The security robustness of Modbus/TCP protocol in industrial control systems

Hassan Alsaad

Advisor: Mohammadjafar Esmaeili, Ph.D.

Department of Engineering Management, Systems, and Technology, University of Dayton

Objectives

- For remote applications, multiple PLCs can be connected to each other to form a controlling network that uses Modbus/TCP communication protocol utilizing private/ public networks.
- This research focuses on examining the security vulnerability of the Modbus/TCP protocol in Industrial control systems.

Methodology

1. To achieve this goal the researchers utilizes Modbus PLC simulator to simulate different cyber attacks through the local network.
2.The cyber attacks have been formed using the MBTGET Perl script and Metasploit module, in Kali Linux as a penetration testing operating system.

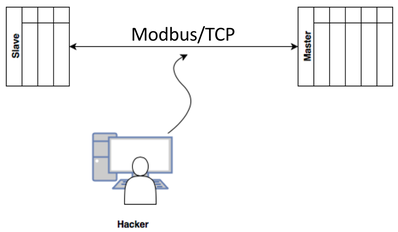


Figure 1: Network Diagram

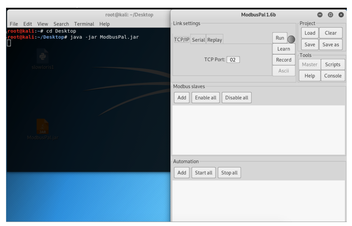


Figure 2: Downloading and Opening the Modbuspal.jar.

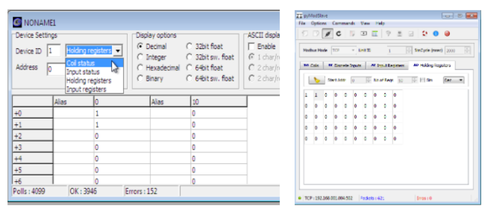


Figure 3: Configure Modbus/TCP connection between the master and slave.

Results

Our research shows some of the major security vulnerability in the Modbus/TCP protocol, which is one of the main communication protocols in ICS system.

Figure 4: The result of searching for modbus/TPC 502 on the network

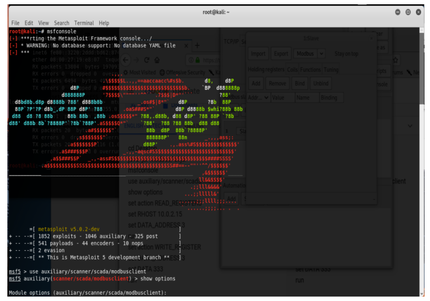
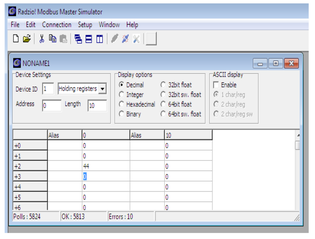


Figure 5: using the msfconsole hacking tool .



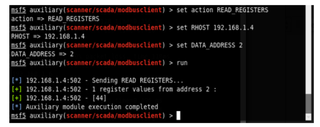


Figure 6: Read the value form “Holding Register” address 2 of the slave.

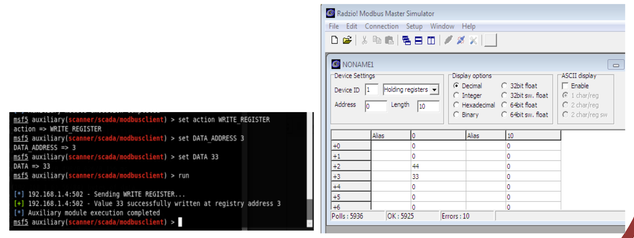


Figure 7: The result of searching for modbus/TPC 502 on the network

Conclusions

- In most of today's applications such as Experimental Physics and Industrial Control Systems (EPICS), Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS) and Programmable Logic Controllers (PLCs) system are getting connected to the internet without paying attention to the security robustness of these devices.
- Industrial Control Systems (ICS) such as SCADA, DCS, PLCs are communicating with industrial equipment such as actuators, sensors, motors, and pumps using a special communication protocol called Modbus, the Industrial should paying attention to the security robustness.