Communication Security for SCADA in Smart Grid Environment

Rosslin John Robles[1], Tai-hoon Kim[1*]

[*]Corresponding Author
[1]Multimedia Engineering Department,
Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon,
Korea
rosslin_john@yahoo.com, taihoonn@hnu.kr

Abstract: - Supervisory Control and Data Acquisition systems are basically Process Control Systems, designed to automate systems such as traffic control, power grid management, waste processing etc. Conventionally, SCADA is connected only in a limited private network because SCADA is considered a critical infrastructure, and connecting to the internet may put the society on jeopardy, SCADA operators hold back on connecting it to the public network like the internet. However, connecting SCADA to the Internet can provide a lot of advantages in terms of control, data viewing and generation. SCADA infrastructures like electricity can also be a part of a Smart Grid. Connecting SCADA to a public network can bring a lot of security issues. To answer the security issues, a SCADA communication security solution using crossed-crypto-scheme is proposed.

Key-Words: - SCADA, Security Issues, Encryption, Crossed Crypto-scheme, Smart Gird

1 Introduction

Smart Grid was built when energy was relatively inexpensive. While minor upgrades have been made to meet increasing demand, the grid still operates the way it did almost 100 years ago—energy flows over the grid from central power plants to consumers, and reliability is ensured by maintaining excess capacity. Infrastructures like electricity which is controlled by SCADA can play a big role on Smart Grids.

SCADA is a concept that is used to refer to the management and procurement of data that can be used in developing process management criteria. The use of the term SCADA varies, depending on location. In North America, SCADA refers to a distributed measurement and management system that operates on a large-scale basis. For the rest of the world, SCADA refers to a system that performs the same basic functions, but operates in a number of different environments as well as a multiplicity of scales. While the use of the term SCADA may not be uniform, many components are the same, regardless of the scale of the process.

On the Next parts of this paper, we discuss SCADA, the conventional setup and the Smart Grid. Advantages which can be attained using the Smart Grid are also covered. Security issues are being pointed out. We also suggest a security solution for a Web based SCADA using symmetric key encryption.

2 SCADA Systems

SCADA systems are primarily control systems. A typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station.

For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (sometimes referred to as the RTU). The Remote Terminal Units consists of a programmable logic converter. The RTU are usually set to specific requirements, however, most RTU allow human intervention, for instance, in a factory setting, the RTU might control the setting of a conveyer belt, and the speed can be changed or overridden at any time by human intervention. In addition, any changes or errors are usually automatically logged for and/or displayed. Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention.

One of key processes of SCADA is the ability to monitor an entire system in real time. This is facilitated by data acquisitions including meter reading, checking statuses of sensors, etc that are communicated at regular intervals depending on the system. Besides the data being used by the RTU, it is also displayed to a human that is able to interface with the system to override settings or make changes when necessary.

2.1 SCADA Software

Supervisory Control and Data Acquisition software can be divided into proprietary type or open type. Proprietary software are developed and designed for the specific hardware and are usually sold together. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems are designed to communicate and control different types of hardware. It is popular because of the interoperability they bring to the system. [1] WonderWare and Citect are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system.

2.2 SCADA Hardware

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves. [2]

2.3 Human Machine Interface

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

3. Installation of SCADA Systems

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.[3][4]

3.1 Conventional Supervisory Control and Data Acquisition

The function of SCADA is collecting of the information, transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens. Systems automatically control the actions and control the process of automation.

Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU and other electronic devices, manufacturers incorporated digital electronics into relay logic equipment. Programmable logic controllers or PLC's are still the most widely used control systems in industry. As need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs

(Programmable logic controllers) and DCS (distributed control systems) are used as shown in Figure 1.

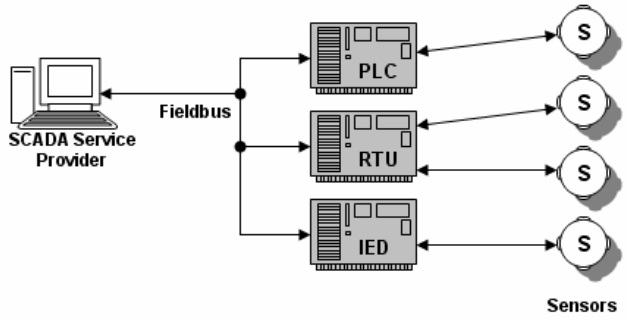

Figure. 1 Common SCADA Installation utilizing Remote Terminals (PLC/DCS, Sensors) and Master Station connected using a fieldbus.

4. Smart Grid

A smart grid includes an intelligent monitoring system that keeps track of all electricity flowing in the system. It also incorporates the use of superconductive transmission lines for less power loss, as well as the capability of integrating alternative sources of electricity such as solar and wind. When power is least expensive a smart grid could turn on selected home appliances such as washing machines or factory processes that can run at arbitrary hours. At peak times it could turn off selected appliances to reduce demand. Similar proposals include smart electric grid, smart power grid, intelligent grid (or intelligrid), FutureGrid, and the more modern intergrid and intragrid. In principle, the smart grid is a simple upgrade of 20th century power grids which generally "broadcast" power from a few central power generators to a large number of users, to instead be capable of routing power in more optimal ways to respond to a very wide range of conditions, and to charge a premium to those that use energy at peak hour.

The conditions, to which a smart grid, broadly stated, could respond, occur anywhere in the power generation, distribution and demand chain. Events may occur generally in the environment (clouds blocking the sun and reducing the amount of solar power, a very hot day), commercially in the power supply market (prices to meet a high peak demand), locally on the distribution grid (MV transformer failure requiring a temporary shutdown of one distribution line) or in the home (someone leaving for work, putting various devices into hibernation, data ceasing to flow to an IPTV), which motivate a change to power flow.

Latency of the data flow is a major concern, with some early smart meter architectures allowing actually as long as 24 hours delay in receiving the data, preventing any possible reaction by either supplying or demanding devices. [3].

The Smart Grid is the application of modern information, communication, and electronics technology to the electricity delivery infrastructure as shown in figure 2.

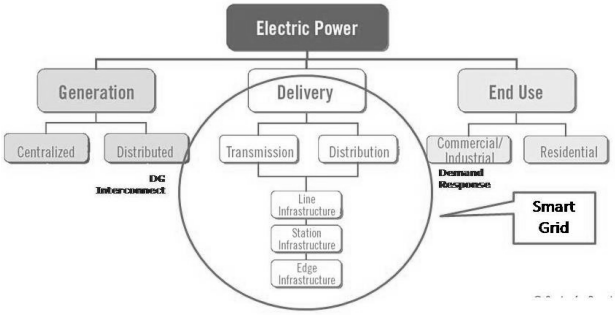

Figure 2. Smart Grid

The earliest, and still largest, example of a smart grid is the Italian system installed by Enel S.p.A. of Italy. Completed in 2005, the Telegestore project was highly unusual in the utility world because the company designed and manufactured their own meters, acted as their own system integrator, and developed their own system software. The Telegestore project is widely regarded as the first commercial scale use of smart grid technology to the home, and delivers annual savings of 500 million euro at a project cost of 2.1 billion euro. [5]

5. SCADA and Smart Grid

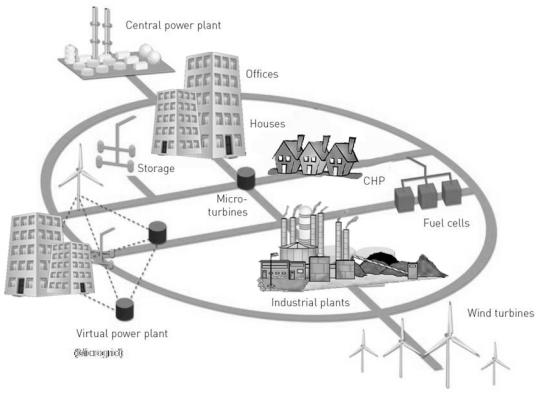

Figure 3. Vision of Smart Grid

Central & distributed generation Virtual aggregation of generators and loads for system management Grid components connected by both electrical and data networks Bi-directional power flows. The following figure shows how Smart Grid will look like.

5.1 Advantages of SCADA in Smart Grid

- The Tolerant of attack – mitigates and stands resilient to physical and cyber attacks
- Provides power quality needed by 21st century users
- Fully enables competitive energy markets – real-time information, lower transaction costs, available to everyone
- Optimizes assets – uses IT and monitoring to continually optimize its capital assets while minimizing operations and maintenance costs – more throughput per $ invested.
- Accommodates a wide variety of generation options – central and distributed, intermittent and dispatchable.
- Empowers the consumer – interconnects with energy management systems in smart buildings to enable customers to manage their energy use and reduce their energy costs.
- Self-healing – anticipates and instantly responds to system problems in order to avoid or mitigate power outages and power quality problems.

6. Crossed-Crypto Scheme for SCADA in Smart Grid

In cryptography, there are major types of encryptions: the symmetric encryption and the asymmetric encryption. From the two major types of encryptions we can say that Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost. On the other hand symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be considered as the correct and most appropriate security solution for many applications. [6] In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption. Diagram of a crossed crypto-scheme is shown in Figure 4.

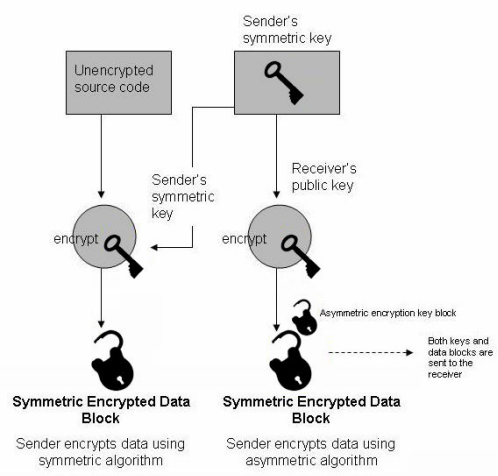

Figure 4. Crossed crypto-scheme

The crossed crypto-scheme can be integrated in the communication of the SCADA master and SCADA assets. The algorithm presented here combines the best features of both the symmetric and asymmetric encryption techniques. The plain text data is to be transmitted in encrypted using the AES algorithm. Further details on AES can be taken from [7].

The AES key which is used to encrypt the data is encrypted using ECC. The cipher text of the message and the cipher text of the key are then sent to the SCADA assets. The message digest by this process would also be encrypted using ECC techniques. The cipher text of the message digest is decrypted using ECC technique to obtain the message digest sent by the SCADA Master. This value is compared with the computed message digest. If both of them are equal, the message is accepted otherwise it is rejected. You can see this scenario in figure 5.

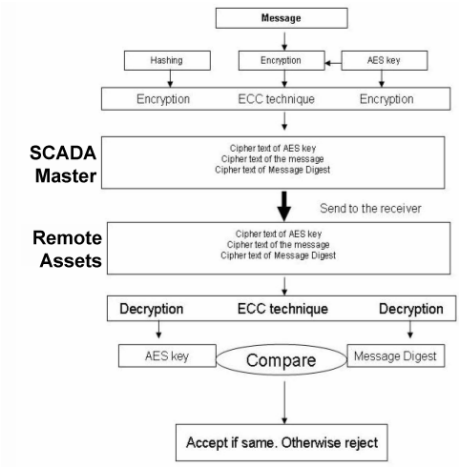

Figure 5. Chain of operation

7. Conclusion

In summation, it is easy to observe that SCADA technology holds a lot of promise for the future. The economic and performance advantages of this type of system are definitely attractive. The security of any future Smart Grid is dependent on successfully addressing the cyber security issues associated with the nation's current power grid. The implementation of Smart Grid will include the deployment of many new technologies and multiple communication infrastructures. In this paper, we propose the integration of the Crossed crypto-scheme to the SCADA system in Smart Grid environment.

References

1. D. Bailey and E. Wright (2003) Practical SCADA for Industry
2. Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems
3. http://earth2tech.com/2008/05/01/silver-springs-the-cisco-of-smart-grid/ Accessed: May 2010
4. http://earth2tech.com/2009/05/20/utility-perspective-why-partner-with-google-powermeter/ Accessed: May 2010
5. National Energy Technology Laboratory (2007-08) (pdf). NETL Modern Grid Initiative — Powering Our 21st-Century Economy. United States Department of Energy Office of Electricity Delivery and Energy Reliability. p. 17. http://www.netl.doe.gov/smartgrid/referencesh elf/whitepapers/Modern%20Grid%20Benefits_Final_v1_0.pdf. Accessed: May 2010
6. M.Balitanas, R.J. Robles, N. Kim, and T. Kim, "Crossed Crypto-scheme in WPA PSK Mode," Proceedings of BLISS 2009, Edinburgh, GB, IEEE CS, August 2009, ISBN 978-0-7695-3754-5
7. Federal Information Processing Standards Publication 197 (2001) Announcing the ADVANCED ENCRYPTION STANDARD (AES) http://csrc.nist.gov/publications/fips/fips197/fips -197.pdf Accessed: January 2009