MODBUS and Network Hacking Laboratory

Cyber Physical Systems and IoT Security - Prof. Alessandro Brighente, 2022/2023

Description

In this lab, you are connected in the same network of a client/server application working over MODBUS/TCP, variation of the protocol for supervisioning and controlling industrial equipment. This version has the useful caractheristic to work over the TCP/IP protocol suite, making is suitable in many different environments.

The application running is a very simplified control system that can read/write elementary commands.

Short Overview

MODBUS encodes the data with Big Endian representation, meaning that when information is sent through the network, the Most Significant Byte (MSB) is sent first. This is an example (same as in the lab), where we have MODBUS packets of 16 bits:

```
16-bit      0x1234  -->  0x12 0x34
```

In this case, we use a "custom" MODBUS implementation structured as follows:

```
|-- TRANSACTIN ID (1B)
|
|-- PROTOCOL ID   (2B)
|-- LENGTH        (2B)
|-- UNIT ID       (1B)
|
|-- ACTION        (1B)
|-- ADDRESS       (2B)
|-- VALUE         (2B)
```

Info & Goal

You know that in the network there is a MODBUS server controlling two LEDs, the states of the LEDs are ON and OFF. In the same network there is a MODBUS client managing the state of the LEDs, sending MODBUS messages through TCP/IP. You know that the server can handle multiple connection at the same time.

Your goal is to get the modbus packets, understand the protocol structure and inject your messages to control the LEDs. In a second time, you can DOS the server in order to keep the LEDs off.

```
|--MODBUS server --|
|                  |-- LED 1
|                  |-- LED 2
|
|-- MODBUS client
|
|
|-- Your PC
```

What you need

Your laptop (probably in groups) with these tools installed:

- nmap
- arspoof
- wireshark
- suggested: python3 for scripting

We can take care of Ethernet Adapters, Cables, and Switch.

In order to get your ETH adapter in the same network, you can manually set the IP of the adapter in this range:

```
IP adapter network: 169.254.0.0/16
DO NOT USE 169.254.0.1 or 169.254.255.255
Everything in 169.254.26.1-30 is the best option
```