Vulnerabilities in SCADA and Critical Infrastructure Systems

Rosslin John Robles[1] , Min-kyu Choi[1], Eun-suk Cho[1],
Seok-soo Kim[1], Gil-cheol Park[1], Sang-Soo Yeo[1]

[1] Department of Multimedia Engineering,
Hannam University, Daejeon, Korea
rosslin_john@yahoo.com, freeant7@naver.com, eunsukk@empal.com,
{sskim,gcpark,ssyeo}@hnu.kr

Abstract. Critical Infrastructures are so vital that a damage or breakage of it will greatly affect the society and economy. SCADA systems play a big role on Critical Infrastructure since most of these infrastructures are controlled systems. Presented in this paper are the vulnerabilities of a SCADA system, its effect to the society and the ways to prevent such vulnerabilities. Also, the background of the SCADA system and its difference to the common computer system is discussed.

Keywords: SCADA, Control Systems, Vulnerability, Critical Infrastructure

1 Introduction

We are at least confident of the application or operating systems that are running in our desktop, servers and even cell phones. Whenever there are new vulnerabilities that will emerge, software companies release a fix or patch for it. Installing patches, fixes or updates is a good way of maintaining the security of the system. [1] It could take some time but it is manageable.

Sad to say, this way of handling vulnerabilities is not applicable to most Critical Infrastructure Systems. Most Critical Infrastructure Systems are control systems running the World's critical national infrastructures like power, water and transportation. SCADA Systems or Supervisory Control and Data Acquisition Systems play a big part to this Critical Infrastructure Systems. Unlike application or operating systems, These systems usually sold as bundled packages by the vendors, so the end-user really doesn't know what is inside and what needs patching to keep it safe from emerging threats and vulnerabilities.[2].

2 Supervisory Control and Data Acquisition

Before we point out the vulnerabilities in the SCADA systems, we must know what a SCADA system really is. SCADA (supervisory control and data acquisition) existed

long when control systems were introduced. A SCADA system that time uses data acquisition by using panels of meters, strip chart recorders and lights. Unlike modern SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control. These devices are still used to do supervisory control and data acquisition on factories, plants and power generating facilities.

Modern SCADA systems are now used in modern manufacturing and industrial processes, mining industries, public and private utilities, leisure and security industries. In these situations, telemetry is needed to connect systems and equipment separated by long distances. Some of this ranges to up to thousands of kilometers. Telemetry is automatic transmission and measurement of data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations. SCADA is the combination of telemetry and data acquisition.

SCADA is compose of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that information on the operator screens. The required control actions are then passed back to the process. [3].Typically SCADA systems include the following components: [4]

1. Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate.

2. Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.

3. Local processors that communicate with the site's instruments and operating equipment.This includes the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.

4. Short range communications between the local processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.

5. Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the process; receive alarms, review data and exercise control.

6. Long range communications between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, frame relay and cellular packet data.

2.1 SCADA Hardware

SCADA Systems usually have Distributed Control System components. RTUs or PLCs 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 RTUs and PLCs. 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. [5]

2.2 SCADA Software

SCADA 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. [3]

3. SCADA and its role to Critical Infrastructure Systems

The term “infrastructure” was defined by The American Heritage Dictionary [6] as:

“The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons.”

The US President issued an Executive Order 13010 which states that “certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States". [7] It is where the term "critical infrastructure" was highlighted. According to E.O. 13010, these critical infrastructures were: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue) and continuity of government. Figure 1 shows the infrastructures that were commonly pointed out as “critical”.

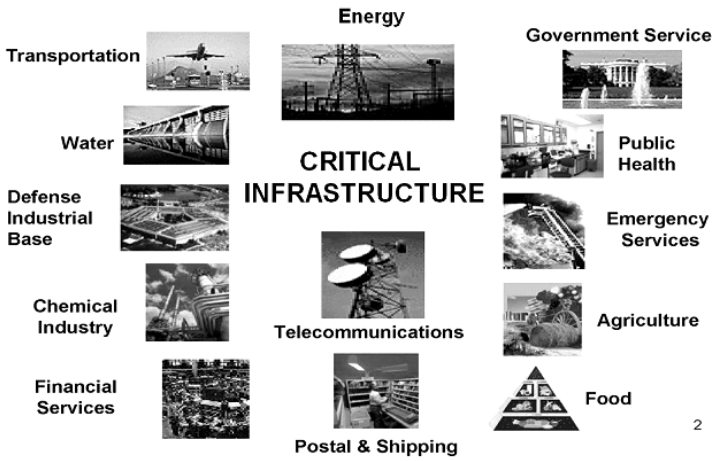

Fig 1. Critical Infrastructures

Most of these so-called critical infrastructures nowadays are controlled by controlled systems, SCADA in particular. So if the SCADA will malfunction, it will cause debilitating impact to the community and society.

4. Computer System Security

Computer Systems are usually not as broad as the SCADA systems. This system can be your Personal Computer (PC), PDA, Server, Cell phone, etc. It is much easier to debug and fix the errors in this kind of systems. Security threats to this system can be prevented or minimized by using the following: Setting a password on the system so only people who have access to it can access the information on it; Use of anti-virus software to prevent viruses from damaging the system; Use of anti-spyware software to protect your system from spyware that may attempt to monitor what the user is doing online; Have a firewall permanently turned on as the first line of defense against viruses, spyware and hackers; [8] and patching you system when new vulnerabilities emerge. This ways of protecting a computer system may take some but it is manageable. Since SCADA systems are different from usual computer systems, some of these techniques are not applicable to SCADA systems.

5. SCADA Vulnerabilities

The SCADA was developed, the goal was to create a control system that will provide good performance and have features that will make it easy to control and could do the tasks easily. Security was not a concern then. Common misconception regarding

SCADA security was SCADA networks were isoloated from all other networks and so attackers could not access the system. [9] As the industry grows, the demand for more connectivity also increased. From a small range network, SCADA systems are sometimes connected to other networks to increase the scope. This situation give rise to new security concerns to these SCADA networks. Once the SCADA network is connected to other networks, it is also open to threats that connected is open to attackers. This makes the SCADA system also vulnerable. The use of open standards for SCADA communication protocols are also increasing. Main reason is because its not as costly as proprietary standards. This reason makes it also easier for attackers to gain access to information in SCADA systems. The open standards make it very easy for attackers to gain in-depth knowledge about the working of these SCADA networks.

The use of COTS hardware and software to develop devices for operating in the SCADA network also contribute to its lack of security. COTS-based design can be cheaper and reduce design time, but it also raises concerns about the overall security of the end product. COTS software is not always secure. COTS software are not mainly designed to the system. It is usually used because of some of its features that are usable to the system. This is usually the target of the attack. When new vulnerabilities emerge it is difficult or sometimes impossible to patch these softwares. Devices that are designed to operate in safety-critical environments are usually designed to failsafe, but security vulnerabilities could be exploited by an attacker to disable the fail-safe mechanisms. This makes these devices must not only be designed for safety but also for security.

6. Incidents caused by SCADA Insecurity

To understand the importance of knowing the vulnerabilities of SCADA systems, here are just few of the incidents caused by insecure SCADA systems. As confirmed by the Nuclear Regulatory in August 2003, On January 2003, the Microsoft SQL Server worm known as Slammer—infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio. It disabled the safety monitoring system for nearly 5 hours. Also, the plant’s process computer failed, and it took about 6 hours for it to become available again. Slammer reportedly also affected communications on the control networks of other electricity sector organizations by propagating so quickly that control system traffic was blocked. [10]

On April 26, 1999, Gazprom, Russia's huge gas monopoly was one of a growing number of targets hit last year by computer hackers, hackers who controlled the company's gas flows for a short time. Hackers were able to get past the company's security and break into the system controlling gas flows in pipelines. The central switchboard of gas flows was "for some time“under the control” of external users. [11]

7. Recommended Strategy

These vulnerabilities can be overcome by developing new security technology and techniques to protect SCADA systems and Critical Infrastructure. Policies and Standards should be develop and design to fit the need of a specific system. Implement effective security management programs which are applicable to SCADA and Critical Infrastructure systems. Also, increase the security awareness and sharing of information on how to implement more secure architectures and existing security technologies. Network vulnerabilities on SCADA systems may be dealt with the use of a "honeypots". It is a technique used to trap, detect, deflect, or in some manner counteract attempts at unauthorized access to the network. [12] There's one SCADA honeypot project which may be utilized for this purpose. [13]

8. Conclusion

Critical Infrastructures are vital and very important to the society. Most Critical Infrastructures are controlled by Control Systems like SCADA. As presented in this paper, SCADA has some vulnerability that needs attention. If these vulnerabilities will not be attended, it will cause great effect to the society. As we know, SCADA was designed not focusing on security so ways to keep it from emerging vulnerabilities should be performed.

Acknowledgement

This work was supported by a grant from Security Engineering Research Center of Ministry of Knowledge Economy, Korea

References

1. Foley, J. and G. V. Hulme (2004). Get ready to patch. InformationWeek, August 30.
2. Eric Byres (2008). Hidden Vulnerabilities in SCADA and Critical Infrastructure Systems, February 19.
3. D. Bailey and E. Wright (2003) Practical SCADA for Industry
4. Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems
5. Wikipedia – SCADA http://en.wikipedia.org/wiki/SCADA Accessed: October 2008
6. Houghton Mifflin Company. Boston, MA. 2000 The American Heritage Dictionary of the English Language, Fourth Edition.
7. Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.
8. Securing your computer http://www.staysmartonline.gov.au/securing_your_computer accessed: October 2008
9. Carlson Rolf (2002) Sandia SCADA program – high-security SCADA LDRD final report
10. R. Dacey (2003) CRITICAL INFRASTRUCTURE PROTECTION Challenges in Securing Control Systems
11. T.C. Greene (2000) Russia welcomes hack attacks: Script Kiddies cut teeth hijacking critical infrastructure
12. Wikipedia - Honeypot (computing) http://en.wikipedia.org/wiki/Honeypot_(computing) Accessed: October 2008
13. V. Pothamsetty and M. Franz. SCADA HoneyNet Project: Building Honeypots for Industrial Networks. http://scadahoneynet.sourceforge.net/ Accessed: October 2008.