IMPLEMENTING MODBUS PROTOCOL STACK WITH DETERMINASTIC INTRUSION DETECTION RULES

Sneha Kunte¹, J. A. Shaikh ²
¹Department of Electronics Engineering
²Department of Electronics Engineering PVPIT Budhgaon, Shivaji University sangli, Maharashtra, India

ABSTRACT:
The Technology seems to concern about connectivity these days. Using that connectivity, the data switching work can be done in more flexible ways with protocols like modbus. To use it in industry sectors and to have the complete robustness and reliability of modbus protocol, software protocol stack is necessary. The MODBUS protocol was not initially designed with keeping the security aspects in mind hence it lacks the mechanism to avoid the classical information security threats. For better commercial usage of the modbus, it should work efficiently in any adverse and challenging situations. This paper discussed simple, secure and practical means of communication which can be extended to the industrial automation field with the help of modbus stack implemented with Deterministic Intrusion Detection Rules [1].

Keywords: Protocol stack, Deterministic intrusion detection rules, Modbus protocol.

[1] INTRODUCTION

In this era, Industrial control systems are a fundamental part of critical infrastructure, helping to simplify operations in vital sectors such as electricity, oil and gas, water, transportation, and chemical. A growing issue with security and its impact on industrial control systems have highlighted some significant risks to critical infrastructures. To address security issues for industrial control systems, a clear understanding of the security challenges and specific defensive countermeasures is required. Today, Industrial control system products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial software. All this has led to cost reductions, ease of use and enabled the remote control and monitoring from various locations. However an important drawback derived from the connection to intranets and open communication networks, is the increased vulnerability to computer network-based attacks. Industrial control systems constitute a strategic asset against the rising potential for catastrophic terrorist attacks affecting critical infrastructures. Concerns in regard to security and control systems are related to both the legacy nature of some of the systems as well as the growing trend to connect industrial control systems to other networks. These concerns have led to a number of identified vulnerabilities and have introduced new categories of threats that have not been seen before in the industrial control systems domain. Many of the legacy systems may not
have appropriate security capabilities that can defend against modern day threats, and the requirements for availability can preclude using contemporary security solutions. An industrial control system’s connectivity to a corporate, vendor, or peer network can exacerbate this problem. A general approach, one that uses specific countermeasures to create an aggregated security posture, can help defend against security threats and vulnerabilities that affect an industrial control system. This approach can be applied to industrial control systems and can provide for a flexible and useable framework for improving security defenses. Based upon a review of the modbus protocol for industry uses, this paper introduces a new approach of implementing MODBUS protocol stack on the basis of intrusion detection system rules [1] which will reduce some of the major security lacks of the protocol. In this paper some of the industrial scenarios and security measures are discussed to encourage the effective use of modbus protocol on the various system platforms.

[2] RELATED WORK

MODBUS TCP/IP comes up as a ‘de facto’ communication standard. For those networks there are commercial products that can analyze traffic, detect intrusions and even take actions. However most of them have their own hardware and Software platforms and are not always as transparent and flexible as could be expected. Additionally their cost can even made them not suitable for all deployments, The Javier Jiménez Diaz proposes a method to approach the problem in a cost effective manner, based on the use of well-known open source tools and a methodology to develop the rules to detect intrusions in his paper [2] As a result the IT resources of an organization (employees, hardware and software) can also take care of the company industrial network security without high additional cost in equipment or training time. Snort is a rule based open source network intrusion detection and intrusion prevention tool [3]. Snort collects and logs network traffic, analyzes network traffic searching for rule violations, and alerts the administrator of suspicious activity. Snort is commonly used to monitor Ethernet and TCP/IP communications traffic. Quickdraw [4] is a Snort preprocessor and a set of snort rules developed for industrial control systems using the MODBUS/TCP, DNP3, and Ether/IP communication standards. The quick draw rules include alerts for invalid device configuration attacks, coil and register read and write attacks, high traffic volume attacks, malformed MODBUS application data unit (ADU) content attacks, unresponsive device scenarios, and port and function code scanning attacks. Currently, the Quickdraw preprocessor and Snort rules are limited to protecting TCP/IP systems. The article ‘Deterministic Intrusion Detection Rules for MODBUS Protocols’ by Thomas H. Morris[1] describes a mechanism to enable use of the Quickdraw Snort rules and other Snort rules to protect a serial based industrial control system. The Quickdraw MODBUS/TCP rules were used to validate the work described in respective article. Many researchers have developed statistics based intrusion detection systems targeted for industrial control systems. Statistical intrusion detection systems use statistical methods to classify network traffic as normal or abnormal. Various model types or classifiers can be used to build the statistical model, including neural networks, linear methods, and regression models. There are two types of inaccuracies in intrusion detection systems: false positives and false negatives. False positives generate a false alarm when there is no intrusion, while false negatives miss an actual intrusion. False positives may lead to dropping a valid communication
packet which can have catastrophic results on an industrial control system. Snort uses pattern matching to deterministically detect rule violations. Correctly formed rules will not generate false positives. Because Snort is deterministic, validated rules may be used with Snort in intrusion prevention mode; a mode which drops illegal network packets. SCADA (Supervisory Control and Data Acquisition) network using Modbus protocol is designed to be inherently insecure and vulnerable to attacks. The paper “SCADA Network Insecurity: Securing Critical Infrastructures through SCADA Security Exploitation” [5] addresses the common security mechanisms in the modbus protocol such as authentication, confidentiality and integrity. Also the paper The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems’ by Matthew Franz and Darrin Miller [6] describes the application of the attack tree methodology to SCADA communication systems based on the common MODBUS protocol stack. The authors identify eleven possible attacker goals and identify security vulnerabilities inherent in both the specification and in typical deployments of SCADA systems. These are then used to suggest possible best practices for SCADA operators and improvement to the MODBUS standard.

[3] MODBUS PROTOCOL ANALYSIS

MODBUS is the most popular industrial protocol being used today, for good reasons. It is simple, inexpensive, universal and easy to use. The main reasons for the use of Modbus in the industrial environment are, it is developed with industrial applications in mind, openly published and royalty-free, easy to deploy and maintain, moves raw bits or words without placing many restrictions on vendors. Even though MODBUS has been around since the past century early 30 years almost all major industrial instrumentation and automation equipment vendors continue to support it in new products. Although new analyzers, flow meters and PLCs may have a wireless, Ethernet or field bus interface, MODBUS is still the protocol that most vendors choose to implement in new and old devices. Another advantage of MODBUS is that it can run over virtually all communication media, including twisted pair wires, wireless, fiber optics, Ethernet, telephone modems, cell phones and microwave. This means that a MODBUS connection can be established in a new or existing plant fairly easily. In fact, one growing application for MODBUS is providing digital communications in older plants, using existing twisted pair wiring. OSI reference model is a seven-layer’s structure, which can support a strong network communication. When achieving communication between the workshop level in the industrial field, the designer should consider the following factors: First, to constitute a real open interconnection system, how to create and choose the proper network Communications reference model, whether Open Systems Interconnection model meets the conditions of the special status of industry or not, and simplifying it still meets the control network or not. According to different application areas, communication protocols were carried out to integrate and simplify, therefore, data can communicate only requires simple interface. According to the international OSI 7 layer network model, the standard Modbus protocol defines the communication physical layer, link layer and application layer. Physical Layer is the asynchronous serial communication standard of RS232 and RS485; Link Layer provides the number identification based station, master / slave mode of medium access control, Application Layer provides the information specification (or message format) and communication services; There are two communicate modes about Modbus protocol ASCII mode and RTU (Remote
Terminal Unit) mode. ASCII mode is a byte of two ASCII characters to send, while RTU mode is in hexadecimal form of data, a byte is one frame, so efficiency of data transmission is more than ASCII mode, the majority of industrial controllers are using RTU mode. In the same network, regardless of the master or slave, must use the same communication patterns and the same transmission rate. At present, commonly transmission rate of Modbus protocol is 1200 bit/s ~19200 bit/s. During communications on a Modbus network, the protocol determines how each controller will know its device address, recognize a message addressed to it, determine the kind of action to be taken, and extract any data or other information contained in the message. Controllers communicate using a master/slave technique where only one device, the master, can initiate transactions or queries. The other devices, slaves, respond by supplying the requested data to the master or by taking the action requested in the query. Typical master devices include host processors and programming panels. Typical slaves include programmable controllers.

![Modbus Protocol Stack](image)

**Figure: 1. Modbus Protocol Stack**

**[4] SECURITY ASPECTS OF PROTOCOL**

Protocol standards specially designed for control systems frequently have specific application to deal with, so mostly there is very little regard for security taken in consideration. Many times implementers think about the security only when trouble arises while deployment of the protocol or they consider close and secure environment, this will increase the risk of failures in real environments. Sometimes security is a major part of consideration but the security postures defined are not clear enough to evaluate the risks in the real challenging environments. Also most of the present protocols were designed when the traditional system was a closed serial network that contained only trusted devices with little or no connection to the outside world, at the long time before network security supposed to be a problem. Evolution of the control system brought the TCP/IP and Ethernet in to picture and it became common approach to replace the traditional networks with the new TCP/IP networks causing the different results than traditional systems. There was not any closed trusted model for the systems which introduced the different types of vulnerabilities and a risk that was not appeared before. The increasing use of TCP/IP in business networks led the insecurity and uncertainty of the systems, by putting industrial production, environment integrity and human safety at risk.
Vulnerabilities in the communications protocols and their implementations were major cause for various sever attacks on the business systems. The lack in security aspects of protocol designing eventually made the control system very weak against the damaging attacks.

One of the primary weaknesses exploited in attacks against the Internet and business information systems are SCADA networks and its protocols are developed based on reliability, availability, and speed but with no or little attention paid to security. The use of the Modbus protocol in the SCADA networks is much common practice but the Modbus based SCADA systems are very much likely to be insecure and vulnerable to attacks. The lack of common security mechanisms in the protocol such as authentication, confidentiality and integrity has gigantic impact on the SCADA networks. Though Modbus standard is flexible and easy to implement, it has some inherent protocol vulnerabilities that 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 because the protocol was not initially designed with keeping the security aspects in mind hence it lacks the mechanism to avoid the classical information security threats. The protocol does not include a way of ciphering the traffic, check the integrity of messages, and authenticate master and slave devices. The attackers can easily discover these security weaknesses and begin to exploit them. As such, there is a need to discover these security flaws before critical devices containing them are deployed in the field where they are sometimes expensive to fix and maintain. Once we understand our vulnerabilities, we can fix the security flaws and design mitigation strategies to reduce their impact of the possible attacks.

This paper discusses the new approach of implementation which makes the design and evaluation easier and reduces protocol mutation attacks against industrial control system appliances and also secures application program to crash and cease to function and to cause devices to reset themselves. And consequences of the unsecure communication between master and slave will be discussed to expose the insecurities by design.

[5] EXPLOITING THE VULNERABILITIES

Exploitation of the inherent vulnerabilities is mostly related to the message frames of the MODBUS Protocol. The inbuilt lack of security in the message frames specifies the security flaws of Modbus. To expose the vulnerabilities of Modbus here some attack scenario are explained so that security weaknesses can be easily addressed in the Modbus-based automation systems.

i) When the function code 08 and sub function code 0A is sent to the target device, it clears the counters and alters the diagnostic register values. This changes the configuration of the field device and impacts the diagnostic operations. This attack may lead modification of field device.

ii) When the function code remains same i.e. 08 and sub function code changes to 01 the end device restarts and executes its power up test. This message causes the field device to change the configuration settings since they will not be restored to the original but to the default and also rendered inoperable since it is asked to restart repeatedly. This kind of the attack may cause the interruption and modification of field device.
Implementing Modbus Protocol Stack With Deterministic Intrusion Detection Rules

iii] Function code of 17 when sent to the field device it returns the field device status information which can be sniffed and studied to carry out more attacks. This impacts the confidentiality of the system.

iv] Messages can be broadcasted from the intruder to the field devices and the attack can go undetected since there are no reply messages for broadcast requests. This can bring down the whole set of remote stations and can hamper the whole operation. These types of attack may lead the interruption and modification of system.

v] Messages flowing between the master and field devices can be stored and replayed. In this way the intruder will confuse the end devices and spoil the flow of operations. These types of attack may lead the interruption, modification, and fabrication.

vi] The intruder can randomly generate addresses and send messages to the field devices to obtain its configuration and status information. This scanning attack causes loss of confidentiality of information.

vii] Another attack is delaying the flow of information to the master from the slave so that it receives out of data messages and hence discards it. These attacks threaten the system by interrupting and modifying the messages.

viii] The replay attacks are also possible i.e. capture the message frame being sent and reuse them by fabricating it to do some other functions.

Attacks are carried out on the Modbus protocol structure where a function code within the message frame is modified and hence the result of acts corrupts the end system. Impacts of the above attacks are loss of confidentiality occurs when an attack reveals information about field devices or messages. Loss of availability occurs when operators are unable to obtain accurate and timely information about a process either due to denial of service or data modification; attacks interrupt field devices, network connectivity or messages, as well as those that modify the master or involve the fabrication of field devices. The worst category, loss of integrity, occurs when an attacker spoofs the master and/or seizes control of the process; attacks modify field devices, network paths or messages as well as those that result in the fabrication of the master, network paths or messages.

[6] SECURITY MEASURES

In order to fight the above attacks there must be solutions developed which make it more usable and hence provides reliability of data transmitted as well as protected data. To improve and strengthen the overall security of modbus system, it is essential to enhance the security features and use them while implementation of the protocol. It is necessary to analyze existing protocols such as Modbus and understand the vulnerabilities present in the protocols. This will help with the development of security measures that can be added into the protocol specifications. The best way to solve this issue is by repairing the Modbus protocol at its source. But this will require architecture modifications which are significant changes. Another
way to approach this issue is by introducing smaller security mechanisms to protect against attacks. The following listed countermeasures are application specific but can be applied on Modbus based systems depending on its application, to provide security and the common security threats this may help to reduce the vulnerabilities associated with protocol and will improve the overall performance of the Modbus system in real challenging environment.

1] Authentication of Master –
When the master sends a message to the field device, it needs to first authenticate the device from which it obtained the message frame and then process the frame. E.g. Modbus frame can have Master Signature in each frame for safe and sound communication. Modbus protocol lacks this ability and hence attacks can easily take place in Modbus. This attack can bombard the slave units with messages and cause denial of service to the original legal master.

2] Function Code Margins-
MODBUS implementers may wish to limit the set of allowed public function codes to Master. This will restrict the master to perform unwanted actions and further limits the possible criticalities.

3] Sub Function Code Margins-
MODBUS implementers may wish to limit the set of allowed public sub function codes. For example function code 8 is a diagnostic function code which provides such commands as force to listen only mode and clear counters and diagnostic register. Particular master may have the set of allowed public function codes with restricted subsystem codes, permitted by the MODBUS system implementer.

4] User Defined Function Code Margins-
User defined function codes must be in the specific range defined by the System implementers. System implementers will wish to limit the user defined function codes to the set of implemented user defined function codes.

5] Classified Data Access-
Modbus implementers can limit the master from approaching the whole memory locations of the slave. E.g. Master can have access the limited access to data associated with the slave. Hence all the processing data of the slave will not be affected by Master.

6] Check for PDU length -
A protocol mutation attack may alter the size of a data access response to not match the expected size. Checking the response packet PDU length detects this attack.

7] Data Value Margins -
System implementers also put the boundaries for quantity values that master can write for any particular registers address pair. And also put alerts whenever the quantity value is illegal. For example: function code 6 (Write Single holding register) Holding Register [4001] = {0, 1, 2, 4} are Legal values. Values other than above are not legal if master tries to write one of the illegal values it will get alert for it.

S. Kunte and J. A. Shaikh
8] Data Register Margins –
System implementers also put the boundaries on pair of addresses that particular master can access. If master tries to access one of the restricted areas of memory addresses then it will get alerts. For example: Allowed pair of the address = {4001, 4002, 4003, 4004, 4005} Addresses other than above are not legal if master tries to write one of the illegal address of pair it will get alert for it.

In addition to checking for illegal quantities separate rules can be added to check for supported quantities. As with many other rules MODBUS system behavior is predefined and limited. As such a limited set of used quantities will exist for each allowed function code and used address pair.

[7] SECURE MODBUS PROTOCOL

The secure architecture that is covered below is intended to satisfy the security requirements of modbus.

1] A secure Modbus protocol must preserve confidentiality, integrity of the message. In order to satisfy these requirements unauthorized entity must not be allowed to access or modify the contents of the message.

2] There should not be an intruder who can emulate the master or can negate a performed action. This may cause attack, leading the interruption, modification, and fabrication.

3] Integrity of the data is maintained by using a secure hash algorithm. Like CRC is used to generate the digest and transmitted along with the message frame. The integrity is verified by computing the digest with the same algorithm and comparing it.

4] The above scheme does not prevent an intruder to create an own message frame and send it to the field device. To avoid this kind of attack it is important to authenticate the master. Therefore a signature based scheme should be used. E.g. the master signs the digest with the private key and the field end device will use the public key to release the digest and check on authenticity. With this algorithm even availability will be fulfilled since only the owner with the specific private key can send the message frame.

5] The above two schemes don’t provide replay protection. Reason being the message frame can be sniffed and obtained by an intruder. Hence a time stamp scheme is used which will help identify if the packet was sniffed or is the original message frame.

6] This modbus modules should be developed by considering the security rules. These security rules will define the list of authorized behaviors i.e. The right combination of command and destination. System description database contains description of the system to be analyzed. This database works in sync with the rules database to determine any malicious activity on the process network. The event tracker is used to correlate events and is used in stack architecture.
The Modbus analysis engine analysis all the data collected and identifies malicious behavior. Alert manager notifies about the potential malicious activity.

[8] CONCLUSION

Modbus based systems has a number of security issues. The aim of this paper is to build the Modbus protocol stack by considering these security issues and put the light on the countermeasures to improve the behavior of the Modbus based systems. There are a number of vulnerabilities that can be exploited in the modbus master and slave units which can be easily avoided by considering some minor and major points while implementing the Modbus Protocol on any automation system.
REFERENCES