The Security Related Function of SCADA in Critical Infrastructure

L. Arockiam[1)]

Abstract

Critical Infrastructures are so crucial to the society and community that a disruption of it can cause great damage. Many of these identified Critical Infrastructures are controlled by control systems like SCADA or Supervisory Control and Data Acquisition. Because of this, SCADA becomes a target of terrorists and other threats. In this paper, we discuss the relationship of Critical Infrastructure and SCADA, the threats and vulnerabilities and provides steps to minimize these threats and vulnerabilities. We also discuss the function of SCADA systems and other control systems to sectors which were considered Critical Infrastructure.

Keywords : Critical Infrastructure, SCADA, Control Systems

1. Introduction

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. SCADA or Supervisory control and data acquisition networks contain computers and applications that control and perform key functions in providing essential services and commodities such as electricity, natural gas, gasoline, water, waste treatment, transportation, etc.

In Simple words, SCADA controls Critical Infrastructure. Aside from SCADA's internal vulnerabilities, the fact that it controls Critical Infrastructure makes it more vulnerable and gains many threats. On the next parts of this paper, Critical Infrastructure and SCADA are defined and their relationship is discoursed.

2. Critical Infrastructure (CI)

Received(September 15, 2008), Review request(September 16, 2008), Review Result(1st:October 06, 2008, 2nd:October 26, 2008)
Accepted(December 31, 2008)

[1]Lecturer (SG), St.Joseph's College (Autonomous), Tiruchirappalli- 620 002, Tamil Nadu, INDIA

The term Critical infrastructure is used by governments to describe infrastructure or assets that are essential for the functioning of a society and economy[1]. The US government identified 14 areas or Infrastructures that required protection from threats. This infrastructure is so important because they provide goods and services that have great contribution to the economy and national defense. The survivability, reliability and resiliency of the systems identified as critical infrastructure allow the people to maintain a sense of confidence in their country and themselves. The National Strategy for Homeland Security has identified these 14 areas as: Agriculture & Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information ands Telecommunications, Banking and Finance, Energy, Transportation, Chemical Industry ands Hazardous Materials, Postal and Shipping, National monuments and icons, and Critical Manufacturing.

3. Supervisory Control And Data Acquisition Systems

SCADA systems today are now used in modern manufacturing and industrial processes, mining industries, public and private utilities, leisure and security industries. In these event, 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[2].

4. 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.

4.1 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.

4.2 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.

4.3 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.

4.4 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.

5. Critical Infrastructure Controlled by SCADA

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"[3-4]. It is where the term "critical infrastructure" was highlighted. 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. Power Utilities, Energy Utilities and other major Infrastructures are now converted in SCADA controlled systems.

[Fig. 1] SCADA control station

5.1 SCADA Systems for Measuring and Managing Water

This SCADA system is designed with sensors to the system that collect data on equipment such as pressure at a pump, height of control gates, temperature of air and water, soil moisture, just about anything a user might want to know about the system[5]. With SCADA's telemetry, data can be accessed at any time. SCADA can also be setup to start and stop a system, like when the right amount of water has been applied to a crop

and no more water is needed until the soil water is depleted by the crop to the point where another irrigation is needed. Users can gradually work SCADA into a water delivery system if the user chooses not install a complete SCADA system up front. It can also be applied in canals; the basic startup is with a pressure transducer and a data-logger. The data-logger is connected to the electronic readout on pressurized systems, and to the pressure transducer on canal systems. Basic data for water users to collect is the diverted water and widrawn water. For pressurized systems, the basic startup is with electronic readout on the meter for diverted water and widrawn water, a data-logger, and either a PDA or laptop computer. The timing of data collection by the data-logger is determined by the user and at whatever intervals the user prefers.

[Fig. 2] SCADA controlling irrigation utilities

6. The Negative Aspect of SCADA Over CI

When SCADA controls critical infrastructure, it also will become a target for terrorist. Therefore strict security should be implemented. Previously there are some cases where SCADA malfunctioned and it caused great damage to the society. Failure of SCADA systems can produce damage. Vandalism By The Public Is Also A Risk. Here is some example of incidents that happened due to hacking SCADA systems:

- MOSCOW, April 26 1999, Hackers Cracked Gazprom Security World's largest natural Gas Company lost control of gas flows for some time.
- June 10, 1999, a 16” Olympic Pipeline Company pipeline ruptured and released 237,000 gallons of gas into a creek in Bellingham, Washington[6-7].
- The El Paso Natural Gas 30” Pipeline rupture and fire near Carlsbad NM, August 19, 2000.

7. Steps to Meliorate SCADA Controlled CI’s

Supervisory Control And Data Acquisition System was initially designed to maximize functionality, leaving

little attention to security. This makes SCADA vulnerable to process redirection, disruption of service or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Here are some steps to improve SCADA in Critical Infrastructure[7]:

7.1 Do Not Rely on Proprietary Protocols to Protect System

SCADA systems use unique, proprietary protocols for communications between field devices and servers.

Often the security of SCADA systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, demand that vendors disclose any backdoors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured.

7.2 Implement Intrusion Detection Systems and Incident Monitoring

To be able to effectively respond to cyber attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day; this capability can be easily set up through a pager. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

7.3 Disconnect Unnecessary Connections to The SCADA Network

Isolate the SCADA network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the SCADA network must be a primary goal to provide needed protection. Strategies such as utilization of demilitarized zones and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks.

7.4 Identify All Connections to SCADA Networks

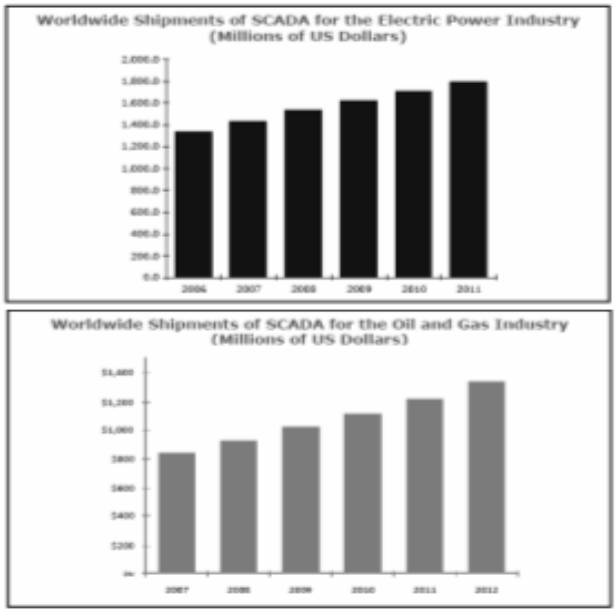
Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network.

Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

7.5 Establish A Strict And on Going Risk Management Process.

Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective.



[Fig. 3] The increase of demand for SCADA in CI utilities[8]

8. Conclusion

Supervisory control and data acquisition (SCADA) networks includes computers and applications that perform key functions in providing commodities and essential services like electricity, transportation, gasoline, water, natural gas, waste treatment to all[8]. In short, SCADA controls most of Critical Infrastructures. The next figure shows the increasing demand for SCADA. With this increasing demand, the number of threats also increases.

Therefore, it is important to focus on the security of SCADA systems and control systems since they control most Critical Infrastructures today.

References

[1] Critical infrastructure - Wikipedia http://en.wikipedia.org/wiki/Critical_infrastructure
Accessed: December 2008

[2] D. Bailey and E. Wright, Practical SCADA for Industrym, 2003.

[3] Houghton Mifflin Company. Boston, MA, The American Heritage Dictionary of the English Language, Fourth Edition, 2000.

[4] Executive Order 13010, Critical Infrastructure Protection. Federal Register, Vol. 61, No. 138, July 17 1996.

[5] SCADA systems for measuring and managing water
http://www.ecy.wa.gov/programs/wr/measuring/images/pdf/scada_systems.pdf
Accessed: December 2008

[6] http://www.council2.com/paper151/pipeline.html Accessed: December 2008

[7] http://www.ntsb.gov/publictn/2003/PAR0301.pdf Accessed: December 2008

[8] ARC Advisory Group Study Brochures
http://www.arcweb.com/StudyBrochurePDFs/Forms/AllItems.aspx Accessed: December 2008

Authors

L. Arockiam

He is working as a Lecturer (SG) in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has published many research articles in the International / National Conferences/Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored a book on "Success through Soft Skills". His research interests are: Software Measurement, Cognitive Aspects in Programming, Web Mining and Mobile Networks.