2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Smart Grid Wireless Network Security Requirements Analysis

Khaja Altaf Ahmed, Zeyar Aung, and Davor Svetinovic
Computing and Information Science
Masdar Institute of Science and Technology
Abu Dhabi, UAE
Email: {kahmed,zaung,dsvetinovic}@masdar.ac.ae

***Abstract*—Power grids are being enhanced by integrating the Information and Communication Technology (ICT) to make them more reliable, economic, efficient, and environmentally friendly. The integration of power grids with ICT to build Smart Grids (SGs) has reduced costs and improved their performances. But, on the other hand, this has also brought the cyber security threats as well. In traditional ICT systems, the end devices are the powerful systems which have high computation power and memory capacity to perform the intense computations to avoid cyber security threats, whereas most of the end devices in SG lack these capabilities. Incorporating the security in the early stages of SG development through systems security requirements engineering can reduce the potential cyber security threats. This paper presents the results of applying Security Requirements Engineering Process (SREP) on the SG wireless network, and proposes the potential solutions that can be implemented such as using Global System for Mobile Communication (GSM)-enabled Intelligent Electronic Devices (IEDs) with Global Positioning System (GPS) support.**

I. Introduction

The success of any system relies on effectively capturing the stakeholders' needs in requirements specification [1], [2], [3]. Some studies show that the cost of adding the requirements in later stages of the system development could be 10 to 200 times higher [4], [5]. Jones et al. [6] propose that, in most of the system development projects, fixing the requirements, design and code defects cost 40% to 50% of the total system development efforts. In addition, more than 50% of the defects originate during the systems requirements engineering; if not done properly it can seriously impact the system. Flaws in requirements typically cost 25% to 40% of the total project costs [7]. This highlights the importance of the requirements specifications as the vital step in the systems development lifecycle. Similarly, security requirements also have greater impact on the fault-free functioning of any system.

Security is a quality attribute of a system. Most of the times, the functional requirements are clearly defined, but non-functional or quality requirements are ignored or added later on. Reliability, availability and robustness of the system depend on how secure a system is. Like functional requirements, security requirements too should be incorporated from the early stages of the systems development lifecycle. It is strongly advised by security experts, e.g, [8], [9], to add security requirements in the initial phases of system development, yet, it is not the common practice in industry up till now. In recent times, we have seen many security breaches even in the presence of the robust and reliable ICT systems. For example, Sony Inc. had to shut down the Playstation network for more than a week. The breach compromised 77 million customers personal information records, including 12.5 million credit cards records [10]. To incorporate security requirements engineering in early stages of the system development, various methods and techniques are available such as [11], [12], [13], [14].

Smart Grid (SG) is capable of converting the present power grid to an intelligent and complete autonomous structure. Almost all aspect of the power grid, most of which are currently manually carried out, can be automated in SG. These include automatic demand response, power storage, distributed power generation and integration, grid control and electricity pricing, etc. ICT control systems take care of the complete control of SG. They require a constant information feedback from all the sources in SG in order to take automatic control actions. The information needs of the control system can only be achieved by a centralized and integrated communication system. Because of their cost and performance benefits, wireless networks form the core of SG communication systems. Some of the places where they are widely deployed include house-to-grid communications and intra-grid communications (for generation, transmission, distribution). Unfortunately, the wide deployment of wireless networks within SG poses significant cyber security threats. The nature of the threats requires a detailed and systematic analysis of security vulnerabilities through systems security requirements engineering methods.

To elicit systems security requirements, we use a security requirements engineering method called SREP (Security Requirements Engineering Process) [15]. These requirements could be used to deter potential security threats or vulnerabilities in SG and to reduce their impact on the overall system. Typically, any security solution should answer three basic questions: what to protect, against whom, and to what extent. SREP takes into consideration these security questions in nine steps. SREP 1) defines the system context; 2) identifies the critical and vulnerable assets which should be protected from attacks; 3) identifies the security objectives and dependencies; 4) identifies threats and vulnerabilities to the assets; 5) assesses risks and analyzes the impact and likelihood of the threats

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.153

and vulnerabilities; 6) elicits and categorizes the security requirements; 7) prioritizes the requirements based on the risk assessment; 8) inspects the requirements, and 9) improves the repository, if applicable.

The major contribution of this paper is the systematic application of the SREP to specify SG wireless network systems security requirements. It provides a step-by-step guide to apply SREP in SG domain. In order to evaluate the elicited systems security requirements, this paper proposes the systems integration of SG with the GSM and GPS networks. Integrating the GSM and GPS networks with SG wireless networks is a novel combination of already evolved and matured wireless communication systems. It is also a new direction for the SG system security solutions.

The remainder of this paper is organized as follows. Section II presents background and related work[1]. Section III presents the results of the study. Section IV presents evaluation and proposed solutions. Finally, Section V presents the conclusions.

II. Background and Related Work

Integration of the power grid with ICT systems to form a SG has brought a number of security challenges to power grids [16]. Through this integration, the power grid has inherent security risks due to the fact that the power grid and applications were not designed for the general ICT environment. To counter the impact of security issues that would arise in the power grid, the security should be incorporated from the requirements gathering phase during SG development. Currently, academic research focuses on either highlighting the possible threats [17], vulnerabilities [18], security issues [19], [20], [21], [22], and challenges [23], or recommending certain frameworks [24] and technologies to be used [22], [16], [25].

Wireless networks are a fast growing trend in ICT and they offer a lot of cost and performance benefits. Our analysis shows that the wireless communication can result in significant savings (see Figure 1). Wireless networks are widely deployed in SGs because of their advantages in cost, performance and ease of installation given the fact that SGs cover large land areas, difficult terrains and various geographic locations.

However, wireless networks add more challenges to the security issues faced by SG, as it can potentially expose the entire power grid to various cyber security threats because of the very nature of wireless communication, which is vulnerable to interception.

III. Results

SREP (Security Requirements Engineering Process) consists of nine steps. SREP itself acts as a research framework according to which SG wireless network security requirements specification was performed. Following are the results of applying SREP on SG wireless networks.

Step 1: Agree on Definitions. The best practice to conduct a study is to follow certain basic standards, definitions

[1]Background and related work section is shortened due to the page limit restrictions.

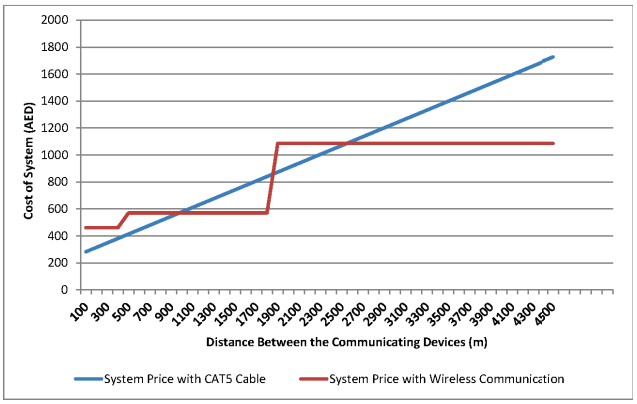

Fig. 1. Wired vs. Wireless Cost Analysis for Non-Line of Sight Link for a Micro-Hydro Project. (Note: AED means United Arab Emirates Dirhams. USD 1 = AED 3.67 as of April 2013.)

and terminology for the purpose of the consistency. Security requirements engineering and SG technology definitions in this research are extracted from international standards such as International Standards Organization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronic Engineers (IEEE). Some of the definitions used in this research are: ***Confidentiality*** is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (source ISO 13335-1:2004). ***Integrity*** is the property of safeguarding the accuracy and completeness of assets (source ISO 15489:2001 and ISO 13335-1:2004). ***Availability*** is the property of being accessible and useable upon demand by an authorized entity (source ISO 13335-1:2004). *Supervisory Control and Data Acquisition* (SCADA) software can be considered as part of the Energy Management System (EMS) application. The monitoring and control functions of the EMS application are performed by SCADA while the optimization functions are performed by remaining EMS [26]. *Home Area Network* (HAN) is a residential local network whose purpose is to communicate with the digital devices installed within a household [27].

Step 2: Identify Vulnerable and/or Critical Assets. The SG is controlled by an interoperated communication network and a distributed control system. The communication systems are thus considered to be the critical assets of the whole SG [28]. Similarly, the network operations are critical assets of SG because they handle all the aspects of grid information and control instructions. Every aspect of SG where wireless network exists is now a vulnerable asset. These two networks are prone to data theft or cyber attacks. Some vulnerable assets of SG are:

1) House-to-gird wireless data and control network
2) Intra-grid wireless data and control network (encompassing power generation, transmission, and distribution facilities)

The wireless network between a household and the grid refers to the connectivity between the Advanced Metering Infrastructure (AMI) and SG's control center, where the power

flow is monitored and recorded for various purposes as required by the stakeholders. Table I shows the vulnerable data that is communicated in this segment of SG network. This data is available within AMI at each household, and can be breached if the household to SG network is vulnerable to security threats.

V1	Number of appliances in a household
V2	Power and wattage nature of the appliances
V3	Ideal parameters and loading status of the appliances
V4	Threshold power values for the appliances
V5	Present load received at the household
V6	Present activeness of the appliances
V7	Secondary power (as distributed energy resources) storage information

TABLE I
DATA-RELATED VULNERABILITIES IN HOUSE-TO-GRID NETWORK.

The intra-grid network covers the communications among the various facilities of SG such as power generation, transmission, and distribution centers. It has two independent tasks to be addressed, namely, grid control and consumer data handling. Grid control involves certain parameters about the generator, transmission, and distribution power management systems. Among all this, system failure information (available to a number people responsible for grid control) and reliability and accuracy of the grid communication devices are the most vulnerable subjects.

Table II presents the network-related vulnerabilities in SG (both for house-to-grid and intra-grid networks). If SG's wireless network is breached through one or more of those vulnerabilities, this can in turn trigger the data-related vulnerabilities mentioned in Table I. In other words, the data-related vulnerabilities are dependent on the network-related ones.

V8	Network monitoring and interception vulnerabilities
V9	Network discovery and access control vulnerabilities
V10	MAC Address Access Control List (ACL) provides minimal access control to limited people with authorized wireless cards
V11	SSID - Any wireless consumer, malicious or not, can be able to listen to this beacon to get the SSID and bypass this low level access control
V12	Authentication mechanism vulnerabilities
V13	Shared key authentication flaw
V14	802.1X/EAP vulnerabilities
V15	WEP vulnerabilities
V16	WPA/WPA2 Vulnerabilities
V17	Way handshake and weak pass-phrase vulnerability

TABLE II
NETWORK-RELATED VULNERABILITIES.

Figure 2 presents a simplified SG and the wireless communication. A dotted line represents wireless communication and solid line represents electricity connection. The home network is extended and shown in detail along with data-related vulnerabilities. The left side of the diagram depicts the various devices that are part of SG along with the communication links. The vulnerabilities associated with the wireless network are also presented.

The network-related vulnerabilities are a challenge for any wireless network irrespective of the system (whether it is house-to-gird or intra-grid). Hence, these network-related vulnerabilities are the major concern for security requirements engineering process for SG. Since the data-related vulnerabilities are dependent on the network-related ones, in order to address the vulnerabilities in Table I it is critical to first address those presented in Table II. Further steps of the SREP derive several precautionary steps and security requirements that should be implemented in SG's development.

Step 3: Identify Security Objectives and Dependencies. The security objectives for a system should be determined based on safeguarding the assets or the system from vulnerabilities and their associated threats, also considering the scope of any future threats.

In order to mitigate the vulnerabilities identified in Step 2, the basic objective should be to prevent SG's various wireless network components such as Access Points (APs), Routers & Switches, Power Amplifiers, Transceivers, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs) from potential attackers. The types of attacks are determined in later steps of the SREP.

Confidentiality, Integrity and Availability (CIA) are the basic security goals to be achieved in order to secure SG's wireless networks. These CIA goals as used in SG wireless networks are discussed below:

Confidentiality of information or controls that exist on SG's wireless network are safeguarded by protecting the network components that are vulnerable to frequent attacks. It means preserving the privacy of information by protecting invalid access to it.

Integrity prevents unauthorized modification or alteration of information and ensures the originality of information. Integrity is attained by proper and restricted authorization of those who can access the data on SG network.

Availability means the system is available continuously to every authorized user without any disruption. This can be achieved by avoiding threats of attacks on SG wireless network. SG's wireless network should be designed to resist any attacks that might lead to service disruption.

The ultimate goal is to secure wireless transmissions in SG. Building a wireless network that responds effectively to a particular attack will ensure the security of a particular piece of information. For example, to protect the consumer data from being breached, SG's wireless network should be made robust against the Access Point (AP) attack via several possibilities discussed earlier, and the Wired Equivalent Privacy (WEP) should also be designed to resist and detect any potential attack. In essence, for each single task of SG to be effectively performed, the wireless network should be made to resist any attacks that are likely to happen.

Step 4: Identify Threats and Develop Artifacts. The major threats to SG are the network-based attacks. Attacks on networks have several intended characteristics ranging from data breach through system disruption. Besides network attacks which originate outside SG, certain threats also evolve