A Study on Improving the Security Vulnerabilities of Modbus-Based SCADA Control Systems

Giovanni A. Cagalaban*, Seoksoo Kim*, Kyung-jae Ha*
*Dept. of Multimedia Engineering, Hannam University
**Dept. of Computer Engineering, Kyungnam University

Modbus 기반 SCADA 제어 시스템의 보안 취약성 향상에 관한 연구

조바니 카가라반*, 김석수*, 하경재**
*한남대학교 멀티미디어공학과
**경남대학교 컴퓨터공학부
e-mail:gcagalaban@yahoo.com

요 약

SCADA control systems and protocols are developed based on reliability, availability, and speed but with no or little attention paid to security. Specifically in Modbus protocol, there are inherent security vulnerabilities in their design. The lack of common security mechanisms in the protocol such as authentication, confidentiality and integrity must be addressed. In this paper, security vulnerabilities of Modbus-based SCADA controls systems will be studied. An in-depth analysis of the message frame formats being sent between master and slave will be discussed to expose the security vulnerabilities. This will enable SCADA users to find ways to fix the security flaws of the protocol and design mitigation strategies to reduce the impact of the possible attacks. Security mechanisms are recommended to further enhance the security of SCADA control systems.

1. Introduction

Many infrastructures and industries use computer-based systems, commonly known as to remotely control sensitive processes and physical functions previously controlled manually by its operators. These systems, commonly known as Supervisory Control and Data Acquisition (SCADA), allow a physical system such as water utility to collect data from sensors and control equipment located at remote sites [1].

SCADA systems have traditionally used combinations of radio and direct serial or modem connections to meet communication requirements. Protocols are designed to be very compact and many are designed to send information to the master station only when the master station polls the Remote Terminal Unit (RTU).

Hundred of both proprietary and non-proprietary protocols have been developed for serial, LAN and WAN based communications in a wide variety of industries including automotive, transportation, and electrical distribution. Among the protocols that currently dominate the industrial marketplace include protocols such as Modbus, Ethernet, Profibus, IEC 60870 and DNP3.

Modbus has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices. It emerged because it is good, simple to implement and are adapted by

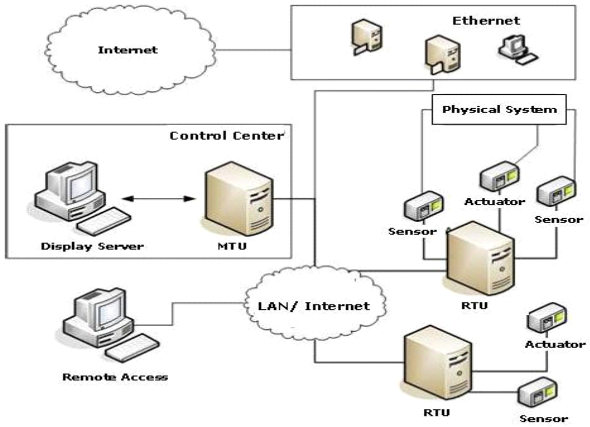
many manufacturers.

Despite the fact that Modbus standard is flexible and easy to implement, it has some inherent protocol vulnerabilities that SCADA users must be concerned with. There are security weaknesses that are built into the protocol specification and not the result of programming or design errors.

This paper will study the vulnerabilities of SCADA control systems based on Modbus protocol by using a rigorous analysis of specifications. The inherent lack of security in the message frames specifies the security flaws of Modbus which will be discussed in this paper. The paper will then expose the vulnerabilities of Modbus and an attack scenario will also be given.Then security measures will be presented to address the security weaknesses of Modbus-based SCADA control systems.

2. Related Study

SCADA system operation involves real time data exchange from the field devices as well as with other control systems such as Distributed Control System (DCS) and Plant Information (PI) systems. Protocols allow these data exchanges to occur as well as the RTU/SCADA units to communicate with each other. Figure 1 shows a typical SCADA architecture.



[Fig. 1] SCADA Architecture

Understanding the network architecture of SCADA control systems is critical to effectively evaluate their security status. At the lowest level, the field devices are proprietary devices running embedded operating systems. These devices originally used serial communications to report to the centralized control center utilizing field bus protocols like Modbus. Given the low bandwidth connections, these devices reported on a polling basis or a report-by-exception basis to minimize network traffic. The SCADA controller is responsible for managing all of these communications, analyzing the data, and displaying the alerts and events on the human machine interface (HMI) systems.

Byres [2] analyzed SCADA protocol vulnerabilities and specifically in Modbus protocol, he suggested the use of attack trees to define a series of attacker goals, determine possible means to achieve that goal and identify the weak links of the system. He identified some robustness issues the lack of command and session structure as well as simplistic framing technique.

Currently, Modbus-based SCADA control systems have no existing solutions that address specifically the Modbus protocol over Ethernet links. Despite the inherent lack of security in the design of Modbus, no security tools exist that are geared toward the detection of malicious Modbus traffic.

3. Modbus Vulnerabilities

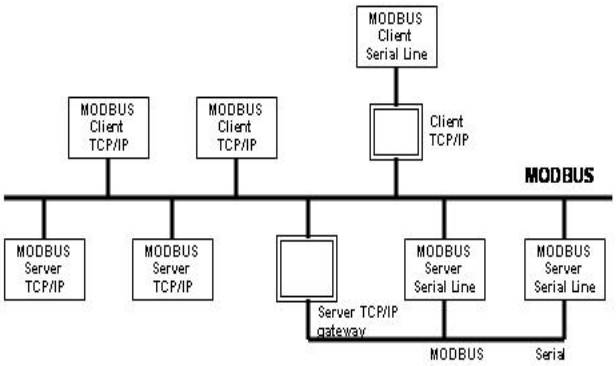
Modbus is an application-layer messaging protocol which is situated at level 7 of the Open Systems Interconnection (OSI) model [3]. Considered as a de facto communications protocol in industries since 1979, Modbus continues to enable millions of automation devices to communicate with each other. Modbus is a request/reply protocol and offers services specified by function codes. Besides the standard Modbus protocol, there is another Modbus protocol, called Modbus Plus.

Modbus RTU format uses binary coding which makes the message unreadable when monitoring but reduces the size of each message which allows for more data exchange in the same time span. When devices communicate on a Modbus serial line using the RTU mode, each 8-bit byte in a message contains two 4-bit hexadecimal characters.

Modbus ASCII is human readable, and more verbose [4]. They are coded in hexadecimal values represented with readable ASCII characters. Character 0..9 and A..F are used for coding. When devices are setup to communicate on a Modbus serial line using American Standard Code for Information Interchange (ASCII) mode, each 8-bit byte in a message is sent as two ASCII characters.

Use of Modbus/TCP also eliminates the need

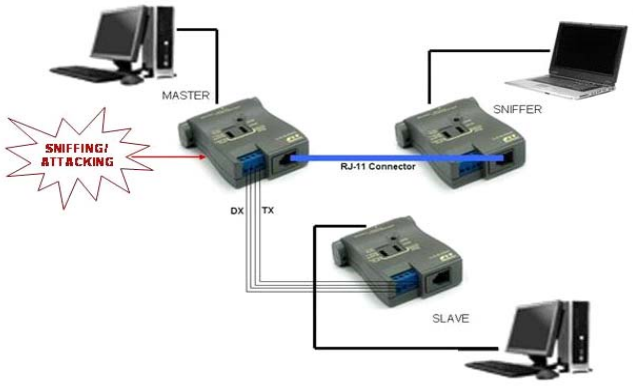
to use a gateway to get to the internal network, and makes it easier to integrate other devices such as security appliances, smart cards and bar code scanners. Connectivity to the IP-based business network also allows remote control of devices without having to issue commands from the control room. See Figure 2 for the communication architecture of Modbus TCP.



[Fig. 2] Modbus TCP Communication Architecture

4. Attacking the Modbus Protocol

To perform the exploitation of Modbus security vulnerability, a control function scenario is set up. The hardware configuration is show in Figure 3 where there is one computer that serves as the master, another was assigned as the slave and the third as the intruder (attacker). In the physical configuration, RS232 to 485 transceivers we set up to connect each computer. While two devices communicate with each other using RS transceivers, a third (attacker) device monitors messages sent by the master to the slave and perform exploitation of security vulnerabilities of the system.



[Fig. 3] Modbus TCP Communication Architecture

This type of exploitation of security vulnerability is a man in the middle attack. It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker [5].

5. Securing SCADA

There are security considerations to make in order to strengthen SCADA networks. One security consideration is to improve security in the design of the SCADA network and to develop efficient security-monitoring tools. The security mechanisms developed to address this security issues will ensure that even if an attacker manages to enter the SCADA network, it will be difficult to carry out any sort of attack. The security monitoring tools will provide cryptography and help detect intrusions and other suspicious activities on the network. Another security consideration is to improve the security management of the SCADA network. The following are security consideration to be applied to strengthen SCADA cyber security.

5.1. Firewalls and intrusion detection systems

The installation of a firewall blocks unauthorized traffic from entering the protected network. It prevents the establishment of a direct connection from the outside Internet to the local SCADA network [6]. They can be configured to control and monitor the activities of authorized entities accessing the network. Despite certain limitations of intrusion detection systems (IDS), they can be paired with firewall in recognizing monitoring malicious attacks to the networks [7].

5.2. Cryptography and key management

There are numerous cryptographic tools exist that aid in improving the security properties of a particular system. However, SCADA protocols are initially designed not to support any sort of security more so in cryptography. This security feature is very useful in securing SCADA networks. The uniqueness and complexity of the design of SCADA networks make it difficult to adapt existing cryptographic techniques into these systems. Some constraints include the limited computational capabilities of SCADA devices and low-rate data transmission on SCADA networks which makes implementation of cryptography in SCADA protocols difficult and complicated.

5.3. Security management

For a system to have a good security, it requires good management aside from efficient use of proper security technologies. Nowadays, more and more companies have developed good use of information technology in security practices. So, SCADA industries need to improve their security management. They must have security policy that must be comprehensive and clearly define the procedures that must be implemented to achieve the security objectives.

5.4. Protocol vulnerability assessment

It is necessary to analyze existing protocols and understand the vulnerabilities present in the protocols to strengthen the security features of a system. This will aid the implementation of security mechanisms that can be included into the protocol definitions. An understanding of the protocol vulnerabilities would also help in developing rules for IDS. For instance, it is possible to develop attack signatures for each of the potential exploits, which could be included in the IDS. SCADA network administrators will find these IDS signatures useful for monitoring the security of their networks.

6. Conclusion

The interconnectivity of SCADA networks continue to grow which exposes itself to an increasing risk of cyber attacks and thus there is a critical need to improve the security of these SCADA networks. This study describes the general SCADA architecture, security vulnerabilities and attacks to these networks which can prove harmful to everyone as well as to a whole nation. The security attacks and vulnerabilities in these networks are also discussed followed by security considerations for SCADA networks to employ.

As such, it is beneficial to formulate and enforce security measures to strengthen the cyber security of SCADA networks. This study describes methods to exploit vulnerabilities of Modbus protocol based SCADA systems and recommends the security measure that are beneficial to improve the overall security of SCADA networks.

References

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

[2] Byres E., Understanding Vulnerabilities in SCADA and Control Systems October 2004.

[3] http://www.modbus.org/specs.php

[4] http://www.Modbus-IDA.org, October 2006.

[5] http://en.wikipedia.org/wiki/ Man-in-the-middle_attack

[6] http://en.wikipedia.org/wiki/Firewall

[7] http://en.wikipedia.org/wiki/ Intrusion_detection_system