Cyber Threats and Defence Approaches in SCADA systems

Dong-Ho Kang, Byoung-Koo Kim, Jung-Chan Na

Convergence Security research Section,

ETRI(Electronics and Telecommunications Research Institute), Korea

{dhkang,bkkim05,njc}@etri.re.kr

***Abstract*— The use of SCADA systems has been increased since the 1960s as a need arose to more efficiently monitor and control the status of remote equipment. And they are becoming more and more susceptible to cyber-attacks due to utilize standard protocols and increase connectivity. The objective of this paper is to introduce our on-going work and discuss challenges and opportunities for preventing network and application protocol attacks on SCADA systems.**

***Keywords*— Industrial Firewall, Cyber-attacks, ICS Security, Network Security, SCADA**

I. INTRODUCTION

In general, SCADA (Supervisory control and data acquisition) systems include systems, software, and networks used to monitor and control various physical infrastructures or facilities in industrial environments. In the past these systems were completely physically isolated environments from external networks and used proprietary hardware and protocols [1][2]. But modern SCADA systems have distributed architecture and are connected to the corporate network and even to the Internet. As well, these systems use general-purpose operation systems and industry-standard communication protocols such as Modbus, DNP3 for communication between a SCADA System and field devices such as PLC, RTU. The increased connectivity and the use of standard protocols can help to optimize manufacturing and distribution processes, but it also exposes the safety-critical industrial network to the myriad security problems of the Internet [3]. To solving that problem, a challenge that SCADA systems face is that security technologies used in enterprise networks must be adequately deployed in a SCADA network. We are developing an industrial firewall based on network security concepts and technologies used in enterprise environments.

The objective of this paper is to introduce our on-going work and confirm the validity of our approach for preventing network and application protocol attacks on SCADA systems. For that, this paper is organized as follows. In the next section, we address the general SCADA architecture and protocols. Section III presents cyber-attacks characteristics of SCADA networks and defence approaches. Section IV introduces our research and Section V is given conclusions.

II. SCADA ARCHITECTURE AND PROTOCOL

This section provides an overview of the traditional SCADA architecture and Modbus protocol.

A. The SCADA Architecture

SCADA systems are used to monitor and remotely control critical industrial processes while providing human operators with continuous, real-time information about the current state of those processes. They were initially targeted for on-site automation, they were modified over time to allow remote downloading of logic and configuration changes which enabled them to be used in widely dispersed geographical locations [4]. Figure 1 shows the architecture of a typical SCADA system.

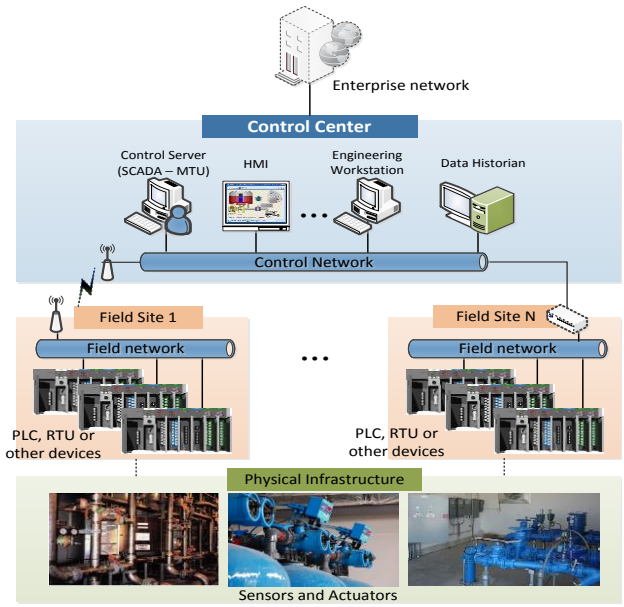

Figure 1. SCADA system General Layout

The SCADA architecture usually has the following three different areas [5].

- A control network includes HMIs, SCADA servers and historian systems for process control, the gathering of

data in real time from field devices in order to control sensors and actuators.

- A field network contains multiple field devices that send commands to actuators and provide the data received from sensors to SCADA servers.
- Physical infrastructure consists of many different types of sensors and actuators that are monitored and controlled by a field device.

Most SCADA systems generally tend to have static topologies, a limited number of application protocols and regular communication patterns [6][7].

B. Modbus Protocol

Modbus is an application layer messaging protocol which provides client/server communication between devices in SCADA systems and offers services specified by function codes [8].

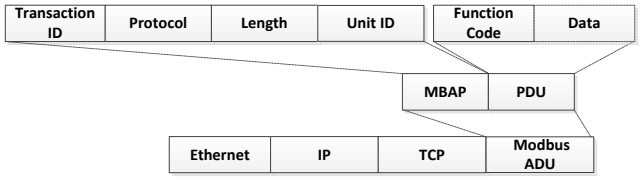

Figure 2. The format of Modbus TCP/IP ADU

The client (or master) that initiates a Modbus transaction builds the Modbus ADU (Application Data Unit). The Modbus ADU is consists of the MBAP (Modbus Application Protocol) header and the PDU (Protocol Data Unit). The PDU has a function code and function parameters. The function codes indicate to the server (or slave) which kind of action to perform. The Modbus TCP/IP uses the TCP/IP stack for communication and extends the PUD with an IP header.

There are no security elements in the Modbus. Any attacker that can reach a Modbus server will be able to read and write to the field device as well as reboot the device and run diagnostic commands. The simplicity of the Modbus protocol and widespread availability of free Modbus clients makes it relatively simple to attack a Modbus server [9].

III. CYBER THREATS & DEFENCE APPROACHES

A. Cyber Threats

We surveyed vulnerability assessment tools, Metasploit [10], Nessus [11], and Modscan [12] for the classification of Cyber threats on SCADA systems. These tools are commonly available to find known and newly discovered vulnerabilities on SCADA systems. And we surveyed some reports that were released by DigitalBond's Project Basecamp [13]. As a result of our survey, we describe that various type of attacks on SCADA systems can be grouped into two categories: Network Protocol attacks, Application Protocol attacks

1) Network Protocol attacks

These types of Attacks use weak points of network protocols such as TCP/IP suite that have a number of serious security flaws. Therefore, most network protocol based attacks happened in Internet environment may be caused in SCADA networks were adopted IP network technologies. We introduce some common types of Network protocol attacks.

TABLE 1. TABLE 1. NETWORK PROTOCOL ATTACKS

Attack Type	Attacks
Host Discovery	OS Fingerprinting
Scan	TCP SYN/ACK Scan TCP connect( ) Scan TCP FIN Stealth Scan Xmas Tree Stealth Scan TCP Null Stealth Scan Windows Scan RPC Scan Version Detection Scan
DoS attack (Denial-of-Service)	TCP/UDP Flooding Smurf Attack

Host Discovery is the process for gathering information about each host, such as its operating system and version to verify whether they can be accessed or not. Using the information gathered about each target hosts in the host discovery step attackers launches scan to conform what ports are open, with listening services on target systems. Host Discovery and Scan attack are the commonly type of passive attacks to collect the fundamental information of vulnerabilities on target systems. DoS(Denial-of-Service) attack is active attack to make systems or network resource unavailable. Network protocol attacks have two characteristics as the following.

- ***Random access***: these attacks generally send packets with the sequential or random destination addresses and ports to target networks or systems for obtaining the list of target systems and their services.
- ***Source address Spoofing***: DoS attack does not consider about receiving responses to the attack packets. Therefore, Attackers can send packets with a forged source IP address for obscuring the true source of the attack.

To prevent unauthenticated access to field devices in a network connected to an external network it is necessary to implement IP packet filtering between two networks. IP packet filtering will make it harder for network protocol attacks to enter into field devices.

2) *Application Protocol attacks*

In our work, we only surveyed Modbus as application protocol. Application Protocol attacks can cause damage to field devices being controlled by sending out improper commands, because they don't support integrity checking and authentication mechanism. Like network protocol attacks, these attacks also preceded by a step of gathering information about devices for finding vulnerable targets in a network. TABLE 2 shows generally types of application protocol attacks.

TABLE 2. TABLE 2. APPLICATION PROTOCOL ATTACKS

Attack Type	Attacks
Application Scan	Modbus Version Scanner PLC Modbus Mode Identification PLC IO Scan Status Report Slave ID Function Code Scan
Improper command Execution	Force Listen only mode Read/Write Request to a PLC Slave Device Busy Exception Code Delay Acknowledge Exception Code Delay Broadcast Request from an Client

Application protocol attacks have a characteristic.

- ***Unpredictable Command***: SCADA systems generally produce predictable sets of command used for communication between a SCADA server and field devices. On the contrary, Application protocol attacks tend to use unconventional commands at irregularly interval.

Network Intrusion Detection that is capable of recognizing SCADA traffic could detect suspicious or unconventional SCADA commands by inspecting a command value in the payload of all packets.

B. Defence Approaches

1) IP Packet filtering

As we described above, IP packet filtering have been recommended as an effective way to protect field devices from network protocol attacks. IP packet filtering is a network security mechanism used to control network access by monitoring incoming and outgoing packets and allowing them to route or drop based on filtering rules using 3,4 layer on OSI model. This process is shown in Figure 3.

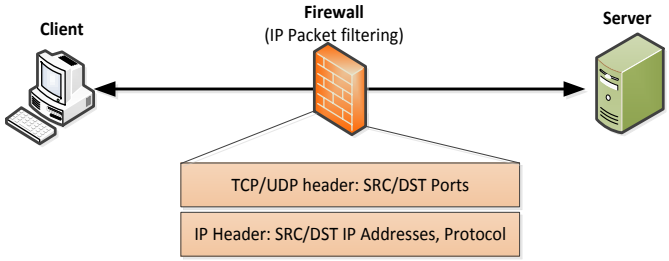

Figure 3. The process of IP packet filtering

The filtering rules (Blacklists or Whitelists) are expressed as a list of conditions and actions until a decision to route or drop the packet is reached. A rule is composed to the source address, the destination IP address, the source port, the destination port and protocol. Most packet filtering systems apply the rules is manually configured by administrators to determine whether to drop or route the packet. Consequently, administrators are forced to know all the services and systems deployed in a network to correctly define the filtering rules. The crucial task of IP packet filtering is that the filtering rules is correctly and completely configured [14].

2) Network Intrusion Detection

Network Intrusion Detection is the most well-known security approach in cyber security techniques. Misuse and anomaly based methods are used for intrusion detection. Misuse based methods are sometimes referred to as signature-based detection trying to detect abnormal behaviour by analysing the given traffic and matching several rules. While misuse detection is effective in known attacks, an obvious limitation of these methods is that they cannot detect new attacks whose signatures are unknown. As the example of research projects on misuse based detection for SCADA systems, Digital Bond developed SCADA IDS pre-processors and provide several attack signatures that have been defined for the open source IDS system Snort [15]. These signatures include some rules for detecting application protocol like DNP3, Modbus based attacks. Therefore, misuse based method could detect abnormal control commands using the predefined SCADA signatures. This method has to sometimes update new signatures for detecting the newly known attacks from external network. But, SCADA systems should be operated in the isolated environment as much as possible from any other network. Because of the reason, IDS based on misuse based method for SCADA is the unsuitable approach.

Anomaly based methods build models of normal data and detects any deviation from the normal model in incoming traffic. Anomaly detection methods have the advantage that they can detect attacks that are not known beforehand. But, anomaly based method have the problem that they often generate false alerts. This problem is especially very critical in a SCADA environment.

Network Intrusion Detection as network security technique to reduce the threat of cyber-attacks on a SCADA network should solve the update of new signatures and the generation of the number of false alerts.

IV. OUR WORK-IN-PROGRESS

We are working on an industrial firewall research project. The aim of the project is to secure communication of SCADA server and field devices. Because of the limited computational capabilities of field devices and the requirement for critical response times from the devices across the network. We don't consider any techniques of cryptography in our works. We studied the ongoing work in SCADA network security areas like firewalls and intrusion detection systems. As a result of study, we designed the industrial firewall that performs deep packet inspection. The firewall is based on whitelists and can inspect Modbus application protocol. In traditional enterprise networks, whitelist based packet filtering technologies has been mostly not used due to unmanageable and unpredictable traffic characteristics. But, most SCADA networks generally tend to have static topologies, a limited number of application protocols and SCADA systems and regularly traffic patterns.

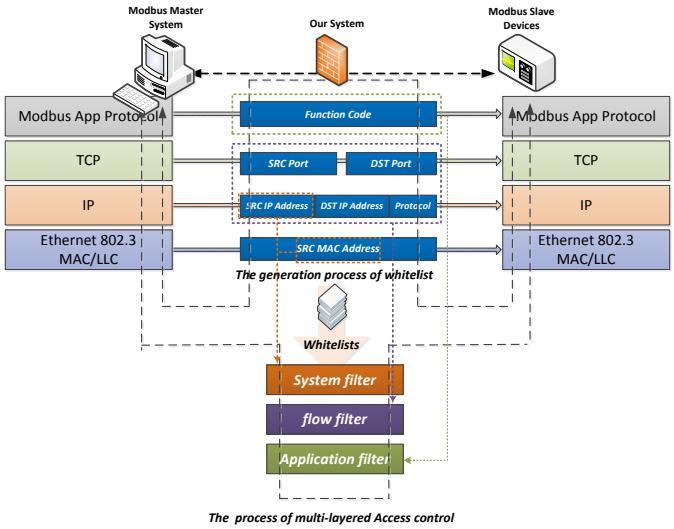

Figure 4. The generation process of whitelists

There are two primary subsystems that make up our system: the automatic rule generation, the multi-layered filtering subsystem. After our system is deployed on a communication path between a control network and a field network, the automatic rule generation subsystem automatically generates whitelists by from traffic captured during specific period of time and transfers them to the multi-layered filtering subsystem. And then the multi-layered filtering subsystem performs the process of filtering with whitelists for preventing network and application protocol attacks on SCADA systems. Our system generates the three types of whitelists. The industrial firewall tries to find the normal characteristics from all packets in generated traffic of SCADA server and field devices and translates the characteristics to whitelists for access control. Whitelists is used to only permit authenticated access to field device from SCADA systems. Our whitelists is composed of system whitelist for system authentication, flow whitelist for legitimate flow and application whitelist for allowable Modbus command. System and flow whitelist is used for preventing network protocol attacks. Application whitelist is for rejecting application protocol attacks. Figure 4 shows the generation process of whitelists and the process of multi-layered filtering in our system. The structure of system whitelist consists of the source MAC address and the source IP address. The structure of flow whitelist is composed of the source/destination IP addresses, the source/destination ports, and protocol. Application whitelists is a list of the function codes of Modbus as allowable commands. When the particular packet matches the condition specified in each whitelist, the packet is routed. If the condition is not matched, the packet is dropped using inbound filtering on a given network interface.

We point out above that the bottleneck problems faced by the existing IP packet filtering and Intrusion detection mechanisms for securing SCADA devices. For overcoming the problems, our system has two characteristics. First, our system generates automatically the filtering rules to decrease the complexity of configuration complexity with IP packet filtering. Second, the filtering rules is generated by our system is used as a table of conditions by the multi-layered filtering.

V. Conclusions

SCADA systems are facing the threat of cyber-attacks due to utilize standard protocols and increase connectivity to external networks. We are working on an industrial firewall research project to decrease various cyber threats on SCADA systems. This paper described cyber-attacks and the existing defence mechanisms. And then, we introduced our project. We have some advantages to solve the bottleneck problems faced by the existing IP packet filtering and Intrusion detection mechanisms for securing SCADA devices.

In our work, the automatic build of the filtering rules is relatively easy. But, it is very hard to confirm whether the authenticated traffic is only routed in the internal network using whitelists in the real world. We will address the evaluation of the proposed approach in our future work.

Acknowledgment

This work was supported by the IT R&D program of MSIP/KEIT. [010041560, A development of anomaly detection and a multi-layered response technology to protect an intranet of a control system for the availability of pipeline facilities]

References

[1] Keith Stouffer, Joe Falco, and Karen Scarfone, "*Guide to Industrial Control Systems(ICS) Security, Special Publication 800-82*", NIST
[2] Brendan Galloway, and Gerhard P. Hancke, "*Introduction to Industrial Control Networks"*, IEEE Communications surveys & tutorials, vol. 15, NO. 2, 2013
[3] V. M. Igure, S. A. Laughter, and R. D, *"Williams. Security issues in SCADA networks*" Computers & Security, 25(7):498--506, 2006.
[4] Shaw, William T, "*Cybersecurity for SCADA Systems*", Tulsa: Penn Well Corporation, 2006
[5] K. Stouffer, J. Falco, K. Kent, "*Guide to SCADA and industrial control systems security*", Special Publication NIST-SP-800-82-2006, NIST, 2006.
[6] R. Barbosa and A. Pras, "*Intrusion detection in SCADA networks*" AIMS, 2010.
[7] R. Barbosa, A. Pras, and R. Sadre, "*Flow whitelisting in SCADA networks*", In Seventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, 2013.
[8] *Modbus Application Protocol V1.1b*3, Modbus Organization, Inc. Retrieved 2 August 2013.
[9] http://www.digitalbond.com/scadapedia/protocols/modbus-2/
[10] http://www.metasploit.com/
[11] http://www.tenable.com/products/nessus
[12] https://code.google.com/p/modscan/
[13] http://www.digitalbond.com/tools/basecamp/
[14] A. Rubin, D. Geer, and M. Ranum, "*Web Security Sourcebook*", Wiley Computer Publishing, 1997
[15] http://www.digitalbond.com/tools/quickdraw/