Information Systems 53 (2015) 147–160

Contents lists available at ScienceDirect

Information Systems

journal homepage: www.elsevier.com/locate/infosys

Integrated smart grid systems security threat model

Husam Suleiman [a], Israa Alqassem [b], Ali Diabat [c], Edin Arnautovic [d], Davor Svetinovic [b,*]

[a] Electrical and Computer Engineering at University of Waterloo, Canada
[b] Electrical Engineering and Computer Science at Masdar Institute of Science and Technology, Abu Dhabi, United Arab Emirates
[c] Engineering Systems and Management at Masdar Institute of Science and Technology, Abu Dhabi, United Arab Emirates
[d] Institute of Computer Technology at Vienna University of Technology, Vienna, Austria

ARTICLE INFO

Article history:
Received 6 May 2014
Received in revised form
13 October 2014
Accepted 8 December 2014
Available online 16 December 2014

Keywords:
Systems security threats
Systems security threats modeling and analysis
Smart grid
Smart grid vulnerabilities

ABSTRACT

The smart grid (SG) integrates the power grid and the Information and Communication Technology (ICT) with the aim of achieving more reliable and safe power transmission and distribution to the customers. Integrating the power grid with the ICT exposes the SG to systems security threats and vulnerabilities that could be compromised by malicious users and attackers. This paper presents a SG systems threats analysis and integrated SG Systems Security Threat Model (SSTM). The reference architecture of the SG, with its components and communication interfaces used to exchange the energy-related information, is integrated with the results of SG systems security threat analysis to produce a comprehensive, integrated SG SSTM. The SG SSTM in this paper helps better depict and understand the vulnerabilities exploited by attackers to compromise the components and communication links of the SG. The SG SSTM provides a reference of the systems security threats for industrial security practitioners, and can be used for design and implementation of SG systems security controls and countermeasures.

1. Introduction

Smart grid (SG) is a modernization of the power grid to monitor, control, protect, and automatically optimize the control and reliability of the power grid operations, through monitoring and distributed control systems [1]. The main objectives of the SG are to achieve high efficiency, reliability, safety in the power transmission and distribution, and a secure and reliable power delivery to customers [2,3]. This is achieved through the integration of the power grid with the Information and Communication Technology (ICT) to maximize the benefits by enabling remote monitoring, control, and processing of remote end devices [4,5]. This integration enables intelligent interaction between the SG and its stakeholders, and improves power delivery and customer services [4].

Due to the increased dependence on the ICT, increased connectivity and openness to the Internet and corporate networks, and increased use of hardware, software, and standard protocols, the SG is even more vulnerable to internal and external security attacks. It is critical to analyze and model the systems security threats and vulnerabilities exploited by attackers. From an industrial practitioner's perspective, it is useful to have a comprehensive reference architecture and a systems security model for the system under consideration. In this paper, given a lack of such reference systems security models in literature, we performed an extensive systems security requirements, threats, and vulnerabilities analysis, and specified and presented a comprehensive Systems Security Threat Model (SSTM).

Thus, this paper presents the integration of the results of the SG reference architecture research with the results of the systems security requirements, threats, and vulnerabilities analysis in order to produce a new comprehensive,

* Corresponding author.
E-mail address: dsvetinovic@masdar.ac.ae (D. Svetinovic).

http://dx.doi.org/10.1016/j.is.2014.12.002
0306-4379/

integrated reference SG SSTM that can be used by industrial systems security specialists to facilitate design and implementation of SG systems security controls and countermeasures. The integrated SG SSTM facilitates understanding and visualization of the main systems security threats in the SG. We specified the communication architecture of the SG by showing the components and the two-way wired and wireless communication infrastructure used to communicate the energy-related information. The main systems security threats under this architecture are specified and analyzed. The integrated SG SSTM is presented.

The remainder of this paper is organized as follows. Section 2 summarizes the background and related work. Section 3 analyzes the systems security threats of the SG. Section 4 presents the integrated SG SSTM. Section 5 discusses the results and evaluates the integrated SG SSTM. Finally, Section 6 concludes the paper.

2. Background and related work

The SG is a system of systems that collaborate via two-way electrical (physical) and communication (logical) interfaces. Each interface should maintain collaborators' privacy while communicating with each other. Collaboration between the SG's entities is required to enable better integration between them. A SG includes electrical storage units, distributed generation, home and building automation systems, industrial automation systems, Distribution Management Systems (DMS), and wired and wireless communication technologies [6]. The SG enables its participants to participate effectively in aligning energy supply with demand.

The SG consists of seven domains, and each domain is divided into sub-domains, actors, applications, associations, and interfaces [1]. These domains are bulk generation, transmission, distribution, customer, service provider, markets, and operations. The bulk generation domain delivers electricity to be carried over the transmission network; then, the electricity is transferred to the distribution network to be delivered to the customers.

Openness of the SG makes it highly vulnerable to the major systems security attacks. Wei et al. [7] discuss the major challenges and strategies required to protect the SG against internal and external security attacks. They proposed a conceptual layered framework to protect the SG. McLaughlin et al. [8] present the methods that could be used by attackers to play with the transmitted and stored data through the AMI network. AlAbdulkarim and Lukszo [9] provide an overview of the main consequences resulted from breaching the information systems security in the smart metering case in the SG. Lenzini et al. [10] discuss the trust, systems security, and privacy issues, integrity and availability, and usability and energy-awareness of the data for the AMI.

With the use of ICT in the SG, the power load can be controlled remotely through the Internet. Mohsenian-Rad and Leon-Garcia [11] outline a variety of practical loads in the SG that could be vulnerable for the Internet-based load altering attacks. These are Direct Load Control (DLC), indirect load control, and data centers and computation load. They present defense mechanisms to protect the SG from the Internet-based load altering attacks.

In the power transmission system, wired communications are integrated in the backbone of the power network. Wireless communications are integrated in the power distribution system. Wireless communications are reliable and provide low cost high speed links and easy setups of connections among smart devices distributed through the distribution system. But, wireless communications are also vulnerable to security attacks, like the wired ones. Wang and Yi [12] propose a wireless communication architecture for the Smart Distribution Grid (SDG) based on a Wireless Mesh Networks (WMNs). They analyze the security framework under this architecture. They develop a new intrusion detection mechanism called smart tracking firewall to meet the special requirements of the SDG wireless communications.

The industrial and critical infrastructure functions in the SG (such as electricity, gas, water and waste) are monitored and controlled using the SCADA system. It is important to analyze the security threats and risks in the SCADA systems to develop a proper security solution. Queiroz et al. [13] propose a modeling simulation tool to simulate the SCADA system. This modeling simulation tool supports the integration of the external devices and the applications, and tests the attack effect on them. Fernandez and Larrondo-Petrie [14] study the general structure of the SCADA system, analyze the main attacks that could be performed against it, and present methods to build a secure SCADA system using security patterns. Also, the vulnerabilities of the SCADA system are systematically evaluated using a vulnerability assessment framework proposed by Ten et al. [15–17] based on three levels: system, scenario, and access points. This is to study the effect of a security attack on the SCADA systems. A comprehensive survey on security of electric power infrastructure system is conducted and an attack-based method for impact analysis based on power system control network is developed by Ten et al. [18,19].

Gungor et al. [20] present a security analysis of the SG communication technologies. They provide a detailed description of the SG communication technologies, requirements, and standards. Advantages and disadvantages of these communication technologies are also presented. The communication technologies include ZigBee, WMN, cellular network communication, Power Line Communication (PLComm), and Digital Subscriber Line (DSL). The SG communication requirements, which are security, system reliability, robustness, availability, scalability, and Quality of Service (QoS) are also presented. Mahmood et al. [21] present the design and implementation of the Automated Metering Reading (AMR) SG system with more advanced features to enable efficient monitoring and control and to minimize outages and losses in SG system. The presented AMR concepts include automated reading and enable monitoring of load transformers using the SCADA system. Qui et al. [22] experimentally discuss ways of energy consumption in different security algorithms. They experimentally study that by taking different power sites. They measure the energy consumption of these algorithms and propose a set of principles on using these algorithms in Wide Area Monitoring System (WAMS) nodes.

Wei et al. [23] propose a framework for a SG automation system to protect the SG against security attacks. More specifically, they discuss the communication and network