

# Development of laboratory exercise "Cybersecurity of IIoT protocols"

Aleksandar Hristov<sup>1</sup>

**Abstract** – The aim of the paper is to present one of the laboratory exercises for students in the Technical University of Sofia. This lab explores the possibilities for conducting man-in-the-middle (MITM) attacks in industrial networks when using one of the most widely spread protocols - Modbus and then explores the capabilities for protecting from MITM attacks by changing the communication protocol from Modbus to Secure Modbus.

**Keywords** – Laboratory exercise, Modbus, Secure Modbus, man-in-the-middle attack, cybersecurity, Industrial Internet of Things.

## I. INTRODUCTION

Today, the cybersecurity [4] is very actual research area. The author of this paper is assistant at the Faculty of Computer Systems and Technologies at the Technical University of Sofia and conducts laboratory exercises with bachelor students in various disciplines related to cybersecurity and IoT. One of these disciplines is "Internet of Things". According to the curriculum, there are 5 laboratory exercises, each lasting 4 hours. One of these labs is dedicated to the cybersecurity of Industrial Internet of Things (IIoT) protocols and is titled "Research on specific solutions for network and information security in IoT".

The task in this lab is to investigate the possibilities of attacking the Modbus [2] protocol, to protect it by encapsulating it in the TLS protocol, and to test whether the protected traffic that uses the secure version of the protocol (Secure Modbus) can be compromised. For this purpose, the students have to implement a project of a sample traffic light system [5] using Programmable Logic Controllers (PLC). It should not be forgotten that modern methods are welcome, e. g. [6].

For the software implementation of the project, the Siemens SIMATIC STEP 7 (TIA Portal) v17 software package is used [1,3], which makes it possible to configure, program, test and diagnose the PLC controllers, Human Machine Interface (HMI) panels, and other devices.

The labs are conducted in a laboratory of the Department "Information Technologies in Industry" and the hardware used are Siemens controllers. They are chosen for performing the lab because after a study of different PLC controllers has been conducted, the results showed that Siemens PLCs are the only ones that have implemented the Secure Modbus protocol.

<sup>1</sup>Aleksandar Hristov is with Technical University of Sofia, Faculty of Computer Systems and Technologies, 8 Kliment Ohridski Blvd, Sofia, Bulgaria, 1000, E-mail: ahristov@tu-sofia.bg

The TIA Portal v17 software is used for creating the configuration and the logic of the controller, setting the network topology of all the devices, and designing the Graphical User Interface (GUI) of the HMI panel. The function for creating and signing certificates is used for the implementation of Secure Modbus communication.

The aim of the paper is to explore the capabilities of one of the oldest and most widely used protocols - Modbus for protecting industrial networks from man-in-the-middle (MITM) attacks [6], due to the fact that Modbus is implemented in almost every PLC controller. The proposed laboratory exercise investigates the security of a smart traffic light system (part of a smart city) based on Siemens industrial controllers and the use of Modbus and Secure Modbus protocols for the connection between the controllers.

## II. USING SIEMENS PLC FOR TRAFFIC LIGHT CONTROL SYSTEM

The algorithm of the traffic lights, which are located in the corners C1—C4 at the intersection of two equivalent highways A—A and B—B is shown in Fig. 1.

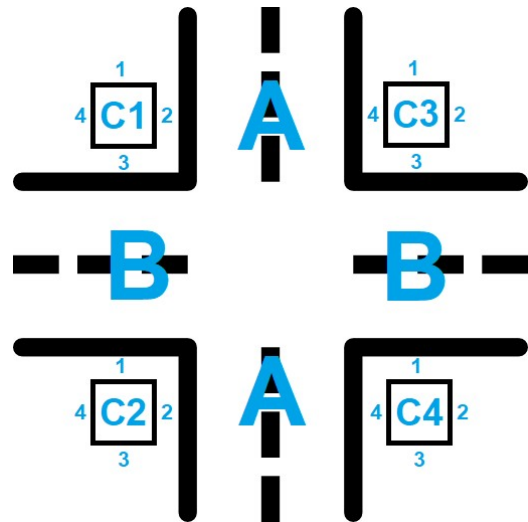


Fig. 1. Intersection of two equivalent highways

At the beginning the traffic light system is in state 0, in which the red lights on sides 1 and 3 ("Red 1"), and the green lights on sides 2 and 4 ("Green 2") are on for a predefined interval of time. Then the green and red lights will go out simultaneously and the yellow lights will light up on all sides for 1 second. After that, the yellow lights will go out and the green lights on sides 1 and 3 ("Green 1") and the red lights on sides 2 and 4 ("Red 2") will be on for a predefined interval of time. At the end of the loop, the green and red lights will go

out and the yellow lights will light up again, after which the traffic light system goes to state 0, in order to start the loop again. Usually, the yellow light is turned on for 3 to 5 seconds, depending on speed limit and other factors, but for the laboratory exercise the value is chosen to be 1 second. The red and green lights are switched on for certain time intervals, which depend on the traffic intensity and traffic situation at the intersection. The time duration of "Red 1" and "Green 2" is interval A. Accordingly, the time duration of "Green 1" and "Red 2" is interval B. Their durations can be independently set in increments of 1 second ranging from 1 to 99 sec.

The proposed traffic light control system consists of three functional units - timer controller (PLC client), traffic light controller (PLC server), and HMI that is used for manual controlling by the buttons in the GUI.

The algorithm of the timer controller is responsible for switching the traffic light between daytime and night mode at specified times of the day as it is shown in Fig. 2. This is accomplished by creating a watch that sends requests to the PLC server through Modbus or Secure Modbus protocol each day at specified moments -  $t_1$  and  $t_2$  for changing its tag "operating mode". Then, the PLC server switches operation mode of the traffic light system: from moment  $t_1$  to moment  $t_2$ , the traffic light operates in daytime mode and from  $t_2$  to 0 (24) and from 0 to  $t_1$  the traffic light operates in night mode. The times  $t_1$  and  $t_2$  are configurable.

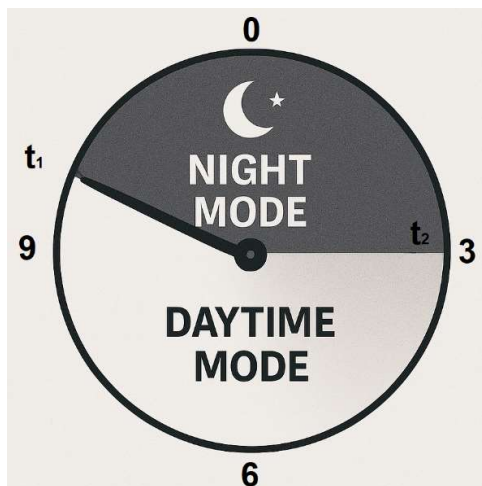


Fig. 2. Daytime and night mode of the traffic light system

When the timer (PLC client) changes the value in the memory of the PLC server (from '0' to '1'), it switches the traffic lights from daytime mode to night mode, and vice versa.

The traffic light controller (PLC server) implements the algorithm of its operation during the daytime. The algorithm is implemented through Ladder Logic (LAD). Part of the ladder diagram that contains changing the state of the traffic light from yellowAfterRed to GreenLight and from green light to yellowAfterGreen light is shown on Fig. 3. The traffic light system has also night mode with yellow flashing lights in all directions when the other lights are off. Communication between client and server (the two PLCs) is accomplished via the Modbus protocol. As it was mentioned above, the Siemens

controllers used for the system implementation support both Modbus and Secure Modbus versions of the protocol.

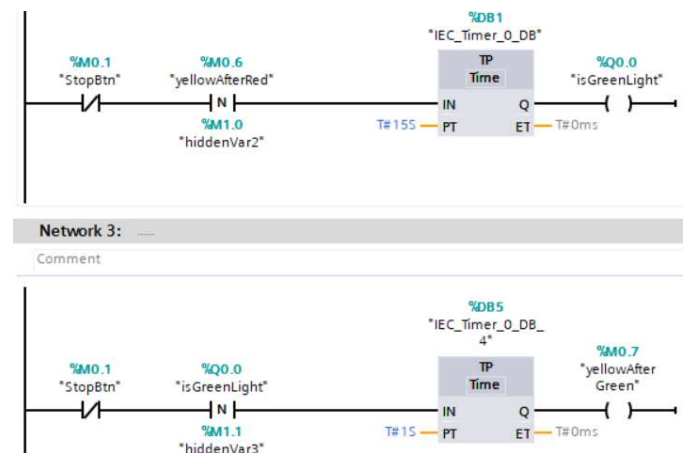


Fig. 3. Ladder diagram for changing the state of the traffic light

Due to the limited volume of the paper, fig. 3 shows only part of the ladder-logic diagram [3] (Network 3 and Network 4 are depicted) for the TP timer instructions in order to create a multiphase flip-flop. This diagram assumes appearing negative front as input pulse signal for this phase (time interval) when the previous phase expired. The first TP timer is preset with a value of 15 seconds and output "1".

When the "START" button on the HMI is pressed, the Network 1 (not depicted on fig.3 due to paper length constraints) is TRUE, the TP timer output Q is set to "1" for 20 seconds (duration of interval A), and the lights "Red 1" and "Green 2" are on. When the time interval A expires, the traffic light system changes the state and goes to the next phase, in which the "Yellow" and "Red 1" glow together (tag "YellowAfter Red"). When this phase (time interval of "Yellow" = 1s) expires, the next phase starts, causing the lights "Green 1" and "Red 2" to be on (fig. 3, Network 3, tag name "isGreenLight"). When this phase (time interval B) expires, "isGreenLight" negative signal edge is detected (fig. 3, Network 4, --|N|-- instruction scans the operand for negative signal edge) and the last phase starts, causing the "Yellow" light to be on. Then, the loop starts from the beginning.

The third node of the developed system is the HMI on which the buttons and textboxes for controlling are located. They implement the following functionalities when working with the timer controller:

- Selection of the operating mode - by pressing the "Start" or "Stop" buttons the logical signal level of the microcontroller is inverted, thereby assigning the operation mode of the traffic light system to day or night respectively;
- Input the value of the time intervals (for red, yellow, and green signals). Using these controls, the required values for duration of intervals A and B are set. After setting the duration time of the intervals, they are recorded in the PLC's data memory.

The HMI panel (SIMATIC HMI, KTP700 Basic) is configured with IP address 192.168.1.30 and communicates with the PLC controllers through the Profinet protocol.

The PLC controllers are configured with the following IP addresses: Client - 192.168.1.10 and Server - 192.168.1.20. For the communication between them, Modbus and Secure Modbus protocols are used.

The "MB\_SERVER" instruction [1] is used for communication as Modbus server over the PROFINET interface of the CPU. The "MB\_SERVER" instruction processes the requests of a Modbus client and also receives Modbus requests and sends response messages.

The implementation of Secure Modbus in TIA Portal is easy, as the only thing that has to be done is issuing or adding the certificates of the devices that have to communicate in encrypted way and replacing the CONNECT variable as it is shown in fig 4 ("CONNECTION" value of the variable is used for Modbus communication and "SECURE\_CONNECTION" value is used for Secure Modbus).

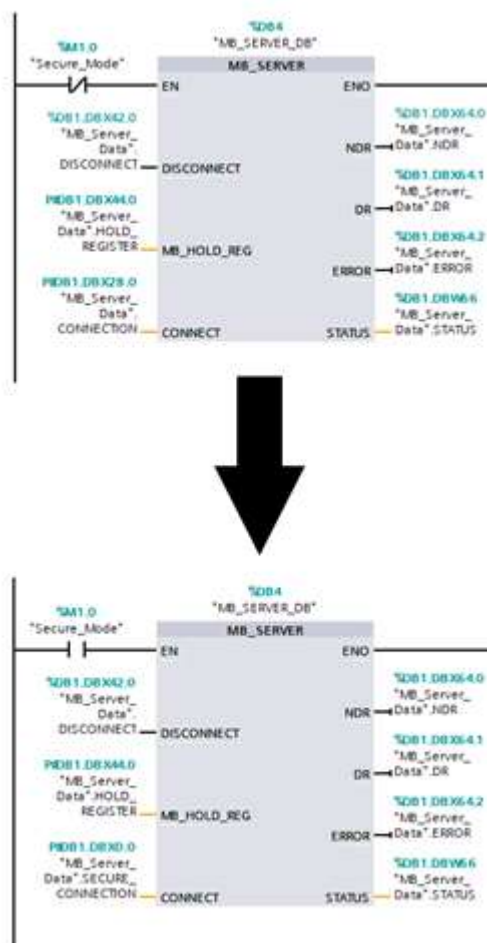


Fig. 4. Replacing the CONNECT variable from "CONNECTION" to "SECURE\_CONNECTION"

The algorithm for switching from Modbus to Secure Modbus communication includes the following actions:

- Creating certificates for each device in the Secure Modbus communication;
- Adding the certification authority to each device;

- Importing the certificate to the respective device;
- Configuring the devices to work with the certification authority and with the imported certificate;
- Testing the Secure Modbus communication. Here, the devices use the lowest common version of TLS that all devices support during the handshake process.

### III. LABORATORY EXERCISE EXPERIMENT

The aim of the lab is to explore the possibilities for conducting man-in-the-middle (MITM) attacks in industrial networks when using one of the most widely spread protocols - Modbus and then exploring the capabilities for protecting from MITM attacks by changing the communication protocol from Modbus to Secure Modbus. The lab is meaningful for the students due to the fact that Modbus is implemented in almost every PLC controller.

After customizing the parameters of the ladder diagram of the traffic light system, students have to press the "START" button on the HMI to start the PLC server controller.

There are some peculiarities for conducting the experimental cyberattack:

- using Ettercap, hosts in the network are scanned, after which the client with IP address 192.168.1.10 is selected as target 1 and the server with IP address 192.168.1.20 is selected as target 2. After selecting the targets, an ARP poisoning attack of the network is performed;
- After the ARP poisoning attack, using Wireshark, the Modbus packets sent (for reading and writing in the address space of the traffic light system) can be analyzed by the "hacker". In real environment, this would expose to a risk the safety of people and cars, as the hacker will be able to affect the traffic light system. For example, when using the unprotected version of Modbus protocol, an external device using QmodMaster can read from the server the information about the operating mode of the traffic light system, then compromise it. In the case of the laboratory exercise, the "hacker" will be able to switch the traffic light system to night mode by writing "1" in the memory of target 2 (address 40002).


In order to simulate an attack, the students that act as a hacker use third PLC controller (fake client) that has Siemens S7-1200 Simulator Module with 8 Inputs connected to it. By changing the value of the switch SW1, that is connected to the fake client, students try to write "1" in address 40002 of the server memory. When using unprotected Modbus communication, the fake client can read and write data in the memory of the server controller of the traffic light system. If a student reads "1" from the tag in the server (192.168.1.20) memory as operating mode, he or she will be able to change this tag to "0". As soon as the value for this tag becomes "1", server controller goes to night mode and starts generating "Yellow" pulses as an output with intervals of 1 second, in which the light is on and 1 second, in which the light is off.

Unlike unprotected Modbus, where by using sniffer software, the data in packets could be read, in protected mode - Secure Modbus (Fig. 5), the communication is encrypted, i.e. captured data are useless.




ens33

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp



tls



No	Time	Source	Destination	Protocol	Length	Info
0.	0.138149480	192.168.1.10	192.168.1.20	TLSv1.2	88	Application Data
0.	0.167454366	192.168.1.20	192.168.1.10	TLSv1.2	87	Application Data
0.	0.172152055	192.168.1.10	192.168.1.20	TLSv1.2	93	Application Data
0.	0.188435413	192.168.1.20	192.168.1.10	TLSv1.2	88	Application Data
0.	0.191638619	192.168.1.10	192.168.1.20	TLSv1.2	88	Application Data
0.	0.206430666	192.168.1.20	192.168.1.10	TLSv1.2	87	Application Data
0.	0.210358722	192.168.1.10	192.168.1.20	TLSv1.2	93	Application Data
0.	0.232463646	192.168.1.20	192.168.1.10	TLSv1.2	88	Application Data
0.	0.236017101	192.168.1.10	192.168.1.20	TLSv1.2	88	Application Data
0.	0.255466610	192.168.1.20	192.168.1.10	TLSv1.2	87	Application Data
0.	0.259769610	192.168.1.10	192.168.1.20	TLSv1.2	93	Application Data
0.	0.276429345	192.168.1.20	192.168.1.10	TLSv1.2	88	Application Data
0.	0.280339784	192.168.1.10	192.168.1.20	TLSv1.2	88	Application Data
0.	0.294445325	192.168.1.20	192.168.1.10	TLSv1.2	87	Application Data
0.	0.297996246	192.168.1.10	192.168.1.20	TLSv1.2	93	Application Data
0.	0.312430511	192.168.1.20	192.168.1.10	TLSv1.2	88	Application Data
0.	0.316381655	192.168.1.10	192.168.1.20	TLSv1.2	88	Application Data

Frame 38: 93 bytes on wire (744 bits), 93 bytes captured on interface ca

Ethernet II, Src: Siemens\_cb:d8:82 (ec:1c:5d:cb:d8:82), Dst: Siemens\_cb:d8:82 (ec:1c:5d:cb:d8:82)

Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20

Transmission Control Protocol, Src Port: 54746, Dst Port: 54746

Transport Layer Security

TLSv1.2 Record Layer: Application Data (Protocol: TLSv1.2)

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 34

Encrypted Application Data: 9596e9f8fc068d8fee

0000

00 0c 29 e2 20 64 ec 1c 5d cb d8 82 08 00 45 00

..).d.]....E.

0010

00 4f 9f 20 00 00 40 06 58 1a c0 a8 01 0a c0 a8

-0-.-@.X.....

0020

01 14 d5 da 01 f6 ba e6 13 b9 ba 7b 92 bd 50 18

.....{..P.

0030

20 00 04 fd 00 00 17 03 03 00 22 95 96 e9 f8 fc

.....".....

0040

06 8d 8f ee 56 3e 94 ce 2e f7 cd 66 7c 82 8b be

...V>...f|....

0050

af c1 d9 68 a6 9d 9e 75 82 52 2b 59 45

...h...u..R+YE

Fig. 5. Communication over Secure Modbus

The data in the captured packets is in unreadable format and MITM attack could not be conducted (because crypto keys are 2048-bit and it requires a significant time to break).

Additionally, when using the secure communication, students that act as a hacker cannot send to the server controller valid requests for writing data in its memory, because their certificate (working on this controller) is not signed by the certification authority.

During the lab exercise, it is discussed that IIoT security should be improved by using encrypted protocols, such as Secure Modbus (as it is shown on figure 5). The screenshot from Wireshark shows an encrypted connection between two Siemens industrial controllers - client and server. According to the author of the paper, ARP poisoning attacks can easily be prevented by statically configuring the ARP protocol.

#### IV. CONCLUSION

The proposed laboratory exercise investigates the security of a traffic light system (part of a smart city) implemented by using Siemens industrial controllers with connection between one another through Modbus and Secure Modbus protocols. The results obtained here are of great importance not only for engineering education but also for practice and cybersecurity of IIoT. Here are some notes for the implementation of the traffic light system: the power can be supplied to the traffic light lamp through optotriacs. In the control circuit of the optotriacs voltage of 24 V is applied through the relay contacts of the server PLC controller. Each traffic light lamp is connected to the power 230V outputs (line and neutral wires) of the optotriac module that is controlled by signals from the corresponding pins of this PLC controller.

#### ACKNOWLEDGEMENT

The author of this paper would like to thank the Research and Development Sector at the Technical University of Sofia for the financial support.

#### REFERENCES

- [1] [https://cache.industry.siemens.com/dl/files/340/102020340/att\\_118119/v6/net\\_modbus\\_tcp\\_s7-1500\\_s7-1200\\_en.pdf](https://cache.industry.siemens.com/dl/files/340/102020340/att_118119/v6/net_modbus_tcp_s7-1500_s7-1200_en.pdf)
- [2] <https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-modbus-protocol-in-depth.html>
- [3] Khaled K. et. al., Programmable Logic Controllers Industrial Control, McGraw-Hill Education, ISBN: 978-0-07-181047-0, p.344
- [4] V. Samokisheva, R. Trifonov and G. Pavlova, "Risks and Challenges of Using Ai In Healthcare," 2024 12th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2024, doi: 10.1109/COMSCI63166.2024.10778509
- [5] Chekurov I., Hristov K., Design and Implementation of an Adaptive FPGA-Based Traffic Light Control System Using Verilog, Proceedings of the 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2025, IEEE Conference, Rec # 66328, Ohrid, N. Macedonia, June 26-28, 2025, Accepted
- [6] K. Hristov, "Approach for control of a Three-phase power converter with xPC Target Software," 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2021, pp. 415-417, doi: 10.1109/ISMSIT52890.2021.9604565.