is a risk based information security standard that the risk management process fits into the PDCA model. However, the latest standard, ISO/IEC 27001:2013, does not use this cycle.

Table I. Alignment of ISMS and information security risk management process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

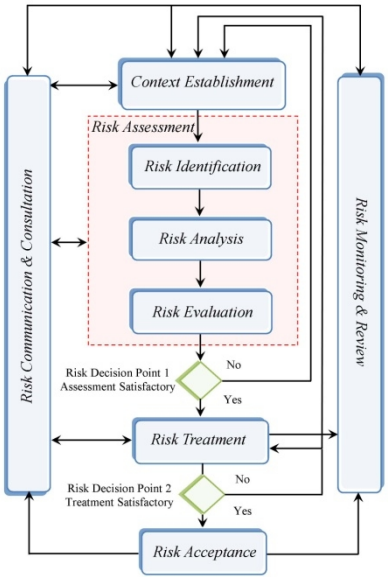

Fig. II. Information Security Risk Management Process [9]

B. Information security risk management process

Risk management (RM) is a comprehensive & continuing process to identify, analyze, evaluate, monitor and reduce risks of some business activities and processes to an acceptable level. To reduce risks, mechanisms & controls will be determined using the results of risk assessment and technical, economical, social and political requirements of organization. Table 1 summarizes the information security risk management process in accordance with PDCA cycle of the ISMS. The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation and risk monitoring and review. Fig. II illustrates the information security risk management process can be iterative for risk assessment and risk treatment activities.[9]

C. FAHAM Security Team

In order to develop a risk management plan and a business continuity plan of FAHAM project, a team of experts with relevant specialty in electrical, telecommunications, computers(hardware & software) , information technology and cryptography was formed and many sessions conducted continuously to identify the assets, determine risks associated and provide necessary controls for reducing risks that are addressed. The core of this team consists of some fixed members and varied members that the varied members depending on the needs of project will be added to it from stakeholders and related organizations.

D. Risk Assessment & Risk Treatment Plan in FAHAM Project

The Scope of FAHAH project is bounded to local distribution company area and consists of residential, commercial, agricultural, industrial, street lighting and public customers. At first, the key concepts is described that used in the risk assessment.

1) Key Consepts

The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security. There is continuous debate about extending this classic trio. [2] Other principles such as authentication, authorization, Non-repudiation and accountability have sometimes been proposed for addition.

Threat

A threat is the potential of human or natural agent that can be harm the assets of organization such as information, processes and etc with exploiting of their vulnerabilities. Threats may be deliberate, accidental or environmental and can be identified generically and by type (e.g. physical damage, natural events, unauthorized actions, technical failures, compromise information and functions).

Vulnerability

Vulnerability is a weakness of one asset or a group of assets that can be exploited by one or more threats. Vulnerabilities are classified according to the asset class that are related to hardware, software, network, personnel, site and organizational. For example insufficient software testing and lack of audit trail related to software and also unprotected communication lines and insecure network architecture related to communication.

2) Risk assessment method

In FAHAM project used risk assessment is performed based on the ISO/IEC 27005 and risk is calculated by:

Risk= Asset Value × Vulnerability × Threat

Asset Value is sum of consequences caused by violation of security services including confidentiality, integrity and availability (CIA). Consequences are considered on financial, reputation and interruption of power supply caused by violation of any security services. OWASP Risk Rating Methodology introduces some factors for estimating vulnerability severity level & likelihood of threat. The threat agent factors are used to estimate the likelihood of a successful attack that occurred in worst case. Also vulnerability factors are used to estimate the likelihood of the discovery and exploit of particular vulnerability. These factors are optimized for FAHAM Project and presented in TABLE II & III.

Table II. Vulnerability Factors

Severity	Level	Factors			
		Ease of discovery	*Ease of exploit*	*Awareness*	*Intrusion detection*
1	**Very Difficult**	Practically Impossible	Practically Impossible	Unknown Vulnerabilities	Active Detection
2	**Difficult**	Lack of Similar Experience	Lack of Similar Experience	Known Vulnerabilities & No	Logged & Reviewed

Severity	Level	Factors			
		Ease of discovery	***Ease of exploit***	***Awareness***	***Intrusion detection***
				Information	
3	**Medium**	Existance of Similar Experience	Existance of Similar Experience	Known Vulnerabilities with Limited Information	Selective Logged & Reviewed
4	**Easy**	Access to Semi-Automated Tools	Access to Semi-Automated Tools	Known Vulnerabilities with Complete Information	Logged Without Review
5	**Very Easy**	Access to Full-Automated Tools	Access to Full-Automated Tools	General Knowledge of Vulnerability	No Intrusion Detection Mechanism

Table III. Treat Agent Factors

Severity	Level	Factors			
		Skill level	***Motive***	***Opportunity***	***Size***
1	**Very Low**	No Technical Skills	No Reward	Full Access & Expensive Resources Required	Developers
2	**Low**	Some Technical Skills	System Disturbance	Full Access Required	System Administrators
3	**Medium**	Advanced Computer Users	System Disturbance & Some Rewards	Special Access Required	Intranet Users
4	**High**	Network And Programming Skills	High Rewards	Typical Access Required	Authenticated Users
5	**Very High**	Security Penetration Skills	Public Disturbance	No Access & Resources Required	Anonymous Internet Users

The important step before risk analysis and after establishing the context is risk identification. The purpose of risk identification is to collect input data for the risk analysis activity and to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen. Risk identification includes five steps: identifying of assets, identifying of threats, identifying of existing controls, identifying of vulnerabilities and identifying of consequences. Output of identification of assets is a list of assets and the business processes related to these assets. Assets in FAHAM project are divided into several categories including hardware, software, network & communication, documents, personnel, site and organizational that presented with more details in Table IV.

Vulnerabilities related to each asset have been extracted using Annex D of ISO 27005 and Chapter 6 of NIST IR-7628 based on the nature, environment and performance of assets. After determining the vulnerabilities, the level of each vulnerability associated with each asset are determined based on vulnerability factors in Table II. A threat has the potential to harm assets such as information, processes, systems and organizations. Threats related to each vulnerability are extracted using Annex C & D of ISO 27005.

After finishing the risk assessment, Risk Treatment Plan (RTP) is developed and determines general risk treatment options and required actions and controls to reduce the risk to an acceptable level. Also a Statement of Applicability (SOA) is prepared and implemented by suppliers. As mentioned before, these processes can be iterative for risk assessment and risk treatment activities.

Table IV. FAHAM Assets

Categories	Assets			
Hardware	Database Server, AHE Server, Web Server, Hardware Firewall	Smart Meters: CT (3φ), CT/PT (3φ),Direct Current (3φ), Household(1φ). Data Concentrator(DC)	IHD, HHU	Flash Memory, CD/DVD, Printers, Scanners, Laptops, Telephone & Fax
Software	Server O.S., User O.S., Active Directory, Software Firewall, Antivirus	System Applications (MDM,DMS, CIS, DRMS, GIS,OMS BS,PMS,SLM)	Meters' Firmware, DC's Firmware	Application Softwares
Network & Coms.	Data Communication Service, Router, Switch, Ethernet	GPRS Interface, PLC Interface	GPRS SimCard	Wireless Modem, Office Phone & Fax
Docs	System Design Requirement, System Design, Security Design, System Test Reports	Guidelines and Procedures, Contracts, Operating Instructions, Installation And Replacement Instructions	Installation and Replacement Forms, Update Forms, Data Collection Forms	Emails
Personnel	Administrators of MDM,DMS, CIS, DRMS, GIS,OMS BS,PMS,SLM Software	Administrative Assistants of MDM,DMS, CIS, DRMS, GIS,OMS BS,PMS,SLM Software	Power Users of MDM,DMS, CIS, DRMS, GIS,OMS BS,PMS,SLM Software	Normal Users of MDM,DMS, CIS, DRMS, GIS,OMS BS,PMS,SLM Software
Site	Server Room in Regional Distribution Companies, Server Room in Distribution Companies	Documents Rooms, Staff Rooms in Regional Distribution Companies	Panel Installation of smart meters (Direct, 1φ), Panel Installation of 3φ smart meters (CT, CT/PT), Panel Installation of DC	Earthing System, UPS System, Air Conditioning System, Fire Suppression System, Security Systems
Org.	Experts & Managers in Employer Org.	Experts & Managers in Executive Org.	Experts & Managers in Consultant Company	Experts & Managers in Contractor Companies

E. Contingency Planning in FAHAM Project

Contingency Planning (CP) is the program developed by organizational planners to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, both human and artificial. The main goal of CP is restoration to normal modes of operation with minimum cost and disruption

after an unexpected event. CP is included following components: Incident Response Plan (IRP), Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). IRP focuses on immediate response to an incident. DRP focuses on restoring operations at the primary site after disasters occur. BCP facilitates establishment of operations at an alternate site, until the organization is able to either resume operations back at their primary site or select a new primary location.
The first phase in CP process is Business Impact Analysis (BIA) that encompasses activities aimed at identifying, quantifying and qualifying the business impact and other effects of a mission-critical activity failure on an organization. The fundamental outcomes of the BIA are identification of mission-critical activities, financial and nonfinancial impacts of a disruption and identification of the minimum level of resources needed to accomplish the organization's business objectives in terms of an acceptable recovery time: Recovery Time Objectives (RTO) and an acceptable recovery status of assets: Recovery Point Objectives (RPO).

IV. SECURITY OPERATION CENTER & NETWORK OPERATION CENTERS

Similar other information systems in the world, Security Operation Center (SOC) with Security Incident Response Team (SIRT) and malware analysis laboratory are used for securing the Iranian smart metering system (FAHAM). Hierarchical Structure of SOC & NOCs is shown in Fig. III . SOC monitors the security incidents and defended the enterprise information systems such as web sites, applications, databases, data centers and servers from cyber attacks. Also, there are Network Operations Centers (NOCs) with Incident Response (IR) teams in each area that is specified in section II.

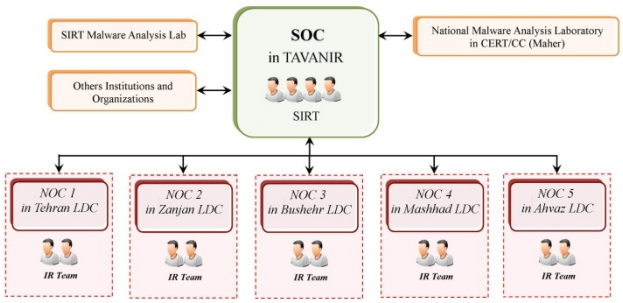

Fig. III. Hierarchical Structure of SOC & NOCs

Coordination and Security knowledge transfer between NOCs are conducted through a SOC in TAVANIR. SOC staff includes analysts, security engineers and SOC managers that are trained in computer engineering, cryptography and network engineering. NOCs are responsible for monitoring and maintaining infrastructure, resolve issues that could affect performance or availability and ensure uninterrupted network services. The Primary responsibilities of NOC include: network monitoring, incident response, communications management and reporting. IR team in NOC provides its services in three categories: Response, Prevention and Recovery.

CONCLUSION

In this paper, we discuss about main issues of information security management in smart metering systems including risk management, business continuity management and security incident response. Also, security mechanisms and controls in FAHAM project are presented. Information systems need consistent information management system with appropriate security mechanisms to deal with the risks of system. Best practices and solutions are used in FAHAM project basis of international standards and best practices on large project of the world. These mechanisms can reduce security risks and improve continuity of services and provide customers satisfaction.

REFERENCES

[1] M. E. Whiteman & H. J. Maltord, 2012, "Information Security: An Introduction, Principles of Information Security",4th ed. Boston, MA, Course Technology, pp. 3-7.

[2] M. Rezaeian,H. Modaghegh & N. Salek Gilani, Aug. 2013, "*Information Security in Smart Metering Systems*", Iran Energy Efficieny Organization (IEEO), Department of Smart Metering Systems & Smart Grid, Special Reports, No. 12, [Online] Available: http://www.iransg.com.

[3] "*What is the Smart Grid?*", [Online] Available: http://smartgrid.ieee.org/ieee-smart-grid.

[4] M. Shabanzadeh & M. P. Moghaddam, 2013, "*What is the Smart Grid? Definitions, Perspectives, and Ultimate Goals*", 28th International Power System Conference, Tehran, Iran.

[5] S. Jamal, Nov.2013, *Iran's smart grid deployment – from smart meter to overall system architecture*, [Online] Available: http://www.metering.com/

[6] *General, Economic, Functional, Technical & Communications Requirements of Iranian Smart Metering Project (FAHAM)*, Iran Energy Efficieny Organization(IEEO), Department of Smart Metering Systems & Smart Grid, Final Rep, Dec. 2011. [Online] Available: http://www.iransg.com.

[7] *Information Technology -Security Techniques - Information Security Management Systems - Requirements*, *ISO/IEC 27001:2005*, Oct.2005.

[8] *Information Security Standards* [Online]. Available: http://www.iso27001security.com/html/others.html.

[9] *Information Technology - Security Techniques - Information Security Risk Management, ISO/IEC 27005:2011*, 2011.