International Journal of of Grid and Distributed Computing
Vol.2, No.2, June 2009

Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems

Rosslin John Robles and Min-kyu Choi

Department of Multimedia Engineering, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
roslin_john@yahoo.com; freant7@naver.com;

Abstract

A damage or breakage of Critical Infrastructure or CI will have a huge effect on humanity and economy. Supervisory Control and Data Acquisition Systems (SCADA) play a big role on Critical Infrastructure since most of these infrastructures are controlled by control systems like SCADA. In this paper, we assess vulnerabilities of a SCADA system, its effect to the society and the ways to prevent such vulnerabilities. We also researched on the background of the SCADA system and its comparability to the common computer system is discussed.

Keywords: *SCADA, Control Systems, Critical Infrastructure Vulnerability*

1. Introduction

Whenever there are new vulnerabilities that will emerge, if we are using a common computer system like a PC, 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 may take some time but it is manageable.

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 vulnerabilities and threats.[2]

2. Critical Infrastructure, Control Systems and SCADA

Before discussing the vulnerabilities in the SCADA systems, we must know what a control systems and SCADA systems really are. SCADA systems, Distributed Control Systems and other smaller control systems are often found in the industrial sectors and critical infrastructures. These are also known under a general term, Industrial Control System. A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. ICSs are typically used in industries such as electrical, water, oil and gas, and chemical including experimental and research facilities such as nuclear fusion laboratories.

The reliable operation of modern infrastructures depends on computerized systems and SCADA systems. 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 includes the Master Station, the remote assets (RTU, PLC, IED) and the fieldbus which is the communication medium. [4]

3. SCADA Components

3.1. SCADA HMI

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).

An HMI is usually linked to the SCADA system's databases and software programs, to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides.

The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram. This means that the operator can see a schematic representation of the plant being controlled. For example, a picture of a pump connected to a pipe can show the operator that the pump is running and how much fluid it is pumping through the pipe at the moment. The operator can then switch the pump off. The HMI software will show the flow rate of the fluid in the pipe decrease in real time. Mimic diagrams may consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols.

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

An important part of most SCADA implementations are alarms. An alarm is a digital status point that has either the value NORMAL or ALARM. Alarms can be created in such a way that when their requirements are met, they are activated. An example of an alarm is the "fuel tank empty" light in a car. The SCADA operator's attention is drawn to the part of the system requiring attention by the alarm. Emails and text messages are often sent along with an alarm activation alerting managers along with the SCADA operator.

3.2. SCADA Software

SCADA software is usually linked to the SCADA system's databases and HMI, to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides. SCADA software can be divided into open type or

proprietary type. The main problem with these systems is the overwhelming reliance on the supplier of the system. [3]

3.3. SCADA Hardware

Distributed Control System components are usually included in SCADA. IEDs, 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]

3.4. Remote Terminal Unit

The RTU connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.

3.5. Supervisory Station

Supervisory Station refers to the servers and software responsible for communicating with the field equipment (RTUs, PLCs, etc), and then to the HMI software running on workstations in the control room, or elsewhere. In smaller SCADA systems, the master station may be composed of a single PC. In larger SCADA systems, the master station may include multiple servers, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server failure.

Initially, more "open" platforms such as Linux were not as widely used due to the highly dynamic development environment and because a SCADA customer that was able to afford the field hardware and devices to be controlled could usually also purchase UNIX or OpenVMS licenses. Today, all major operating systems are used for both master station servers and HMI workstations.

4. SCADA’s role to Critical Infrastructure

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]

Figure 1 shows the sectors which were stated in E.O. 13010 as critical infrastructure. 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.

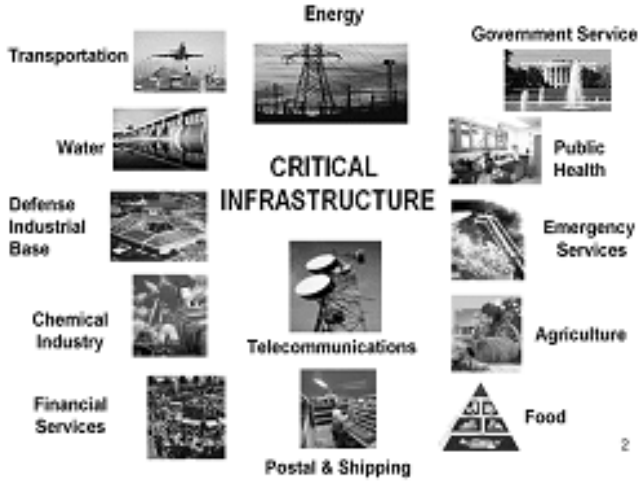

Figure 1. Sectors which are Critical Infrastructure

5. System Security

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. Since SCADA systems are different from usual computer systems, some of these techniques are not applicable to SCADA.

6. Vulnerabilities and Threats

6.1. SCADA Vulnerabilities

Common misconception regarding SCADA security was SCADA networks were isolated 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 like the internet. The open standards also 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. 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.

6.2. The Critical Infrastructure Threats

Accidents, natural disaster, crime, equipment failure and terrorist attack are just some of the threats that could damage or destroy Australia's critical infrastructure. The Government believes that arrangements for protecting critical infrastructure need to cover all hazards. It is therefore working with critical infrastructure owners and operators to make sure our vital services are suitably protected and, if they are damaged or destroyed, they can get up and running again quickly. The responsibility for protecting critical infrastructure is shared between critical infrastructure owners and operators, state and territory governments, and the Commonwealth.

7. SCADA Network Attacks

This part discusses various attack scenarios against SCADA networks. They differ in complexity, intent, and require access vectors for execution. There are different types of security issues that a vulnerable SCADA network represents.

7.1. Affects Status and Display Screens

A majority of SCADA networks have some sort of Master Station. For reliability, most networks have multiple control centers.

Attackers who gain access to a SCADA network can use a variety of techniques to alter the information consumed by the control center. Insiders to the network may be able to compromise servers on the network and change their data. Outsiders to the network may be able to exploit a vulnerability which gives them similar access to that of an insider.

In either case, information about key processes can be altered at the source of the data to present different information to operators and control systems.

7.2. Taking Over the Control Station

If the control station is not protected by security patches, firewalls, intrusion prevention and other mechanisms, it may be possible for an intruder to gain complete control over the SCADA networks.

Modern control centers use a combination of Unix, Windows and Web Based SCADA management tools. Each of these tools may be installed on any number of vulnerable operating systems and applications such as Apache or Microsoft web servers.

An attacker who has control over the SCADA network may not even need to understand the underlying SCADA protocols. Instead they will likely be presented with any user interface that a normal control center operator would use. These displays often include documentation and procedures for emergencies and change control. This information can be used by a remote attacker to understand how to control the SCADA network.

7.3. Disrupting Processes

Any SCADA system which manages a real-time or non stop operation can be used to prevent that operation from occurring. Attackers, intruders and malicious insiders can use network vulnerabilities to send “turn off” and “power off” messages to equipment performing a variety of processes.

If direct manipulation of the SCADA devices is not possible, it may also be possible to prevent communication from a control center to the SCADA devices. This may be all that is required for a hostile agent to prevent “normal” operations of a SCADA network device.

Since SCADA devices are usually physically inconvenient to get access to, an intruder may be able to keep the key systems powered off or out of commission and override any commands sent.

These effects can also be manifested in the case of a worm outbreak. Increased bandwidth usage, support systems being infected with viruses and loading down CPUs can keep a control center from managing their SCADA equipment.

7.4. Equipment and Property Damage

Lastly, since SCADA devices control many different physical processes, it may be possible to not only disrupt or disable operations, but it may also be possible to create permanent damage.

There are simply too many combinations of physical processes and any safety controls which may be in place to truly assess this vulnerability. Most SCADA plants do not have a “self destruct” sequence we see in the movies. Instead, most high availability or all time physical plants have a variety of physical and electronic safety precautions. For example, anything that moves at all likely has a governor on it which limits a top speed, regardless of what the SCADA control unit says. Similarly, ovens, power generators, power relay stations, and so on all have physical safety limitations built into them for what they can and cannot do.

8. Recent Events

On June 11, 2008, Core Security released a security advisory that details a fairly pedestrian stack-based buffer overflow vulnerability. This is similar to hundreds or thousands of this kind of flaw reported over the years except for one thing: it was found in large industrial control systems for things like power and water utility companies. That there is a vulnerability is not surprising—there are certainly many more—but it does give one pause about the dangers of connecting these systems to the internet. The bug was found in a SCADA—better known as SCADA—system and could be exploited to execute arbitrary code. Given that SCADA systems run much of the world's infrastructure, an exploit of a vulnerable system could have severe repercussions. The customers of Citect, the company that makes the affected systems, include "organizations in the aerospace, food, manufacturing, oil and gas, and public utilities industries."

Developers of SCADA systems nearly uniformly tell their customers to keep those systems isolated from the internet. But as Core observes: "the reality is that many organizations do have their process control networks accessible from wireless and wired corporate data

networks that are in turn exposed to public networks such as the Internet." So, the potential for a random internet bad guy to take control of these systems does exist. None of that should be particularly surprising when you stop to think about it, but it is worrying. Many SCADA systems—along with various other control systems—were designed and developed long before the internet started reaching homes and offices everywhere. They were designed for "friendly" environments, with little or no change for the hostile environment that characterizes today's internet. Also, as we have seen, security rarely gets the attention it deserves until some kind of ugly incident occurs.

Even for systems that were designed recently, there are undoubtedly vulnerabilities, so it is a bit hard to believe that they might be internet-connected. According to the advisory, though, SCADA makers do not necessarily require that the systems be physically isolated from the network, instead customers can "utilize technologies including firewalls to keep them protected from improper external communications."

Firewalls—along with other security techniques—do provide a measure of protection, but with the stakes so high, it would seem that more caution is required. It is probably convenient for SCADA users to be able to connect to other machines on the LAN, as well as to the internet, but with that convenience comes quite a risk. Even systems that are just locally connected could fall prey to a disgruntled employee exploiting a vulnerability to gain access to systems they normally wouldn't have.

One can envision all manner of havoc that could be wreaked by a malicious person (or government) who can take over the systems that control nuclear power plants, enormous gas pipelines, or some chunk of the power grid. Unfortunately, it will probably take an incident like that to force these industries into paying as much attention to their computer security as they do to their physical security.

On May 2008, SC Magazine[14] reports a rare SCADA vulnerability being discovered. It indicates that Researchers have discovered a rare bug in a Windows-based control software package used by as many as one-third of the world's industrial plants.The vulnerable software component, Wonderware SuiteLink, is used to help facilitate communications over TCP/IP networks for SCADA (supervisory control and data acquisition) systems, according to an advisory from Core Security Technologies, which discovered the flaw.

The vulnerability, first reported to Wonderware in January, could permit remote attackers to connect to the SuiteLink TCP port and send malicious packets, thus causing a denial-of-service, according to the advisory.

9. Recommended Solution

Vulnerabilities in SCADA can be overcome by developing new security technology and techniques to protect SCADA systems and Critical Infrastructure. Standards and Policies 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 honeypot project which may be utilized for SCADA. [13]

10. Conclusion

SCADA, Control Systems, and Critical Infrastructures are crucial and very important to the society. Many of the considered Critical Infrastructures are controlled by Control Systems like SCADA. AS emphasized 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. SCADA was designed not focusing on security so ways to keep it from emerging vulnerabilities should be performed.

Acknowledgement

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy.

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.
[14] Dan Kaplan (2008) SC Magazine "Rare SCADA vulnerability discovered" http://www.scmagazineus.com/Rare-SCADA-vulnerability-discovered/article/109956/ Accessed: October 2008.