Design on SCADA Test-bed and Security Device

Sungmo Jung, Jae-gu Song, Seoksoo Kim
Department of multimedia, Hannam University, Korea
SungmoJ@Gmail.com, bhas9@paran.com, sskim@hnu.kr

Abstract

Most of the national critical key infrastructure, such as power, piped gas and water supply facilities, or the high-speed railroad, is run on the SCADA (Supervisory Control and Data Acquisition) system. Recently, concerns have been raised about the possibility of these facilities being attacked by cyber terrorists, hacking, or viruses. Thus, it is time to adopt the relevant security management techniques.

This study analyzes the vulnerabilities of SCADA systems through scenarios, designs a test-bed to prove such vulnerabilities, and suggests security devices..

Keyword*: SCADA Test-bed, SCADA Security Device, Modbus Serial Communication*

1. Introduction

The rapid development of information-communication technology in recent years has allowed large-scale facilities such as a railway, a power system, and a power plant to be operated by control systems. A control system is a computer-based system adopted by a number of infrastructure facilities and industries in order to monitor or control delicate processes as well as physical functions. The system collects data from the field and sensors, displays information, and executes sequential commands of local/remote devices. Such large-scale plant networks, based on the control systems, are mainly operated by the government and designated as key infrastructure facilities. What they have in common is that every device is connected with each other or with an external device to make possible remote access/control and equipped with the interactive communication environment for operating systems and giving commands. This environment in a broad sense is called SCADA (Supervisory Control and Data Acquisition), a kind of a control system including DCS (Distributed Control System) which is applied to plants executing distributed processes.

Most governments operate SCADA systems in closed networks and use a vendor's own operation systems/protocols, which makes the systems safe from cyber-attacks. However, when the need for maximum efficiency or external service arises, attempts will be made to connect the systems to the Internet or commercial networks. This allows the public to share all the information operated by the government but the system could be vulnerable to fatal damage [1] inflicted by hackers.

The previous operation of key infrastructure facilities was safe from hackers because of local control, exclusive lines, real-time operation systems, private protocols, terminal PLC, and so on. Yet, more efficient management may need to introduce centralized remote control, TCP/IP network-based protocols, and PCs with common operation systems, which increases security problems [2]. Table 1 shows the comparison of control and information networks.

Table 1. The Comparison of Control and Information Networks

Classification	Control Networks (SCADA)	Information Networks (MIS)
O/S	Real-time O/S	General-purpose O/S (Windows, Linux)
Main Computer	Main Frame	Server
Terminal	PLC	PC
Network	Closed Networks	Opened Network Commercial Network
Protocol	MODBUS Industrial Ethernet	TCP/IP
Feature	Time Critical	Data Critical
Operation Core	Electric / Electron Works	Computation / Computer Works
Construction	Bundle Progress	Order Progress

The SCADA systems have been operated for infrastructure based on closed networks. However, if aging systems are replaced by new internet worked units, it may cause serious vulnerabilities to threats of hackers.

Recent cyber threats tend to increasingly focus on SCADA systems, and once the system is attacked, the damage affects a multitude of people and national reputation is severely impaired. As hacking skills become more intelligent, preventive security measures shall be highlighted even more. For example, Gartner's report [3] released in January 2004 pointed out serious vulnerabilities of major infrastructure facilities such as railway, power system networks, a power plant and a dam. That is, development of IP technology increases security threats to SCADA systems, making them a major target of cyber attacks since 2005. Originally, SCADA systems are operated in closed networks, safe from hackers who attempt remote access, but business rationalization calls for use of the Internet and common controllers using TCP/IP, exposed to fatal damage that hacking tools may incur [4].

Thus, this study is aimed to analyze the vulnerabilities of SCADA systems through virtual scenarios, design a test-bed to verify such vulnerabilities, and suggest security devices.

2. Related Works

2.1. SCADA System

SCADA is an acronym for Supervisory Control and Data Acquisition. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals [5]. A SCADA system gathers information (such as where a leak on a pipeline has occurred), transfers the information back to a central site, then alerts the home station that a leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. These systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or very complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system. Traditionally, SCADA systems have made use of the Public Switched Network (PSniffing) for monitoring purposes. Today many systems are monitored using the infrastructure of the

corporate Local Area Network (LAN)/Wide Area Network (WAN). Wireless technologies are now being widely deployed for purposes of monitoring [6].

SCADA systems consist of:

• One or more field data interface devices, usually RTUs, or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators

• A communications system used to transfer data between field data interface devices and control units and the computers in the SCADA central host. The system can be radio, telephone, cable, satellite, etc., or any combination of these.

• A central host computer server or servers (sometimes called a SCADA Center, master station, or Master Terminal Unit (MTU)

• A collection of standard and/or custom software systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices

Figure 1 shows a typical SCADA system.

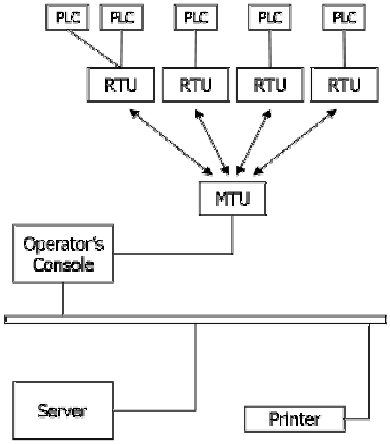

Figure 1. Typical SCADA System

This research uses a scenario that a hacker gets an access to internal networks of a SCADA system as depicted in Figure 1 in order to design an SCADA test-bed for Sniffing attacks targeting MTU (RS485 multiport) and RTU.

2.2. SCADA Communication Methods and Media

An SCADA system uses MODBUS communication, represented by RS232, RS422 and RS485. Therefore, this research uses RS485 and RS232, typical protocols, to examine the communication between RTU and SCADA.

In order to realize MODBUS communication, there are two options: installation of interface devices (PCI or PCMCIA type) and use of an RS485 communication converter [7] connected with an RS232 interface built in a computer. And the latter was chosen, taking the expenses into account.

2.3. MODBUS

MODBUS Protocol is a messaging structure developed by Modicon in 1979, used to establish master-slave/client-server communication between intelligent devices. It is a de fact standard, truly open and the most widely used network protocol in the industrial manufacturing environment. The MODBUS protocol provides an industry standard method that MODBUS devices use for parsing messages [8].

MODBUS communication includes MODBUS serial, MODBUS plus and MODBUS TCP/IP. This research employs MODBUS serial which has the following types.

1. RS232(EIA/TIA-232)
2. RS422
3. RS485(EIA/TIA-485)

The transmission mode defines the bit contents of the message bytes transmitted along the network, and how the message information is to be packed into the message stream and decoded.

Standard MODBUS networks employ one of two types of transmission modes:

1. ASCII Mode
2. RTU Mode

The mode of transmission is usually selected along with other serial port communication parameters (baud rate, parity, etc.) as part of the device configuration.

In the ASCII Transmission Mode (American Standard Code for Information Interchange), each character byte in a message is sent as 2 ASCII characters. This mode allows time intervals of up to a second between characters during transmission without generating errors.

In RTU (Remote Terminal Unit) Mode, each 8-bit message byte contains two 4-bit hexadecimal characters, and the message is transmitted in a continuous stream. The greater effective character density increases throughput over ASCII mode at the same baud rate.

This study designed a test-bed based on RTU mode.

2.4. Expected Hacking Method: Packet Sniffer

A packet sniffer is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network [9]. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC (Request for Comments) or other specifications.

The versatility of packet sniffers means they can be used to:

1. Analyze network problems.
2. Detect network intrusion attempts.
3. Gain information for effecting a network intrusion.
4. Monitor network usage.
5. Gather and report network statistics.

6. Filter suspect content from network traffic.
7. Spy on other network users and collect sensitive information such as passwords (depending on any content encryption methods which may be in use)
8. Reverse engineer protocols used over the network.
9. Debug client/server communications.
10. Debug network protocol implementations.

Example uses as following:

3. A packet sniffer for a token ring network could detect that the token has been lost or the presence of too many tokens (verifying the protocol).
4. A packet sniffer could detect that messages are being sent to a network adapter; if the network adapter did not report receiving the messages then this would localize the failure to the adapter.
5. A packet sniffer could detect excessive messages being sent by a port, detecting an error in the implementation.
6. A packet sniffer could collect statistics on the amount of traffic (number of messages) from a process detecting the need for more bandwidth or a better method.
7. A packet sniffer could be used to extract messages and reassemble into a complete form the traffic from a process, allowing it to be reverse engineered.
8. A packet sniffer could be used to diagnose operating system connectivity issues like web, ftp, sql, active directory, etc.
9. A packet sniffer could be used to analyze data sent to and from secure systems in order to understand and circumvent security measures, for the purposes of penetration testing or illegal activities.
10. A packet sniffer can passively capture data going between a web visitor and the web servers decode it at the HTTP and HTML level and create web log files as a substitute for server logs and page tagging for web analytics.

3. Vulnerability Analysis

3.1. Virtual Scenarios

It is not easy to have access to internal networks of the typical abovementioned SCADA system by hacking into external networks. Yet, a number of hacking tools and sources for common protocols are distributed on the Internet and, even if there is a plenty of preventive measures for such open source software, the system cannot be 100% safe from highly intelligent hackers. Hence, the scenario renders a situation that a high-level hacker attacks external networks and gets access to the internal ones to deliver Sniffing attacks on the SCADA system.

Figure 2 shows how a hacker approaches internal networks through the Internet and Figure 3 how he delivers Sniffing attacks.

The hacker:

1. Collects data from websites possibly connected with SCADA systems
2. Approaches services related with plant facilities through the Internet (such as TCP/IP)
3. Finds methods to avoid firewalls after examining whether or not he can have access to websites or website managers (such as Stealth Scanning)
4. Collects information to prepare attacks
5. Obtains an account of an administrator or vice-administrator
6. Collects information for remote access to SCADA systems (RTU)
7. Attempts access to SCADA systems
8. Finds out vulnerability related with the possibility of access and control (such as Sniffing)

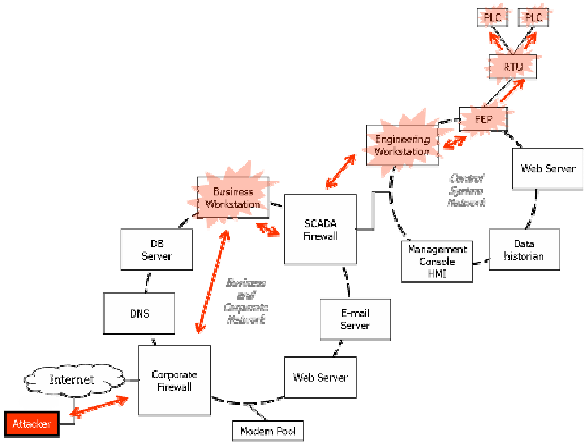

Figure 2. Virtual Scenarios

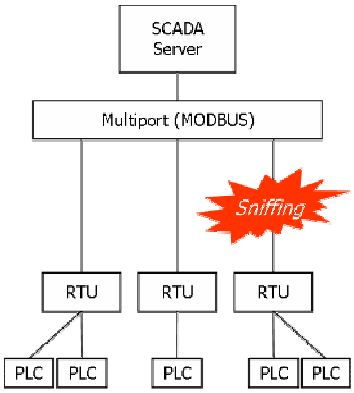

Figure 3. Sniffing Attacks

3.2. Evaluation Factors

The following evaluation factors have been drawn from the scenario.

1. Level of exposure of SCADA systems
2. A port of which the access is available (such as TCP/IP, MODBUS)
3. Access to websites connected with SCADA
4. Vulnerability of websites connected with SCADA
5. Vulnerability of RTU and MTU
6. Status of common firewalls

The security of SCADA system is evaluated mainly by the level of the network connection. Figure 4 shows how 4 steps of general asset analysis can be applied to SCADA.

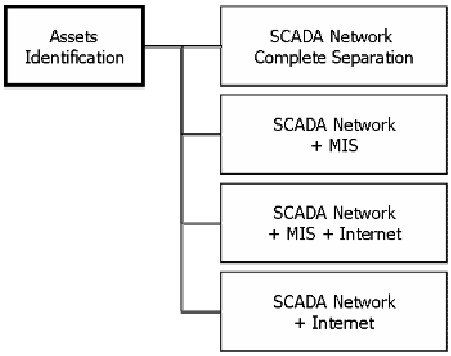

Figure 4. Assets Identification Analysis for SCADA System

As depicted in Figure 4, asset identification includes 4 factors, analyzing the level of connection between SCADA networks and information networks. General security measures are sufficient for completely separated networks like no.1 and no.2. But more technical measures are necessary for networks including contact points for the internal SCADA networks such as no.3 and no. 4. And this study considers hacking from the outside through these contact points, for it is based on a virtual scenario including contacts with internal networks.

When it comes to security design, security measures for interworking points between SCADA networks and information networks are more important than those for SCADA networks. Yet, no security design can be completely safe from high-level hackers who do not use common hacking tools. Therefore, this study provides a test-bed to evaluate a possibility of Sniffing attacks inflicted by a hacker, who has already invaded the internal networks.

3.3. Open Tools for Access to SCADA systems

Generally, open tools, allowing access to SCADA systems using the Internet as a contact point, are as follows.

1. NMAP: Port Scan
2. Nessus: Security Vulnerability Checking Tools
3. Wireshark: Network Analysis

4. Google: Correct Open Information
5. WinHTTrack
6. Netcraft: Internet Monitoring Cooperation. Offer of Servers Operating Times and O/S Information
7. Kartoo: Meta Searching Engine for represent visual Interface about result
8. Newest Scanning and Hacking Tools etc.

4. Design of Test-bed and Security Device

4.1. Sniffing-Detect

Generally, it is possible to peep at a packet of a recipient in a HUB environment only by setting up NIC as Promiscuous from Non-promiscuous.

The SCADA systems, however, have a structure that a packet is sent to only the target recipient, using a switch environment, and thus it is not possible for a hacker to peep at packets even if he sets up the interface as Promiscuous mode. Yet, there are numerous Sniffing attacks available even in switch-using systems such as Switch Jamming, ARP Redirect, ICMP Redirect and SPAN/Monitor port setup.

Figure 5 shows vulnerability in RTU mode, which needs time interval of at least 3.5char in order to send a message. And it is possible to make Sniffing attacks on a packet during this idle state.

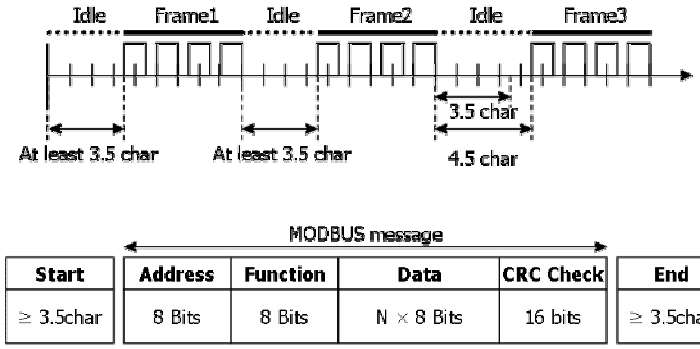

Figure 5. MODBUS Specification

In order to solve this problem, Tx and Rx should be monitored as a packet is sent from Master to Slave.

Figure 6 suggests Sniffing-Detect for the purpose.

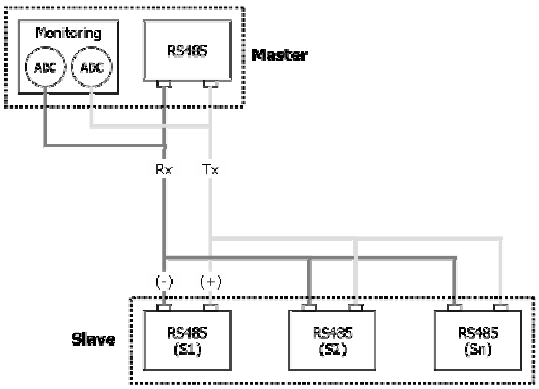

Figure 6. 3.5Char Interval & Data Bus Monitoring

4.2. SCADA Test-bed

SCADA systems truly need security measures but their application to previous systems renders various challenges. In particular, operation of existing SCADA systems or devices shall not be suspended when security measures are applied. Therefore, this research also provides a test-bed that can analyze threats or vulnerability before formulating security measures for SCADA systems.

Figure 7 shows the test-bed, and details are as follows.

1. SCADA Server : Cimon or AutoEye10, Windows O/S
2. RS485 Multiport : MOXA
3. RTUs
4. FEP & IEDs
5. Simulator : Digital I/O, Analog I/O
6. Standard Protocol : MODBUS

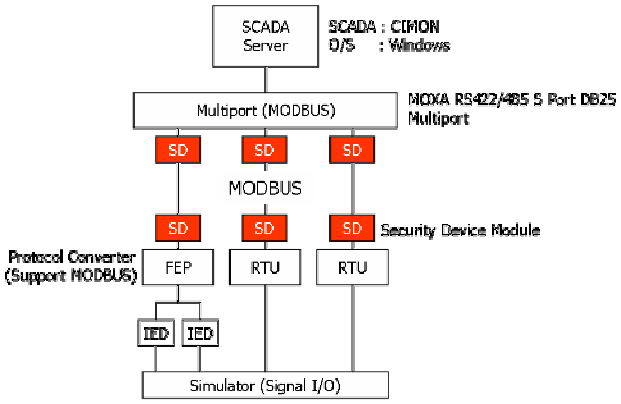

Figure 7. SCADA Test Bed

4.3. Structure of Prototype Security Device

Figure 8 depicts a prototype of the designed security device. Its operation system is Embedded Linux to deal with OpenSSL, SEED and MODBUS codes more flexibly while the communication ports are RS232 and RS485(2 for each), which is major serial communication. Also, the security device includes 2 Ethernets(TCP/IP), which most SCADA networks employ in order for program updates in task form and debugging. It inspects interrupts of a communication port also and processes them in task form.

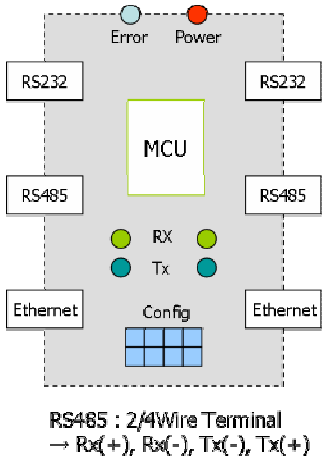

Figure 8. Security Device Prototype

4.4. Effects of the Designed Security Device

The prototype device uses SEED, a symmetric key block encryption algorithm. SEED employs the same key for encryption/decryption in information-processing system and telecommunication networks. In addition, SEED has feistel structure in which plaintext is encrypted through 128-bit block cipher algorithm through several rounds.

Table 2 shows the efficiency of the prototype device assuming that the structure of SCADA network is 100.

Table 2. Comparison of an SCADA network and that adopting the prototype device

Classification	Adopting the Prototype Device SCADA Network
Speed	80
Stability	200
Cost	170
Applicability	70

5. Conclusion

Paradigms shift in information security calls for analysis of threats to key infrastructure as well as corresponding response measures. In case attacks are made on unspecific systems and damage inflicted on the key infrastructure, the public could be the victims also. More recently, anyone can deliver cyber-attacks using open tools available on the Internet and,

thus, the infrastructure is more vulnerable to the threats, which may cause large-scale and wide-area damage that could even paralyze the society.

Although security of SCADA systems cannot be overemphasized, application of proper measures is not easy. Even when vulnerability could be analyzed and measured as suggested, suspension of systems in operation is not easily available.

Therefore, as SCADA systems may introduce centralized or automatic management, and damage to the system could cause enormous social or individual loss, this study aims to provide a virtual scenario designed to analyze vulnerability of communication protocols and to offer SCADA security test-beds based on RTU mode as well as a prototype security device, making possible effective SCADA systems with improved security.

In the future, a research dedicated on implementation of detail testing about hacking tools by the study at site shall be conducted. Furthermore, as many of assessment tasks in the construction industry are interlinked and information sharing among these tasks are crucial, researches dedicated for improving efficiency of assessment tasks and work flow are essential in the future.

5. References

[1] National Intelligence Service, 2004 The White Paper of National Information Security, http://www.nis.go.kr, 2004

[2] GAO, Critical Infrastructure Protection: Challenge and Efforts to Secure Control System, http://www.gao.gov, Mar. 2004

[3] David L, Fraley, Cyberwarfare: VoIP and Convergence Increase Vulnerability, Gartner Report, http://www.gertnder.com, Jan. 2004

[4] Ron Derynck, Cyber-Security and System Integrity for Transportation Networks, Verono White paper, 2004

[5] Technical Information Bulletin 04-1, Supervisory Control and Data Acquisition (SCADA) Systems, NCS TIB 04-1, Oct. 2004

[6] McClanahan, R.H., The Benefits of Networked SCADA Systems Utilizing IP-Enabled Networks, Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C5 - C5_7

[7] LCS-485 Converter (USB to Serial 2p RS432/485), http://kunhocom21.co.kr /product/productView.php?nProdCode=61019&service_id=pcdn

[8] Introduction to MODBUS, Technical Tutorial, Dec. 2002

[9] What is a packet sniffer?. tech-faq.com. Retrieved on Mar. 2008

Authors

Sungmo Jung

In 2008, he received the B.S. degree in Department of Multimedia from Hannam University, Daejeon, Korea. Now, he is working on the Master's degree in Multimedia Engineering from Hannam University. His research interests include Software Engineering, Embedded database systems and Sensor network.

Seoksoo Kim

Received a B.S. degree in computer engineering from Kyungnam University , Korea, 1989, and M.S. degree in Information engineering from Sungkyun-kwan University, Korea, 1991 and Ph D. degree in Information engineering from Sungkyun-kwan University, Korea, 2002. In 2003 he joined the faculty of Hannam University, Korea where he is currently a professor in Department of Multimedia Engineering. His research interests include Multimedia Communication systems, Distance learning, Multimedia Authoring, Telemedicine, Multimedia Programming, Computer Networking. Information Security. He is a Member of KCA, KICS, KIMICS, KIPS, KMS, and DCS.