Security defense model of Modbus TCP communication based on Zone/Border rules

W.L. Shang  
Shenyang Institute of Automation, Chinese Academy of Science, Shenyang, Liaoning, China

L. Li  
Shenyang Ligong University, Shenyang, Liaoning, China

M. Wan & P. Zeng  
Shenyang Institute of Automation, Chinese Academy of Science, Shenyang, Liaoning, China

ABSTRACT: To detect the intrusion of advanced industrial virus of industrial control system, design flaws of Modbus TCP Protocol is firstly analyzed in this paper, and a method is proposed, through which the Modbus TCP packet is deeply inspected to deal with the threat from application layer. Furthermore, a general description form of the security rules is proposed, and defense model for Modbus TCP communication in industrial control system or SCADA system is designed, which is based on intrusion detection rules and “white-list” rules. With definition of the minimum set of normal communication between different zones, the system has eliminated exposure greatly. At last, simulation experiments validate that the proposed method is effective and practical.

1 INTRODUCTION

Industrial Control Systems or SCADA systems are widely used in electric power, water plants, petrochemical, and transportation, aerospace and other fields, which are important parts of the national critical infrastructure and related to the national security strategy. In the early design of industrial control systems, proprietary communication protocols, operating systems and hardware were commonly used, and industrial control systems were isolated from other networks. Therefore, industry control systems are believed to be more secure, and function and physical safety get more attention; information security and network security are less considered.

With the continuous integration of industrialization and informatization, TCP/IP technology, open industrial communication protocols, common hardware, software, and network infrastructure are widely used in the industry communication systems. Industry control system exchanges data with enterprise management information system, or even with the Internet. Thus the closure of the industrial control system is gradually being broken. Industrial control system has many information security and network security flaws that are more vulnerable to hackers, viruses, and penetration attack from hostile forces (Wei, et al. 2013).

Snort2.9 version began to join the Modbus TCP, DNP3 and CIP protocols pre-processor (Xia 2013), which can analyze part of the field of communication protocol and data packet integrity, it can also be combined with the set of intrusion detection rules which is released by the third party agencies, for example, Digital Bond to identify industrial control systems / SCADA system intrusions.

NivColdenberg, Avishai Wool et al. proposed a Modbus TCP communication precise modeling method (Thomas 2013) based on finite state automata. The modeling process according to obtained data packets which grabbed between HMI and PLC data channel, constructed the model based on finite state automata. This method results in a good performance in an actual environment, and it has a low false positive rate. However, the method needs to build on the communication between the HMI and PLC with cyclical characteristics. It needs to be further verified whether it can face the complex industry control system application on the SCADA application.

Dale Peterson et al. have designed a passive method of the security event for DCS system and SCADA system (Goldenberg 2013); this method made up for the lack of records of security incidents and made possible the behavior of audit and fault tracing.

Hadeli, RagnarSchierholz et al. proposed that we can identify abnormal behaviors reliably by the behavior of industrial systems and system description file; they also designed and implemented a framework of generating configuration rules automatically for firewalls and other security facilities configuration rules (Peterson 2013).
Wojciech Tyłman proposed a non-IP protocol processing method based on Snort data acquisition module (DAQ). This method is used for the Modbus RTU communication (Schierholz 2009) and it makes Snort to drill fieldbus layer for intrusion detection. What is more, it does not need to add additional program and hardware or modify the Snort code itself.

Current intrusion detection research work can be divided into two categories (Thomas 2013): Misuse detection and Anomaly detection. Misuse detection is based on the method of matching malicious network traffic with known attack signatures. For the reason that the attack signature database of industry control system could not cover all the cases, Misuse detection is easy to generate false negatives.

Anomaly detection is based on the method of identifying abnormal traffic flow of the industrial control system. The fixed communication traffic mode is established by the state model of the system. In comparison with Misuse detection, Anomaly detection is able to detect unknown attacks, and even the disoperation of operators. But Anomaly detection is easy to generate false alarms because it cannot locate error clearly.

The paper is organized as follows: Firstly, security of Modbus TCP is analyzed, and deep packet inspection (DPI) for Modbus TCP is designed. Secondly, we propose a security defense model of industry communication protocol based on Zone/Border rules. At last, simulation experiments are done, which validates that the proposed method is effective and practical.

2 ANALYSIS OF MODBUS TCP SECURITY

2.1 Modbus and Modbus TCP

Modbus is an application layer messaging protocol, located at level 7 of the OSI model and it has become a standard. Its implementations mainly include the achievement based on the serial link (Modbus RTU/Modbus ASCII), high-speed Token Ring (Modbus Plus), and TCP/IP Technology of Ethernet (Modbus TCP/IP, Modbus TCP for short). As shown in Figure 1, Modbus communication can be connected seamlessly to the same communications system. The role of network gateway is to guarantee conversion of different underlying Modbus communication.

This paper mainly focuses on the communication security which is based on TCP/IP technology of Modbus communication in Ethernet, its request and response packets are encapsulated into the format shown in Figure 2.

MBAP HEADER is the Modbus application protocol header; its purpose is to identify Modbus Application Data Unit. This part mainly includes four parts. They are Transaction Identifier, Protocol Identifier, Length, and Unit Identifier. Function code is a flag of that Modbus client (MASTER) and indicates server (SLAVE) as to what to do, and it can reflect operating intentions of client to server. The DATA is set by the client according to the difference of function and the specific applications and the server responds correspondingly.

![Figure 1. The topology of Modbus TCP.](image)

![Figure 2. Modbus TCP packet format.](image)

2.2 Identification/encryption/authorization deficiency

Industrial control protocol, which is widely used today, almost runs in relatively isolated networks environment in the design stage, and there is no data switching with other networks. Therefore, information security and network security factors do not need to focus on consideration, but function safety and physical security should be concerned more (Xia 2013). Although information security needs the existence of industrial control communication protocol system, it is a complex systems engineering to add the industrial communication protocol to the security mechanism. We believe that the security risk of industrial control systems communication protocol will not change from itself in a long situation.

Modbus TCP communication layer is based on standard Ethernet TCP/IP technology, therefore, the traditional attacks on the IT network are also suitable for the industrial control system, and they even cause more harm (Rodrigo 2008). However, the more effective, the more destructive way for control system to build the aggressive behavior to the application layer data. This is mainly due to the defects
existing in the design of Modbus protocol application layer, it mainly reflects in identification, authorization, and encryption security mechanism deficiency. Performance of identification deficiency is that only a valid Modbus address and legal function code can establish a Modbus session; Performance of authorization deficiency is that any user can execute arbitrary function without role-based access control mechanism; Performance of encryption deficiency is that address and command are transmitted by plaintext transmission and it is easy to capture and parse.

After obtaining control authority of a system or access authority of a network by a series of penetration attack, an attacker can obtain the information he is interested in by monitoring Modbus TCP traffic in the network, and can construct Modbus TCP packet easily as protocol, what is more, an attacker even can launch an attack on an important controller with the corresponding debugging tool directly. For example, in an industrial control system, the digital quantity may correspond to the coil and holding register of PLC. If a value of a coil of PLC is changed, the switch which should be closed will be likely to open. Obviously it will cause serious consequences in industrial control systems which have extremely stringent and reliable requirements. In another situation, the attacker changes a value in the register, while holding register may correspond to the analog input and output or the important parameter in industry control process, therefore technology cannot reach the standard, or it causes an accident directly.

3 MODBUS TCP DEPTH PARISING METHOD

The above analysis shows that if we want to protect the industrial control system security based on Modbus communication, Modbus packets will need depth parsing in order to detect intrusion and attack. Therefore this section establishes a general model of depth parsing of Modbus message. As shown in Figure 3:

![Figure 3: Modbus TCP depth parsing.](image)

Modbus protocol depth parsing model mainly consists of three parts, they are the network layer and the transport layer parsing, Modbus packet header parsing, and Modbus message parsing. Its process is as follows:

Step1: the network layer and the transport layer parsing: This part mainly extracts the source IP address and destination IP address and the source and destination port number and analyzes the information in this part in order to provide basic information for access control in the network layer and transport layer or intrusion detection. Communication network equipments are marked by the IP address and port numbers.

Step2: Modbus packet header parsing: This part mainly explains Protocol identifier, Protocol identifier, Length, and Unit identifier. Protocol identifier provides basis to determine whether it is the Modbus communication or not. The value of the length field represents the unit identifier and the total length of data, by this we can determine the abnormal packets which are constructed artificially. Unit identifier is the address on the Modbus serial link, its length is one byte. Different Modbus devices are addressed according to this field; these different Modbus devices connect with the same protocol conversion gateway and share the same IP address. Therefore, the field is of great significance.

Step3: Modbus message parsing: This part is core and key of Modbus protocol depth parsing, its main duty is to analyze the Modbus function codes which represent the operation intention and to analyze the corresponding data according to different Modbus function codes.

Modbus defines four kinds of data types: they are input coil, coil, input register, and holding register. They correspond to the corresponding variables respectively, such as digital input and output, analog input and output correspond to specific data types of Modbus protocol, it may operate a single or multiple data objects; hence we need to propose a general Modbus messages analytical mode. As shown in Figure 4:

The process is divided into the following steps:

Step3.1: Parse Modbus Function Code field. If it is not relevant to read and write operation in the four data types of Modbus protocol, the Step2 is executed, otherwise, turn to Step3.

Step3.2: Analyze function codes which may exist and analyze the key fields of corresponding function, then the whole analytical process comes to the end.
4.1 Zone division and border establishment of industrial control system.

Zone generally has implemented or supported the same functions and has certain assets with the same security requirements. Border exists in different zones, it is the channel of data switching in different zones, the reasonable division and setting of zones and borders are of great significance for ensuring the information security of industry communication system. Generally speaking, Zone division (Eric 2011) can be considered from several dimensions: network connection, control function, data storage, remote access, communication protocol, and critical degree. In this paper, we mainly consider the industrial SCADA system based on the Modbus TCP, therefore, the general method of system zone division and border establishment are simplified as the follow process:

Firstly, the system needs to have a risk assessment and performs important asset identification, and establishes the appropriate documentation.

Secondly, according to the level of an important asset in the enterprise business, the whole system is divided into four layers in accordance with the order from top to bottom, they are business management information layer, data acquisition monitoring network layer, the control unit layer, and the field device layer.

Again, different zones are further divided in each layer according to the functions to be achieved or operating authority. For example, data acquisition monitoring layer has the monitoring picture site which only reads data from the underlying PLC and may have a write operation on the site; this site belongs to different sub-zones levels of data acquisition monitoring layer.

Finally, in order to manage and control the zone communication, in different zones where data communication sets a border and makes the traffic between the two zones via the border.

What need to pointed out is that a division of the sub-region within the region is further characterized for the security needs of different assets within the region. Therefore, finer the “granularity”, the more divided the region is and the more nested sub-zones are. In addition, the zone can coincide in logic and physics if we adjust the industrial control system network structure.

4.2 Security strategy design

Border protection among zones may have different security defense technology and equipments, furthermore, the rules description are also different, therefore we first abstract general safety rules model:

\[ \text{Action} \] \[ \text{Source Address} \] \[ \text{Source Port} \] \[ \text{Destination Address} \] \[ \text{Destination Port} \] \[ \text{Specific Protocol Fields} \]
Action includes:

- **Allow**: To determine the corresponding data packets is legitimate and releases without any other actions.
- **Deny**: To determine the corresponding data packets is illegal which discards and triggers an alarm.
- **Alarm**: To determine the corresponding data packets is abnormal but it releases, and triggers an alarm.

What is more, Specific Protocol Fields indicate the field conditions related to communication protocol. For Modbus TCP communications, the detailed format is as follows:

```
[Protocol Identifier] [Unit ID] [Function Code][Data]
```

where: Protocol Identifier refers to the protocol identifier in Modbus packet header; Unit ID refers to unit identifier in Modbus packet header; Function Code refers to Modbus specified function code;

The Data field refers to the relevant Modbus function code. When the Modbus function code read and write corresponding to the four kinds of data or other operations, Data field consisting of the Starting address identified the data type and Number or Sub Function:

```
[Data] = [StartAddress][Num] OR [SubFunction]
```

Security defense technology which is used for border may include firewall, IDS, IPS (Sun 2006), etc.

Firewall mainly has access control function for transport layer and network layer, but it lacks support for application layer in industrial protocol. IDS and IPS use schema matching method and take appropriate action to the data packets which meet features.

Judging from deployment, IDS system gets network traffic by bypass monitoring and will not cause the delay effect on network communication. IPS is in the communication link and the illegal communication packages can be intercepted and discarded. Judging from security policy which is reflected from traditional IT information security rules, the security strategy of IDS and IPS mostly take a list of detection rule. If the packet matches, then alarm or discard. While another IPS security policy defines legitimate packet types, then discards any other traffic. These two types of security strategy are shown in Figure 5:

These two security strategies have great limitations for industrial SCADA system. Firstly, the IDS system allows to have a miscarriage, but it is unable to intercept illegal data packet. While as to the “white-list” IPS strategy, if its configuration rules are improper, legitimate packets may be discarded. This is very dangerous to the industrial control system which requires high reliability.

This paper proposed a Modbus TCP communication protection method in industrial control system or SCADA system combining IDS rule with “white-list”, and zone division and the border setting together. As shown in Figure 6. Steps are as follows:

Step1: Zone division and border setting of SCADA system, zone division according to industrial control system of the enterprise production information layer, the data acquisition monitoring layer, the control unit layer, and the field device layer. If each zone needs further zone division, and records the partition results with sign in order to further set safe strategy conveniently.

Step2: Set part of “white-list” IPS strategy.

Step2.1: Make clear the minimum set of Modbus TCP communication for data switching between different zones and sub-zones and define this communication as the legitimate communication. The legitimate data defines jointly according to codes in the part of Modbus TCP protocol depth parsing and data whose codes are needed.

Step2.2: Legitimate packet is described by safety rule description language. For example, the Modbus client can use the 01 function code to access the Modbus server address. Safety rules of three coils starting from 0x0000 can be expressed as,

```
[Action:Allow] [Source Address:Modbus_client] [SourcePort:any] [Destination Address: Modbus_server] [Destination Port:502] [FunctionCode:01] [StartAddress:0000][Num:03]
```

Step3: For those that cannot be recognized as legitimatization completely, take IDS strategy to trigger an alarm but not to intercept. This part of the communication may include the communication which can be used by attackers and systems themselves. For example, function code 08 and the sub-function code 01 are reset functions; it cannot be identified as aggressive behavior. Therefore, the best choice is to trigger an alarm timely.

Step4: Default rule setting, that is to say, give up all the other Modbus TCP communication packets which are not in the setting of Step2 and 3.

In fact, the model is not only suitable for Modbus TCP communication security, if we add depth parsing mechanism of other communication protocols,
such as MMS, GOOSE, FF-HSE and DNP3, etc, this model can be extended according to the same process to become a normal model.

5 SET THE EXPERIMENTAL ENVIRONMENT

5.1 Simulation experiment environment and experiment design

In order to validate Modbus system defense method that this paper supposes, we set up industrial SCADA system simulation environment based on Modbus TCP communication. The topology and structure are shown in Figure 7:

The simulation environment is divided into three layers, the data acquisition monitoring layer, the control unit layer, and virtual field device layer. Data acquisition monitoring layer includes two Modbus clients, they are the monitor screen based on KingSCADA software development and debugging and testing software diagslave of a simulated attack; the control unit layer selects Schneider M340PLC, its CPU model is 2020; virtual field device layer can be implemented in control logic of PLC M340.

Virtual field device layer includes switching values which identify the switch opening and closing, opening analog of three electromagnetic flow valves and the upper and lower limitation of the liquid level and the current level. The logic of PLC limits the current level between the upper level and the lower level. In the real industrial control systems, if the current level is not between the upper and lower limits, it may result in a container explosion or severely affect process quality. Therefore, the attack method design is to modify the holding registers which keep the upper level by diagslave software. After the actual liquid level in the container exceeds the real limits, PLC control logic will not change the state of the input and output valves to control the liquid level.

5.2 Experiment design and results

The best way to resist the attacks mentioned above is to work normally according to the control logic based on the experimental simulation environment, clear the minimum communication setting required by Modbus client and Modbus server, and well-design border protection strategy. Here the border protection strategy selects the Snort. Security defense strategy is described based on Snort grammatical rules. In order to describe briefly, we still take the same safety rules description manner.

By analyzing the scene, we can realize that the data acquisition software simulated by diagslave only has the rights of reading switching value and analog quantity. While KingSCADA has the rights of reading and writing switching values and analog quantity. The level of the upper and lower limits cannot change frequently, so even if the write operation from KingSCADA should also be identified as abnormal operation and triggers an alarm.
In order to simplify the rules, we assume that there is only has the data subject representing the upper limits and its address is 0x0000. The security rules of the system design process are as followed:

Step1: The system is divided into data acquisition monitoring layer and control unit layer, they respond to Modbus client and server. And the data acquisition monitoring layer is divided into two sub-zones according to which the upper limits can be written.

```python
var Modbus_client [192.168.1.1, 192.168.1.2]
var Modbus_client_1 192.168.1.1
var Modbus_client_2 192.168.1.2
var Modbus_server 192.168.10
```

Step2: Set “white list” rules, allowing KingSCADA and diagslave to “read” for the holding register whose address is 0x0000 in PLC.

```plaintext
[Action: Allow]
[SourceAddress: Modbus_client]
[SourcPort: any]
[DestinationAddress: Modbus_server]
[DestinationPort: 502]
[FunctionCode: 03]
[StartAddress: 0000]
[Num: 01]
```

Step3: Set abnormal behavior intrusion detection rules. If KingSCADA has a “write” operation on the PLC, then alarm.

```plaintext
[Action: Alert]
[SourceAddress: Modbus_client_1]
[SourcPort: any]
[DestinationAddress: Modbus_server]
[DestinationPort: 502]
[FunctionCode: 06]
[StartAddress: 0000][Num: 03]
```

Set the default rules and intercept all communication which does not appear in the “White-list”.

```plaintext
[Action: Deny] [SourceAddress: any] [SourcePort: any] [DestinationAddress: Modbus_server] [Destination Port: any]
```

The experimental results show that diagslave and the simulation of the attack source and KingSCADA only read 0x0000 holding register in PLC. At the same time, if the King SCADA modifies the level limits, it will trigger the Snort alarm. This industrial control systems security policy among zones which combines intrusion detection rules with “white list” can greatly eliminate the risk of exposure and guarantee the safe operation of the system.

6 CONCLUSIONS

To solve the problem that it is difficult to detect the intrusion into industrial control system by advanced industrial virus, and design flaws in industrial communication protocols, in this paper we have proposed a method through which industrial communication protocols were deeply parsed. A normal method that describes the security rule is also proposed. Furthermore, this paper designed Modbus TCP zone and border security model based on what combines the intrusion detection rules with “White-list”. The core idea of this model is clearly identifying legitimate Modbus TCP communications among zones, and prohibiting all other unnecessary data switching between zones. However, those legal but suspicious traffics will trigger an alarm. The features of the protection strategy are simple, clear and easy spreading. It is very suitable for industrial control systems where communication flow patterns are relatively fixed in network. Validation tests also showed the effectiveness of this method.

However, the Modbus TCP security rule description model is unable to effectively describe the communication behaviors existing in several packets at the same time. Modbus TCP communication protection strategy depended on understanding and grasping of designers to protocols and industrial processes and the understanding deviation will cause the safety rules setting error. In addition, online defensive measures may cause effect on real-time and reliability of industrial control system communication. In the future, we can further study to solve the attack implied in multiple Modbus packets, and real time and reliability of the safety protection strategies on communication system.

REFERENCES


