Customizing Control System Intrusion Detection at the Application Layer

Mai Kiuchi, Eiji Ohba, Yoshizumi Serizawa
Central Research Institute of Electric Power Industry (CRIEPI)
Tokyo, Japan
{mai, ohba, seri}@criepi.denken.or.jp

Abstract: Off the shelf security products such as firewalls, encryption equipment and IDS can be configured for a specific vendor application and protocol implementation to protect internal control system communication and detect attacks. This paper discusses how a set of IDS rules are written and deployed to check the SCADA protocol used by the application, and detect traffic patterns that should not occur during normal operation through the HMI of that application. The rules must be tailored to the particular vendor application, which demands a deep knowledge of the application behavior, but will also yield better results in detecting suspicious traffic aimed specifically at that SCADA application. This paper describes the IDS settings with scenarios such as multiple successive control commands and consecutive commands in a short period of time.

The internal firewall and encryption equipment add layers of security to the system, and by filtering out obviously malformed traffic, they also relieve the IDS of superfluous computation. However, unlike the IDS, they are installed within the communication path and add a certain amount of latency, which may become an issue in a SCADA system demanding real-time processing. This paper presents some evaluation results concerning the latency introduced by encryption and a firewall.

Keywords: Intrusion Detection System (IDS), Application Behavior Analysis, SCADA Security, Latency

1 Introduction

As SCADA (Supervisory Control and Data Acquisition) systems increasingly use standard IT systems, the SCADA system faces security threats common to corporate business systems. Many security measures used in the corporate business system, such as firewalls, access control, encryption, and IDS (Intrusion Detection System), are also applicable to SCADA systems, although special precautions must be taken when introducing the same solutions [1]. Issues particular to SCADA systems include the demand for 100 percent uptime, and little tolerance for extra latency. Another issue is resource restrictions in controllers and other embedded devices commonly used in SCADA systems. It is also necessary to analyze the network traffic flow to configure firewalls and intrusion detection/ prevention systems accurately.

Off the shelf security products such as firewalls, encryption and IDS can be configured for a specific vendor application and protocol implementation to protect internal control system communication and detect attacks. In this paper, we discuss how a set of IDS rules are written and deployed to check the SCADA protocol used by the application, and detect traffic patterns that should not occur during normal operation by an operator using the HMI (Human Machine Interface) of that application. The rules must be tailored to the particular vendor application, which demands a deep knowledge of the application behavior, but will also yield better results in detecting suspicious traffic aimed specifically at that SCADA application. We discuss the IDS settings in a model SCADA system, with attack scenarios using multiple successive control commands and consecutive commands in a short period of time.

The firewall and encryption equipment add layers of security to the system, and by filtering out obviously malformed traffic, they also relieve the IDS of superfluous computation. However, unlike the IDS that only monitors the traffic, the firewall and encryption devices are placed in-line, and add a certain amount of latency, which can become an issue in a SCADA system demanding real-time processing. This paper presents some evaluation results concerning the latency incurred by encryption and a firewall.

2 The Model System and Applied Security Measures

The model SCADA system used in this assessment, and the applied security measures are shown in Figure 1.

It is assumed here that no connections exist between this SCADA system network and the corporate business network of the utility. All the equipment, applications and security measures in the figure belong solely to the SCADA system network, and the placement and settings mentioned below are irrelevant to the corporate business network. If communication between the corporate business network and the SCADA system network is needed, the connection must have a firewall [2], encryption methods and IDS, but such configurations are not discussed here. Another, and perhaps more realistic, way of viewing this model is to assume an attacker has penetrated a security perimeter and now has a presence on the control system network.

The SCADA system master server located in the control center is the direct control and data acquisition interface to the SCADA system equipment. To control the system equipment in the substation, the master server communicates with the server located in the substation, which in turn sends the actual control signals to the equipment. In this model system, the SCADA system equipment is emulated in the same terminal as the substation server. The state information of the equipment and any responses to the control commands are sent through the substation server to the SCADA system master server, and then sent to any communicating HMI's.

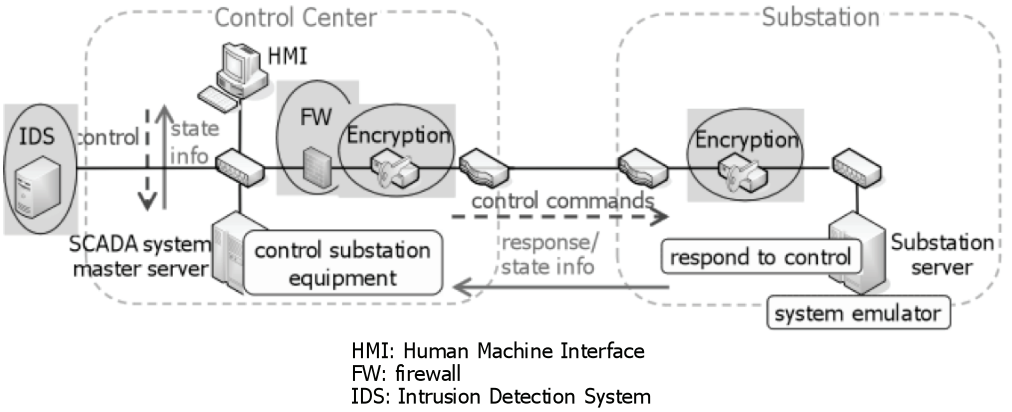

Figure 1 - An Overview of the Model System

The SCADA system is configured to accept only HMI's communicating with predefined IP addresses. The HMI's need a user name and password to access the SCADA application, thus maintaining a certain level of security.

The substation and the control center are assumed to be in physically distant locations. With this assumption, the communication path between the two is encrypted. The encryption and decryption are handled with specialized equipment using symmetric-key cryptography, so that the latency due to encryption is minimized. The encryption equipment checks the IP address of the communication packets, and any unlisted communication packets are not processed. This behavior filters out the less sophisticated attacks that do not have prior knowledge of the used IP addresses.

A firewall is placed in the control center to protect the SCADA system master server, which is a key component in this SCADA system. The firewall checks the IP addresses, ports and the protocol at the TCP/ UDP level. Ideally, there would be an additional firewall to protect the terminals located in the substation, but we considered the control center with the SCADA system master server to have a higher priority.

The IDS sensor is located and configured to monitor all the traffic within the control center. Additional IDS sensors could be placed outside the firewall in the control center to detect incoming attacks and inside the substation to detect more direct intrusions [3]. Again, we prioritized the control center above the substation. However, concerning the application specific IDS rules described in the following section, the basic configuration would be the same regardless of whether the IDS sensor is placed in the substation or the control center.

3 Proposed IDS Settings

Checking the IP addresses, communication ports, and protocols at the TCP/UDP level for non-legitimate connections, and writing IDS rules to match such attacks do not necessarily require knowledge of the protocol details of the SCADA application. This does not mean that such rules are insignificant, but are absolutely necessary to detect

many attacks, and are highly effective [4, 5]. By writing and deploying IDS rules to check the SCADA protocol used by the application and detecting traffic patterns that should not occur during normal operation through the HMI, even more sophisticated attacks could be detected. The rules must be tailored to the particular vendor application, which demands a deep knowledge of the application behavior, but will also yield better results in detecting suspicious traffic aimed specifically at that SCADA application.

3.1 Assumptions Concerning Attacker Behavior

To outline such SCADA application specific rules, particular attack scenarios must be considered.

First, the attacker is able to access the SCADA system network. Basic attacks should be prevented by the firewall and common IDS rules. We assume that it is possible for the attacker to eavesdrop and reverse engineer the SCADA application protocol, or is able to gain equivalent knowledge by some other means. After gaining knowledge of the protocol, one of the objectives of an attacker could be to retrieve information of the SCADA equipment connected to the SCADA system station. Then we assume that the attacker attempts to take control of the SCADA equipment in some way.

With the above assumptions, the following attack scenarios were considered:

1. Use of non-existent system equipment ID
2. Multiple and successive control select commands
3. Consecutive control commands during a short period of time

3.2 Attack Scenarios and Corresponding IDS Settings

In the following, each scenario is explained with the possible logic behind the attack patterns, the communication pattern of the attack and the difference from legitimate communications, and the corresponding IDS settings. The actual IDS rules for detecting the above attacks were assessed using Snort, an open-source network intrusion detection system [6]. It should be noted that processing the SCADA application detection rules for each packet demands computation power.

To minimize the computation needed on the IDS, in this assessment, the more basic detection rules such as use of non-legitimate IP addresses were turned off, relying on the encryption equipment and firewall to filter such basic attacks. The IDS rules that did not apply to this SCADA system were also disabled. This method is not limited to this model system, and can be applied to an actual IDS in a SCADA system to reduce the computation power needed for the IDS sensor.

Scenario 1: Use of non-existent system equipment ID

In order to control the SCADA equipment in this application, the equipment has to be selected with an equipment select packet, the selection acknowledged, and then the control operation becomes possible.

If the attacker has enough knowledge of the protocol to emulate the equipment select packet and the bytes corresponding to the equipment ID, the attacker could change the equipment ID and examine the responses from the SCADA server. If the equipment selection is acknowledged, the equipment corresponding to the ID exists, if an error comes back, it indicates that the equipment for that ID does not exist.

On a legitimate HMI, the equipment is selected in a graphical user interface, restricting the select action to equipments graphically displayed on the HMI, so it is not possible to create an equipment select packet for non-existent equipment. This means that a select packet with a non-existent equipment ID indicates suspicious communication. The flow of the communication is shown in Figure 2. As shown in the figure, the substation server receiving an equipment select packet with a non-existent equipment ID answers with an error packet. It is possible to detect suspicious packets with the error packet. However, an error packet may be invoked for other reasons, such as some problem in the network, so we did not use the error packet for the detection.

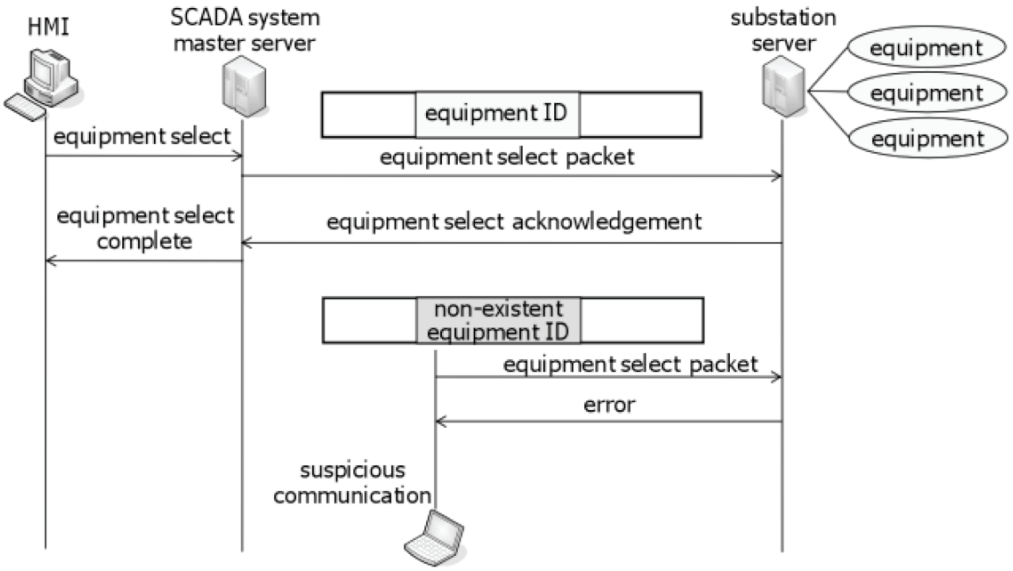

Figure 2 - Select Packet with Non-existent Equipment ID

In the model system, the IDS signature to detect the select packet with a non-existent equipment ID could be written with a single Snort rule. The rule specified the following:

1. Endpoints of the communication (IP addresses and port numbers)
2. The protocol (TCP)
3. Position within the packet that indicates the packet as an equipment select packet
4. Position within the packet indicating the equipment ID
5. The expected equipment ID's

If an unexpected equipment ID is found, the rule is triggered as a possible attack.

If the SCADA system becomes more complicated, the scope of the expected equipment ID's would be larger. It may not be possible to define a complicated series of equipment ID's in a single Snort rule, in which case multiple rules will become necessary.

Scenario 2: Multiple and successive control select commands

In Scenario 1, the attacker attempts to retrieve information from the SCADA equipment connected to the SCADA system substation server using select packets with different equipment IDs. In order to gain knowledge of all the SCADA equipment connected to the server, the attacker would have to send multiple select commands.

On a legitimate HMI in the model application, it is not possible to send select packets successively, unless the previously selected equipment is explicitly deselected, or the equipment control is executed, or the selection is timed out so the equipment ceases to be in a selected state. This means that multiple select commands indicates suspicious communication. An example of a suspicious communication flow is shown in Figure 3.

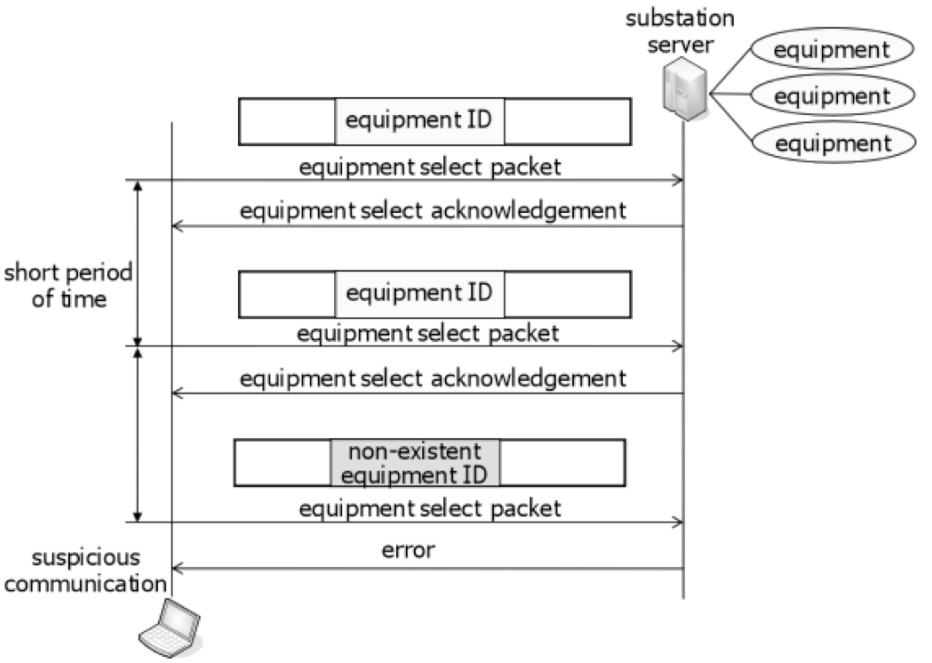

Figure 3 - Multiple and Successive Control Select Commands

The IDS rule for this scenario specified the following in a single Snort rule:

1. Endpoints of the communication (IP addresses and port numbers)
2. The protocol (TCP)
3. Position within the packet that indicates an equipment select packet
4. Tracking multiple packets according to destination
5. Packet count (two) and time span that triggers the alert

If two select packets are observed within the specified time span, the rule is triggered as a possible attack. This time span has to be configured so it is shorter than the time out of the SCADA application.

Scenario 3: Consecutive control commands during a short period of time

After gaining knowledge of the equipment IDs, the attacker attempts to control the SCADA equipment. Consecutive control of one device could lead to damage. On a legitimate HMI in the model application, it is not possible to successively control the equipment within a short period of time, due to the restrictions of the user interface.

Although a damaging operation would typically be physically prevented by a protection device or safety system in a real SCADA system, such a communication attempt would indicate a possible attack. The communication flow is shown in Figure 4.

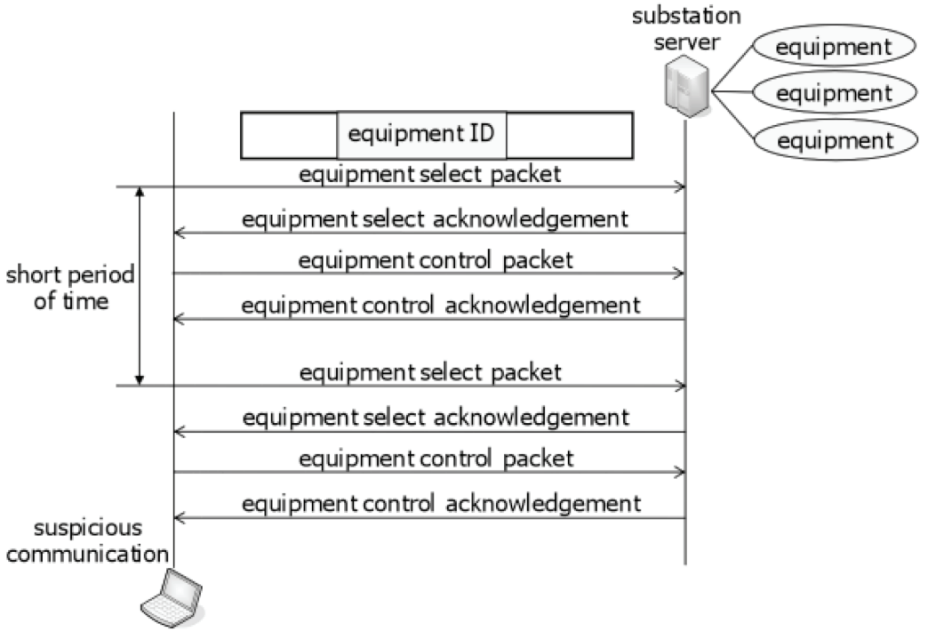

Figure 4 - Consecutive Control Commands within a Short Period

The IDS rule for this scenario specified the following in a single Snort rule:

1. Endpoints of the communication (IP addresses and port numbers).
2. The protocol (TCP).
3. Position within the packet that indicates an equipment control packet.
4. Tracking multiple packets according to destination.
5. Packet count (two) and time span that triggers the alert.

If two control packets are observed within the specified time span, the rule is triggered as a possible attack. This time span must be configured so it is shorter than the time the corresponding operation would take on a legitimate HMI.

Also, if the attacker has enough knowledge to deselect the equipment during the reconnaissance in scenario 2, but executes the selects within a short period of time, it is possible to detect the suspicious communication with this IDS rule.

This IDS rule is triggered using completely legitimate packets and communications, with only the time span between the communications to differentiate between an attack and an actual select and control operation. If an IPS (Intrusion Prevention System) is to be applied to automatically disconnect suspicious communication, extreme care must be taken when setting the time span, so as not to accidentally disconnect legitimate control operations.

4 Latency Due to Adding Encryption and a Firewall

Latency is one of the key issues when deploying security measures to a SCADA system. SCADA systems with applications demanding real-time or deterministic responses generally have a very low tolerance for increased latency. In the model system used in this assessment, the encryption and the firewall are the main sources of added latency.

The latency added due to encryption/ decryption and a firewall for the state information to be accepted at the master server is shown in Figure 5. The latency is slightly different for each packet, and the bars in the figure show the average latency, with the I-beams representing the minimum and maximum latencies. AES (Advanced Encryption Standard) was used for the encryption algorithm, with a 128 bit encryption key. Both the encryption equipment and the firewall are able to communicate at wire speed per specifications, and the latency is less than 1.0 milliseconds. However, as the model SCADA system is very small, further evaluation is necessary to determine the validity of the usage in a real scale SCADA system.

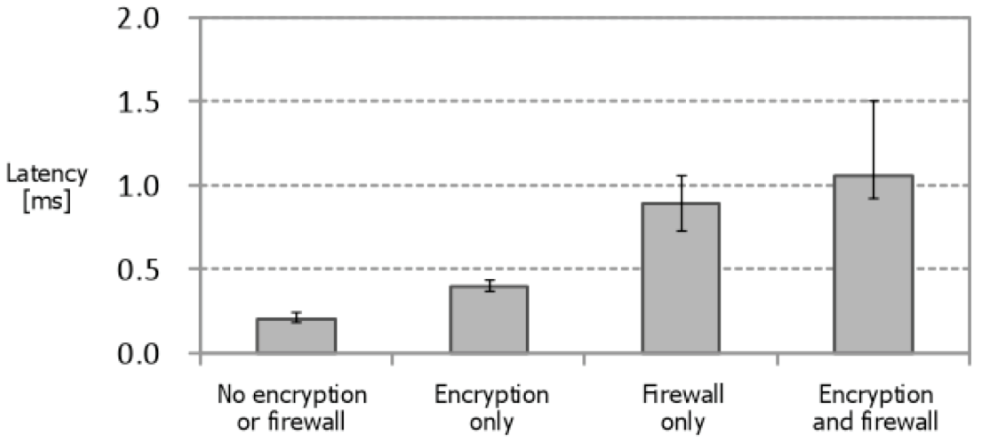

Figure 5 - Latency from Adding Encryption and a Firewall

5 Conclusion and Future Work

This paper discussed IDS rules checking the SCADA protocol used by the application, and detecting traffic patterns that should not occur during normal operation through the HMI of that application. The rules must be tailored to the particular vendor application, which demands a deep knowledge of the application behavior, but will also yield better results in detecting suspicious traffic aimed specifically at that SCADA application. A SCADA system may benefit from such a fine tuned IDS, detecting more sophisticated attacks. However, to determine the rules, an insight of the application and actual management is necessary, and all parameters of the rules must be fine tuned for each application, HMI, and hardware speed, which may take a considerable amount of effort. The rules will have to be updated manually in the event of a system configuration change. Automation may be necessary if this is to be deployed in a changing system, although this may not be pressing in a relatively static SCADA system.

Also, the application level protocol did not use values with variable lengths in this model SCADA system. This made it easier to define the IDS rules. Further work would be necessary to write rules to accommodate more complicated application protocols. Other more sophisticated attack scenarios should also be explored.

The IDS rules depend upon the predictable nature of the SCADA application and protocol. In an emergency such as natural disaster, the equipment in a SCADA system goes through a rapid state change, resulting in an enormous amount of communication and a different communication pattern. It may be necessary to consider the IDS configuration with different rule sets, such as normal mode and emergency mode, to allow for such changes in behavior.

About the Authors – Mai Kiuchi is a research scientist at the Central Research Institute of Electric Power Industry (CRIEPI). She has worked on middleware for SCADA systems, cyber security risk assessments and the overall cyber security of electric utility SCADA systems. She holds the CISSP.

Eiji Ohba is a senior research scientist at the Central Research Institute of Electric Power Industry (CRIEPI). He has worked on reliability analysis of electric utility communication network and cyber security risk assessments. He holds BA and MA on Electric Engineering.

Dr. Yoshizumi Serizawa is the sector leader of the communication systems sector at the Central Research Institute of Electric Power Industry (CRIEPI). He has more than 25 years of research experience on radio/fiber optic communication, time synchronization, power system control and protection, as well as SCADA security. He holds several industry certificates including P.E.E.E. and is a Senior Member of IEEE and IEEJ.

References

[1] NIST (National Institute of Standards and Technology) SP (Special Publication) 800-82, "Guide to Industrial Control Systems (ICS) Security", Final Public Draft, Sept 2008.

[2] "Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks", CPNI (Centre for the Protection of National Infrastructure), Feb 2005.

[3] NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Feb 2007.

[4] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using Model-based Intrusion Detection for SCADA Networks", Proc. of the SCADA Security Scientific Symposium 2007, Jan 2007.

[5] B. Moran and R. Belisle, "Modeling Flow Information and Other Control System Behavior to Detect Anomalies", Proc. of the SCADA Security Scientific Symposium 2008, Jan 2008.

[6] "Snort - the de facto standard for intrusion detection/ prevention", http://www.snort.org