ANNALS OF THE ORADEA UNIVERSITY
Fascicle of Management and Technological Engineering
ISSUE #1, MAY 2015, http://www.imtuoradea.ro/auo.fmte/

VULNERABILITIES OF MODBUS RTU PROTOCOL – A CASE STUDY

Gabor JAKABOCZKI[1], Eva ADAMKO[2]
[1] University of Debrecen, Faculty of Engineering, jakaboczkigabor@gmail.com
[2] University of Debrecen, Faculty of Engineering, adamko.eva@eng.unideb.hu

***Abstract*—**SCADA, CIS, ICS and similar MODBUS based systems were always the target of many types of attacks, but during the last decades because of the fast spread of the internet, these systems become much more vulnerable. This paper is a case study, which aim is to investigate the seriousness of the above described situation.

***Keywords*—** attack, Modbus RTU, SCADA, security

I. Introduction

TALKING about smart homes, smart buildings, intelligent facilities, internet of things the following questions arisen in us.

1) Is SCADA(Supervisory Control and Data Acquisition) or similar systems secure enough?
2) Which part of that systems is the more vulnerable?
3) Is there any solution to protect the communication channel?
4) If there are vulnerabilities in the communication, is it able to cause serious problems?
5) If it can, how serious is the damage?

On the next pages we will try to answer these questions, but the aim of this case study is not to analyze the SCADA or similar systems vulnerabilities part by part in detail, but to investigate one part of it, which part is the communication protocol, and search successful or unsuccessful attacks against it. In this article, we focus on the MODBUS communication protocol because it is a widespread communication standard in the particular field and 22% of the communication protocols used in these types of networks is MODBUS. The paper structure is the next. Section II. gives a brief introduction about the basic concepts. Section III. descripts the MODBUS protocol itself in detail. Section IV presents real attacks against SCADA systems and section V. stands for the conclusion and section VI. is for the future work.

II. Basic concepts

For the better understanding in this section we define some basic concepts.

A. CIS

CIS stands for Critical Infrastructure Systems. Talking about CIS means talking about energy generation, chemical production, manufacturing, water supplying, transportation or any other industrial processes.

B. ICS

ICS stands for Industrial Control System. ICS are command and control networks and systems designed to support industrial processes. According to this definition, ICS is the system which purpose is to realize the processes of the CIS.

C. SCADA

SCADA stands for Supervisory Control and Data Acquisition. SCADA is a special type of ICS. SCADA systems usually includes sensors, PLCs (Programmable Logic Controller), RTUs (Remote Terminal Unit), and HMI (Human-Machine Interface). SCADA systems usually designed to make operation of processes better, improve performance, simplify actuation or reduce error comes from human intervention. SCADA systems are the backbone of most of ICS, it collects, exchanges and analyze the system properties, and other relevant data to help operate the processes more effectively, both in terms of time and materials.

As you can see the above listed systems are essential parts of well-functioning plants, facilities, towns, cities or countries, so a successful attack against it affects not only the actual SCADA systems but also us.

D. MODBUS protocol

The MODBUS protocol was designed by the MODICON in the early seventies. MODBUS is a network protocol, which primary purpose was to build network from PLCs. Through the years it became one of the most common communication protocol. There is three types of the MODBUS protocol according to the messages sending on the channel.

E. MODBUS TCP

There are several research dealing with the weaknesses of this type of the MODBUS, and although it is not typical to use, but several solution exists to protect a SCADA system using MODBUS TCP. One of these solution is to apply firewalls, proxy servers or SSL.

F. MODBUS RTU

The MODBUS RTU is the serial MODBUS protocol, security, although there are several security breaches in it. In Section III. it described in detail.

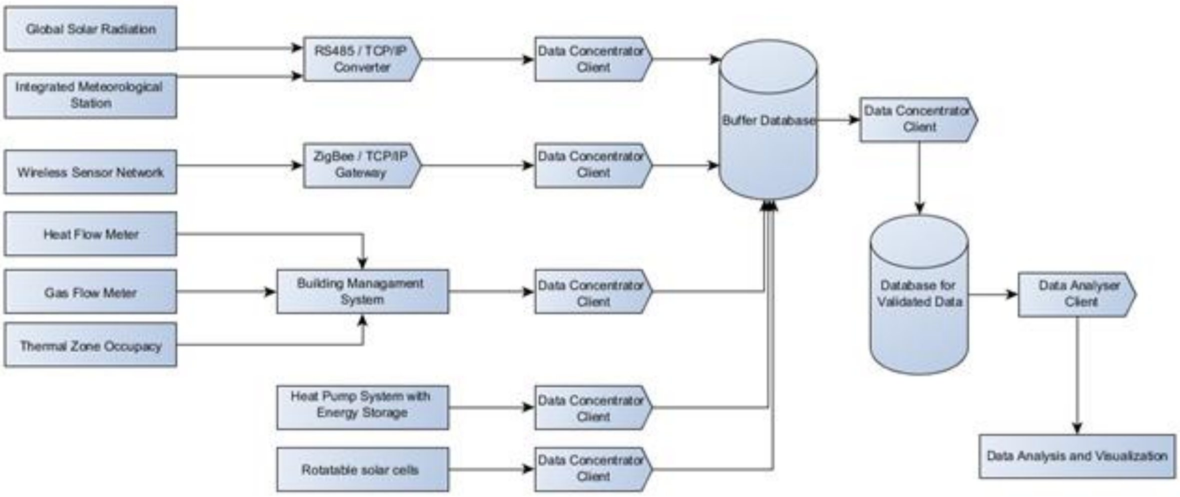


Fig. 1. SCADA system of the Building Mechatronics Research Center in University of Debrecen

G. MODBUD ASCII

Sending ASCII characters through a communication channel is not too widely used solution, so this type of MODBUS is not interesting for us in the respect of secure SCADA systems.

III. THE MODBUS SERIAL PROTOCOL

A. MODBUS serials place in the OSI/ISO model

The MODBUS serial protocol is a Master-Slave protocol, taking place in the Data link layer of the OSI/ISO model. It is a request-reply protocol, typically one node, the Master, requests the transmission of data from the Slave devices. Usually the Slave nodes do not initiate the communication with the Master or with other Slaves.

On the seventh layer of the OSI/ISO model the MODBUS Application layer provides server-client communication.

On the MODBUS serial line the Masters act as clients and the Slaves as servers.

TABLE I
The ISO/OSI Modell And The Modbus Protocol

Layer	ISO/OSI Model	MODBUS
7	Application	MODBUS Application protocol
6	Presentation	
5	Session	
4	Transport	
3	Network	
2	Data Link	MODBUS Serial Line Protocol
1	Physical	ANSI/TIA/EIA-485-A-1998

B. The physical layer

As one of the most widespread serial communication protocols, MODBUS serial usually use the ANSI/TIA/EIA-485-A-1998 standard (also known as RS485) as the physical communication layer. Because the Master-Slave hierarchy of the MODBUS protocol, the RS485 standard used in half-duplex mode, mainly with the two-wire configuration

C. The Master-Slave principle

On the MODBUS serial line several Slaves can be connected, but only one Master at a time. Every Slave must have a unique address, only the Master can communicate successfully without it. As the Master initiates the communication, the Slave acknowledges the request and send back the required data. The Master device can issue these requests in either unicast (one slave) or broadcast (all slave nodes) modes. Upon receiving a broadcast message the Slaves do not send reply.

D. The architecture of the MODBUS serial frame

The Protocol Data Unit (PDU) of the MODBUS protocol is simple and independent from the underlying layers. It is composed of a Function code that determines the action to be taken with the following Data segment. On the serial line the PDU is encapsulated in a frame that contains an address field and an error check part. The address field in the beginning of the frame is an address of a Slave (the target in unicast mode requests, or the origin if it is a reply of a slave) and the error check part is a CRC or LRC byte pair.

There are two coding methods to use, the ASCII where the data (and the entire frame) is sent in characters, or the RTU (Remote Terminal Unit) where the frame is composed of hexadecimal characters. The latter is the default, and its data throughput is greater than the ASCII method (due to character density).

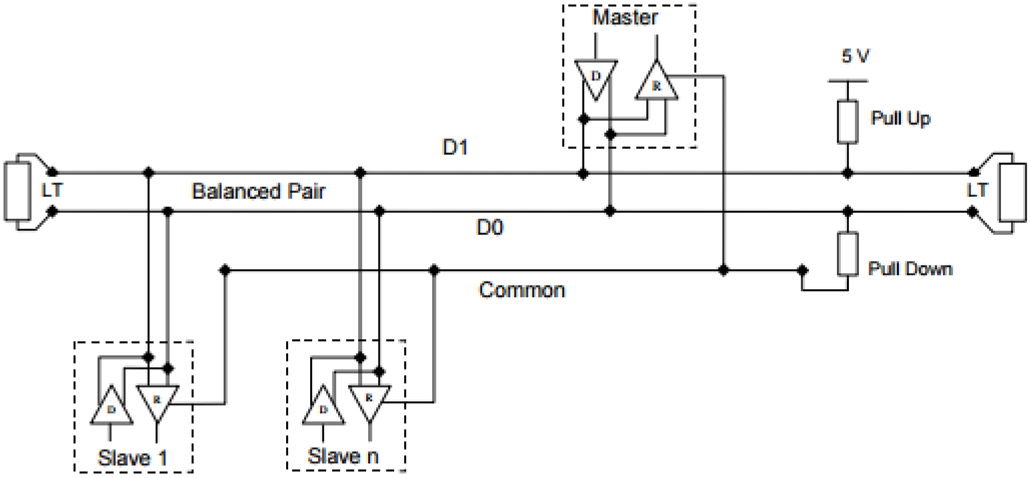
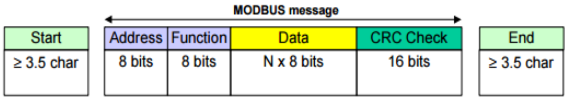


Fig. 2. Typical Master-Slave configuration on RS485 serial network. Note the resistors.



Start	Address	Function	Data	CRC Check	End
≥ 3.5 char	8 bits	8 bits	N x 8 bits	16 bits	≥ 3.5 char

Fig. 3. Architecture of a MODBUS RTU Frame

E. Usage of MODBUS serial

As the second biggest de facto standard in industrial applications (22%, Profibus 28% as of 2010) the MODBUS serial protocol is widespread.

Countless applications are known:

1) End point devices:

a) - Intelligent actuators (motor controllers, pumps, valves etc.)

b) - Sensors (like Radio frequency sensor gateways, thermometers, M-bus integrators etc.)

2) Data acquisition and control devices:

a) PLCs

b) Embedded controllers

3) On site control, monitoring and data presentation devices

a) Industrial computers

b) HMIs and various displays

4) Servers and databanks

F. The weaknesses of MODBUS serial

The most obvious weakness of the MODBUS serial protocol is the lack of built in security measures. There is no means of identifying a device on the bus, if we do not anticipate its presence. There is no built in command to discover connected devices or to verify their authenticity. And foremost the Master nodes do not have to have address, and can communicate over the bus without one.

Another weakness is that the messages transmit over the medium without any encryption, in a simple and clear text format and can be read without decoding.

In an imagined scenario, if an attacker successfully insert a transceiver device between two nodes, it can monitor, disrupt and modify the communication or compromise it entirely.

So, we can declare -without any detailed analysis of the protocol- that several serious security breaches found in the communication through MODBUS.

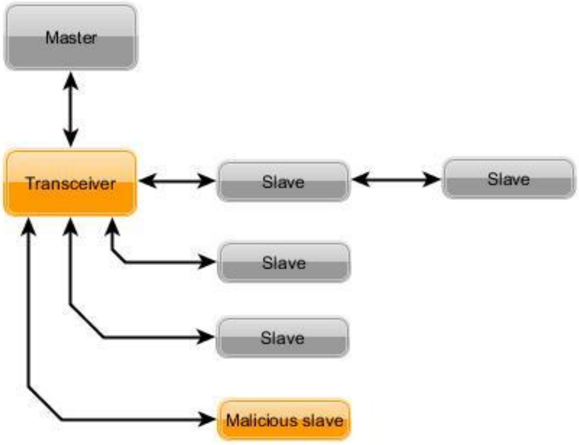


Fig. 4. A compromised MODBUS network topology

IV. SUCCESSFUL ATTACKS

A. Attack against MODBUS/TCP protocol based systems

1) 1982

In 1982 a part of the Trans-Siberian gas pipeline destroyed because of a Trojan virus got into its SCADA system. The explosion was equivalent with a three kilotons of TNT.

2) 2003

In 2003 a US hydroelectric power plant decoy system lost all control because of a hacker group called APT1 [1].

In 2003 seven American states needed the work properly without electricity because of a malware destroyed some CIS. The blackout caused many damage, among other serious things, people died because of it [3].

3) 2013

In 2013 two American cyber security experts took over the control of an oil rig. It could have been cause serious environmental disaster [2].

The above listed events only a tiny part of the known attacks, and most of them happened because these SCADA, CIS and ICS had somehow linked to the internet. Several publications and researches investigate the vulnerabilities of internet linked SCADA systems, or in other words MODBUS TCP based SCADA systems – as it mentioned before -, and of course several solution exists. Nevertheless these solution focus on to protect SCADA systems from attacker who come from the internet.

B. Attack against MODBUS RTU protocol based systems

1) 2010

From 2010 a malware called Stuxnet systematically destroyed a fifth of Iran's nuclear centrifuges by causing them to spin out of control. When the malware installed on a SCADA system it is able to access, read, write, and delete code blocks on the PLCs. It infects USB drives, and then spread like a common flu, that is why the solutions that secure against MODBUS/TCP did not work in this particular case [4].

2) 2011

In 2011 McAfee reported that several of its customers (corporations in the energy sector) got hit by a series of attacks from Chinese origin. The primary goal of the attacks was not to cause damage, but to gather information on the affected companies SCADA network structure (and possible exploitable weaknesses) [5].

3) 2013

In 2013 two ICS expert compromised multiple industrial facilities through radio frequency channel. They took access over temperature sensors, and was able to falsify the real data [7].

The ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) monitoring report of 2013 states that in the first half of that year they discerned more than 200 attacks that targeted ICS systems [6, 8].

In their 2013 presentation at the 30th Chaos Communication Congress, the SCADA Strangelove team reported their findings about the vulnerabilities of several industrial protocols including MODBUS. They exploited "zero day" bugs and took over entire networks within the matter of hours. When a viewer asked after the presentation if the team could take over nuclear plants or similar networks the presenters stated: "It would be better to answer that question backstage, in private."

V. Conclusion

We come to the point to answer the questions of the introduction section. The answer for the first question is clearly no, we can say it because in the previous section lot of successful attacks were presented, and these cases are only the top of the iceberg. Answering to the second question in the absence of a thorough investigation may seem to be guesswork, but it can be said that every system – consisting any types of devices - depends on the underlying communication channel. That is the reason, why we choose the MODBUS protocol as the main topic of the case study. As you can read in the previous sections there are several possible solution to make MODBUS PLC communication more secure, but there are not any solution (or not cryptographically secure solution) for MODBUS RTU. MODBUS communication protocols are backbones of SCADA and CIS systems, which responsible for critical tasks, so ruin such systems can cause not only enormous material damage, but can costs lives.

VI. Future work

After investigating these cases we can say, that a proper solution is needed to make communication over MODBUS RTU secure, and make SCADA systems more reliable, from this point of view too. In the next months we plan to design a secure and cryptographically correct communication protocol on the MODBUS RTU standard and implement on AVR microcontrollers.

References

[1] Simonite, Tom. "*Chinese Hacking Team Caught Taking Over Decoy Water Plant.* (2013) *Online:* http://www. technologyreview. com/news/517786/chinese-hackingteam-caught-taking-over-decoy-water-plant

[2] Smith. "*Not cyber myths: Hacking oil rigs, water plants, industrial infrastructure*" (2013) *Online:* http://www.networkworld.com/article/2225104/microsoft-subnet/not-cyber-myths--hacking-oil-rigs--water-plants--industrial-infrastructure.html

[3] Ackerman, Robert K. "*SCADA Systems Face Diverse Software Attack Threats*" (July 31, 2013) *Online*: http://www.afcea.org/content/?q=scada-systems-face-diverse-software-attack-threats

[4] Albright, David, Paul Brannan, and Christina Walrond. "*Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*". Institute for Science and International Security, 2010.

[5] Keizer, Gregg. "'*Sloppy'Chinese hackers scored data-theft coup with 'Night Dragon'.*" *Computerworld, February* 11 (2011).

[6] Storm, Darlene. " *Brute-force cyberattacks against critical infrastructure, energy industry, intensify*" (July 2, 2013) Online: http://www.computerworld.com/article/2473941/cybercrime-hacking/brute-force-cyberattacks-against-critical-infrastructure--energy-industry--intens.html

[7] Apa, Lucas, and Carlos Mario Penagos Hollman. "*Compromising Industrial Facilities from 40 Miles Away*." *IOActive Technical White Paper* (2013).

[8] *ICS-CERT Year in Review*, Industrial Control Systems Cyber Emergency Response Team, 2013