2015 12th International Conference on Information Technology - New Generations

Smart Grid Security Risks

Jeffrey Anu, Rajeev Agrawal, Cameron Seay
Department of Computer Systems Technology
North Carolina A & T State University
Greensboro, USA
janu@aggies.ncat.edu, ragrawal@ncat.edu, cwseay@ncat.edu

Sambit Bhattacharya
Department of Mathematics and Computer Science
Fayetteville State University
Fayetteville, NV 28301
sbhattac@uncfsu.edu

***Abstract* - Smart grid technology is a collection of existing and up-and-coming technologies working together to improve the distribution of electric energy. It provides the providers and consumer of power real time information on power production and consumption. Cyber technology is being utilized in electric smart grid system from the generation of the power to its distribution to consumers. Nowadays it has become relatively easy for consumers to be monitored through wired and wireless means using these cyber technologies on how they effectively and efficiently manage power provided to them. However with the introduction of cyber technologies in electric grid systems, there is an added risk to its implementation and operation. This paper will be looking at the security risk associated with power production and transmission, the communication protocols used in the smart grid and the security risk for consumers.**

Keywords-Smart grid, security, MODBUS, SCADA, DNP3

I. INTRODUCTION

A careful look at the electric grid systems reveals that it is aging while the demand for power is continuously growing every day. With our phones, cars, and home appliances getting technologically smart, it will not be out of place for electric grid to be improved technologically.

An electric grid is an interconnected system where power is generated from different sources and location and the end product is then distributed to consumers. The grid includes wires, substations, transformers, switches and is classified under generation, transmission and distribution [1]. From the generation of electric power through its distribution and usage by consumers, it has not seen much improvement over the years. Smart grid is a system which seeks to modernize the generation of electricity, its consumption and the data shared along during its lifecycle.

Electricity when generated has to be used or stored and the surplus power sold to competitors or neighboring countries. With internet technology as the driving forcing behind smart grid systems, there is going to be an improvement in power production and consumption; but an added security risk will also emerge with it.

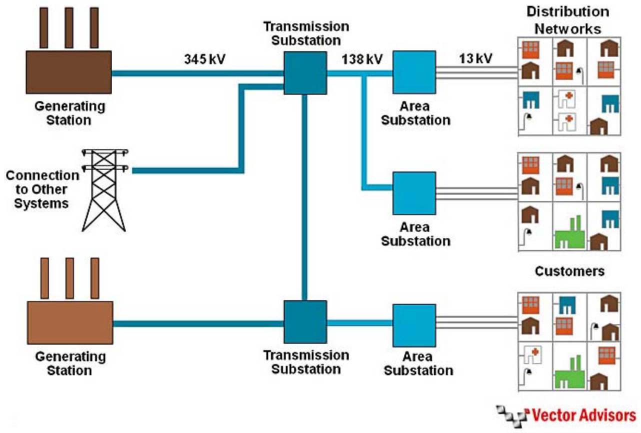

Figure 1. Typical layout of an electric grid

Figure 1 shows a typical electric grid system, displaying power from the generating source through the various substations and final distribution to the consumer [2].

The information technology and telecommunication industry are gradually evolving and integrating into smart grid technology; with both of these industries have known existing threats and vulnerabilities. The threats and susceptibilities of the information technology and telecommunication industry should not be overlooked and treated indifferent but considered in relation with the Smart Grid infrastructure. In addition, these vulnerabilities are also due to the numerous stakeholders and operational complexity.

This paper is organized as follows. In section II, we discuss the existing security system of a smart grid. Section III of this paper talks about some of the possible security threats that might be exposed to the smart grid system. In section IV, some of the documented industrial attacks on the smart grid are listed. The conclusion and future works are discussed in section V.

II. SECURITY SYSTEM OF A SMART GRID

In this section we will describe the security systems deployed under power generation and transmission, communication protocols used and security at consumer premises. The NIST Framework and Roadmap document identifies seven domains within the Smart Grid: Transmission, Distribution, Operations, Bulk Generation, Markets, Customer, and Service Provider. A Smart Grid domain is a high-level

978-1-4799-8828-0/15 $31.00 © 2015 IEEE
DOI 10.1109/ITNG.2015.84

grouping of organizations, buildings, individuals, systems, devices, or other stakeholders with similar objectives and relying on or participating in similar types of applications. These various stakeholders are needed to transmit, store, edit, and process the information needed within the Smart Grid. To enable Smart Grid functionality, the stakeholders in a particular domain often interact with actors in other domains, as shown in Figure 2 [3].

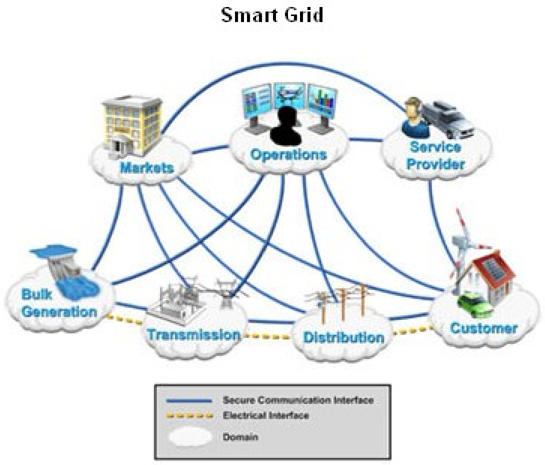

Figure 2. Overview of smart grid

A. *Security during power generation and transmission*

1) Power Line Carrier (PLC) - Secured Communication

Electric energy in the United States has a considerable number of source from which it is generated. Communication by this energy source has traditionally been done using Power Line Carrier's (PLC). PLC uses the power transmission lines to transmit radio frequency signals in the range of 30 kHz to 500 kHz. PLC systems are used to provide voice and telemetry relaying on the communications portions of 220/230 kV, 110/115 kV, or 66 kV interconnected power transmission network.

PLC's provide high physical security for communication since the power line equipments are located with the substations [4]. Even though it provides secured communication, it is becoming increasingly costly because of its low patronage due to low quality of voice, data and number of channels it provides.

2) Process Control Systems (SCADA)

Process Control Systems (PCS) refer to the overall set of systems that remotely monitor and measure remote sensors from a centralized location. Supervisory control and data acquisition (SCADA) is a known centralized system used for gathering and analyzing real time data at power generation stations. A SCADA system can gather information as to the amount of pressure coming out of a valve to a short circuit in a power breaker while displaying this information in a logical and organized way. A SCADA system is made up Remote Telemetry Units (RTU's), communications and a Human Machine Interface (HMI).

These components together are responsible for gathering information from sites and presenting them into forms understood by operators. Data communication within SCADA system over the years has been facilitated using point-to-point communication, power line-carriers, leased telephone lines, very high frequency bands (VHF) and ultra high frequency bands (UHF). But recently manufacturers of SCADA systems have incorporated Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet communications into both their hardware and software programs. SCADA systems are therefore becoming vulnerable to many of the same threats as any TCP/IP-based system [5].

B. *Communication Protocols Used in SMART Gride*

There exists a two way communication between the device/infrastructure within smart grid. And with the introduction of internet technology within the grid system, there has to be standardized formats through which these communication and exchange of data can be achieved. Listed in this section are a few of the most commonly used communication protocols in smart grid systems.

1) MODBUS

MODBUS is a messaging structure used to establish master slave/client-server communication between intelligent devices. It is an application layer messaging protocol implemented using TCP/IP over the Ethernet. It allows for easy communication by allowing for remote operations to be initiated by some devices such as PLC's, HMI, Control Panel, Motion control, Drivers, etc. Figure 3 shows the communication stack for the MODBUS protocol. [6]

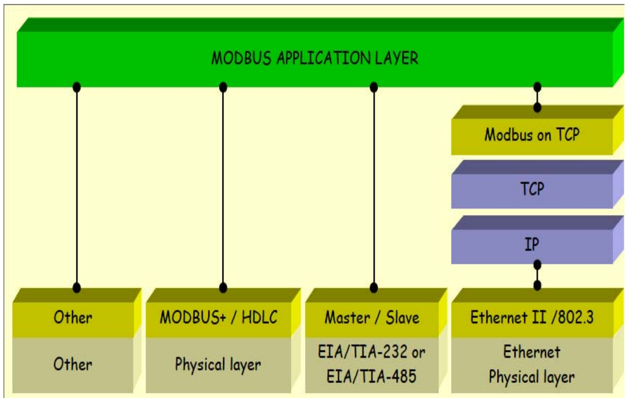

Figure 3. MODBUS Protocol Stack

2) DNP3

Distributed Network Protocol (DNP) is an open protocol used for communication between master stations and RTUs or Intelligent Electronic Devices (IEDs). TCP/IP with link layer frames embedded within is used to transport DNP3 messages. DNP3 is referenced in IEEE standards as IEEE Std 1815-2010 [7].

3) ICCP

Inter-Control Center communication Protocol (ICCP) is used for inter-master station communications. It uses local area and wide area network architecture to transmit data between control stations of utility companies. The ICCP protocol is based on client/server concept with the control center acting as both a client and a server. It is a standard recognized by the International Electrotechnical Commission as IEC 60870-6/TASE.2 [8].

4) OCP

Open Core Protocol (OCP) defines a point-to-point interface between two communicating entities. OCP provide demarcation by which core authors and System-on-Chip (SoC) integrators design [9].

5) RS-232

It is a standard protocol used in asynchronous serial communication. It is used in computer serial ports [10].

6) IEC 60870-5-101

It is based on the EPA architecture (Enhanced Performance Architecture) and defines only the physical link and application layers of the OSI model. It is primarily used with relatively slow transmission media on the asynchronous V.24 interface. IEC 60870-5-101 also allows for extensions with proprietary vendor-specific functions [11].

7) IEC 60870-5-103

IEC 60870-5-103 defines communication for a serial, unbalanced link only. Communication speeds are defined as either 9600 or 19200 baud. An IEC 60870-5-103 device can be interoperable and interchangeable, or only interoperable. Interoperability means that any required application data in the device, which can be coded into an IEC 60870-5-103 data type, can be mapped into the IEC 60870-5-103 address space. This data is recognized by any IEC 60870-5-103 master. Interchangeability means supporting the application data (informative elements) whose semantics are pre-defined by the IEC 60870-5-103 standard [12].

8) IEC 60870-5-104

IEC 60870-5-104 also known as IEC 870-5-104 is an international standard, released in 2000 by the IEC (International Electrotechnical Commission). It enables communication between control station and substation via a standard TCP/IP network. The TCP protocol is used for connection-oriented secure data transmission.

IEC 60870-5-104 limits the information types and configuration parameters defined in IEC 60870-5-101, which means that not all functions available in IEC 60870-5-101 are supported by IEC 60870-5-104. In practice, vendors very often combine the IEC 60870-5-101 application layer with the IEC 60870-5-104 transport profile, without paying attention to restrictions. This might then lead to problems, if a device strictly applies the standard [13].

C. Consumer Infrustracture

Consumer infrastructure consists of the metering, smart appliances and home area networking.

1) Metering Infrustracture

Electric meters used in determining the amount of energy consumed by the customers have come a long way from its initial inception. Meters have evolved from being electromechanical meters (analog meters) through electronic meters to the most current smart meters [14].

Advanced metering infrastructure (AMI) also referred to as smart meters, which perform the same primary function of a conventional meter by determining the amount of electric energy that customers use. But unlike conventional meters they are equipped with wireless devices which have the capability of wirelessly sending information about consumer's energy usage. This eliminates the cost and time of sending personnel from the energy company to manually read the meter of clients. Advanced metering infrastructure consists of a two way communication between the power company and the consumer making use of an assigned IP address to the metering device. AMI is not only provided to domestic or commercial users of electricity. This technology is also being developed for users of electric cars.

Securing a smart meter is a challenge just as securing a conventional meter since both devices are located at the customer premises. There is a risk of customer information being accessed by hackers in the instance of smart meters; while in the instance of both conventional and smart meters information about data usage sent to power companies can be interfered with.

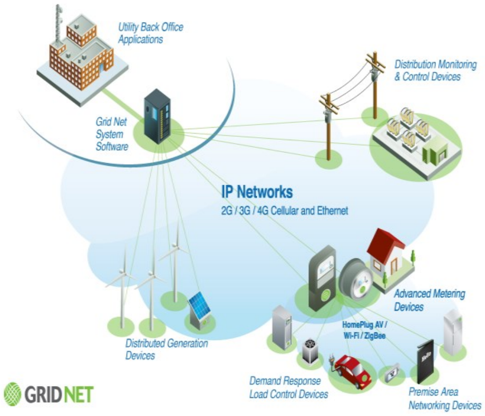
Utility Back Office Applications
Distribution Monitoring & Control Devices
Grid Net System Software
IP Networks
2G / 3G / 4G Cellular and Ethernet
Advanced Metering Devices
HomePlug AV / Wi-Fi / ZigBee
Distributed Generation Devices
Demand Response Load Control Devices
Premise Area Networking Devices
GRIDNET

Figure 4. Networking Infrastructure

Neighborhood Area Network (NAN) represents the network infrastructure used to deliver and support the AMI and Automatic Meter Reading (AMR) capabilities. NANs are typically designed with a mesh network topology, and they rely heavily on a number of wireless-based networking media and protocols, such as cellular, WiMAX, satellite communications and ZigBee [15]. Figure 4 shows the smart meter being used in the smart grid system. The metering infrastructure includes proprietary software used by the utility office, power generated by individuals (i.e. solar power, wind energy), and area networking for premises and distribution and control device centers [16].

III. Recent Security Attacks

Systems and devices used in smart grid are subjected to attacks just like any other TCP/IP communication modeled device. In the instance of SCADA, the manufacturers of the system have made access to information about the operation and the configuration of the system easy to gain. They willingly display it on the internet. Lots of security threats that some utility companies and device manufacturers experience are not reported due to these establishments not wanting to tarnish their image. Two of these attacks which were published in newspaper articles are listed below.

A. Cyber attack on Iranian nuclear power plant

A power plant in Iran's southern coast over the past years has seen virus attacks meant at interrupting its operations. Irrespective of the culprits of these attacks, this incident shows the consequence of smart grid systems not properly secured. An expert suggests that the stuxnet worm was actually developed to look for very specific Siemens settings. The worm injects its own codes into the PLC system that it targets [17].

B. Schneider Electric Hacked

The network of Telvent a subsidiary of Schneider electric was hacked when attackers installed malicious software and accessed project files for their OASyS SCADA system. For fear of customer information being compromised the company temporary discontinued its remote access program to customer computers [18].

C. Pacific Gas & Electric, San Jose

The high-voltage transformers at the 500-kilovolt substation near San Jose were attacked in April 2013 with .30 caliber rounds. This attack caused the transformers to leak cooling oil, overheat, and become inoperative.

IV. Known Security Threats

Securing smart grid involves upgrading endpoints like smart meters and grid controls, along with the chain of networking and software that binds them to the utility enterprise. The system has to protect consumers as well as have an early detection system for imminent attacks. According to NIST, cyber security must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters [19].

A. Possible power generation and transmission threats

Attacks on SCADA systems are often system specific and personalized to the target computer's design. This allows the SCADA system to be attacked with the following:

1) *Denial of Service (DoS)* – Denial of service attack occurs when the smart grid network is flooded with unwarrented traffic. This attack can be used to crash the SCADA server leading to loss of operation [20].
2) *Manipulation and Falsification* – This occurs when changes are made to data points or operators are deceived into thinking a control process is out of control and must be shut down.
3) *System files deleted from the SCADA server* – The system file within the SCADA server can be deleted through the activities of intruders or erronously by employees.
4) *Trojan Attack* – With its apparent natural appearnce as a harmless program or data, trojans are malicious programs which infect computer system files or program. A Trojan if introduced into a grid system, can take complete control of the system.
5) *Keylogging* – This is the process of monitoring the keystrokes from operators to obtain their usernames and passwords
6) *Use SCADA Server as a launching point to defame and compromise other system components within corporate network .*

B. Threats in communication

1) *Spoofing* – The IP address of the metering device can be masked and used by intruders to either manipulate their own accounts or those of others.
2) *Weak encryption* - Obtaining sensitive data through weak or missing encryption from consumer home networks.

C. Possible consumer threats

1) *Burglary* - This can happen due to the studying of the consumers' usage pattern to determine if they will be on vacation or not at home.
2) *Manipulation of meters*- Intruders can manipulate the meter to request for energy usage and demand.
3) *Introducing of devices*- Unauthorized devices such as IP scanners or wireless signal blockers can introduce the delay in the transmission of data or acquire the network information of customers [21].

V. Conclusion and Future Work

This paper reviews the security threats that are associated with the smart grid system. It shows that with the introduction of Internet technology in the grid system, there is the risk from both internal and external sources. Even though lots of security threats were not documented, they do exist and care should be taken to adequately protect smart grid systems. This can be attained by providing real time intrusion detection systems and intrusion prevention systems.

As future work, we would like to further study the most common forms of cyber attacks and exploit a robust end-to-end solution for distribution, transmission and the consumer infrastructure.

REFERENCES

[1] Department of Energy, “Smart Grid”.

Available: http://energy.gov/oe/technology-development/smart-grid

[Accessed November 2, 2014].

[2] Houston’s energy future, “Smart grid Task Force”.

Available:http://www.houstonenergyfuture.com/energy-collaborative/smart-grid-task-force/. [Accessed November 2, 2014].

[3] NISTIR. “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. The Smart Grid Interoperability Panel – Cyber Security Working Group. August 2010.

[4] National Communications System, “Supervisory Control and Data Acquisition (SCADA) Systems. NCS TIB 04-1, October 2004.

[5] NISTIR. “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. The Smart Grid Interoperability Panel – Cyber Security Working Group. August 2010.

[6] Modbus-IDA. “MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b”. DECEMBER 28, 2006.

[7] DNP. “ A DNP3 Protocol primer”. Revision A. March 20, 2005.

[8] IEC. “Telecontrol equipment and systems- Part 6-503: Telecontrol protocols compatible with ISO standardsnand ITU-T recommendations – TASE.2 services and protocol”. Second edition 2002-04.

[9] Open Core Protocol Available: http://www.accellera.org/downloads/standards/ocp/

[Accessed November 2, 2014].

[10] RS-232 Serial Protocol

Available: http://controls.ame.nd.edu/microcontroller/main/node24.html

[Accessed November 2, 2014].

[11] IPCOM GmbH. “IEC 60870-5-101”

Available: http://www.ipcomm.de/protocol/IEC101/en/sheet.html

[Accessed November 2, 2014].

[12] ABB, “IEC 60870-5-103 Communication Protocol Manual”. Document ID: 1MRK 511 243-UEN. Issued: February 2011. Product version: 1.1

[13] IPCOM GmbH. “IEC 60870-5-104”

Available: http://www.ipcomm.de/protocol/IEC101/en/sheet.html.

[Accessed November 2, 2014].

[14] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and David Irwin, “Private memoirs of a smart meter,” In Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys '10). ACM, New York, NY, USA, pp. 61-66.

[15] Ernst and Young, “Attacking the smart grid” insight on governance, risk and compliance. December 2011. [Accessed December 10, 2014].

[16] Image retrived from: http://img1.grid-net.com/img/Grid-Net-Platform.png. [November 2, 2014].

[17] T. M. Chen, S. Abu-Nimeh, "Lessons from Stuxnet," Computer , vol.44, no.4, pp.91-93, April 2011.

[18] Jesse Berst. SmartGridNews. “Think a cyber-attack can’t happen to you? Telvent has been hacked, blogger claims”.

Available: http://www.smartgridnews.com/artman/publish/Technologies_Security/Think-a-cyber-attack-can-t-happen-to-you-Telvent-has-been-hacked-blogger-claims-5151.html#.UO94pOSw8k8. September 28, 2012.

[Accessed November 2, 2014]

[19] NIST, “Guideline for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture and high-level requirements”. NISTIR 7628. August 2010. [Accesssed November 2, 2014]

[20] W. Wenye, X. Yi, and K. Mohit, “A survey on the communication architectures in smart grid,” Computer Networks, Volume 55, Issue 15, 27 October 2011, pp. 3604-3629.

[21] X. Li, X. Liang, R Lu, X. Shen, X. Lin, and H Zhu. “Securing Smart Grid: Cyber Attacks, Counter measures, and Challenges,” Communications Magazine, IEEE , vol.50, no.8, pp. 38-45, August 2012.