Hes·so VALAIS WALLIS
Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

PV presentation scenarios

Date : 10/06/2024
Houre : 15h05 → 16h05
Participants : M. Rieder et R. Heredero

1 Summary attacks scenario

Rémi summary the scenario that have been choose during the last meeting.

1. A wireless replay attack on Zigbee or wireless M-Bus. Rémi prefer Zigbee but wM-Bus is completly relevent for industrial application.
2. A DoS attack by an external sensor. The goal is not to simply saturate the communication medium but to saturate the PLC itself with valid packets. (Medard suggest to use Can Bus for this scenario)
3. A Man in the Middle attack on Modbus/TCP without encryption. An example of how easy it is impersonnate someone else on an unsecured bus. One solution would be to encrypt the communication with a symmetrical key and use a Diffie-Hellman exchange.
4. A Man in the Middle attack on Modbus/TCP with encryption by symetric key (exchange with Diffie-Hellman). The goal is to show that even with encryption, if the attacker can intercept the communication since the beginning, he can impersonnate the device. The solution is to use certificates like Modbus over TLS.

2 Presentation simulation scenario

2.1 Factory I/O

Rémi present Factory I/O. It's a realistic simulation software that can be used to simulate a factory. It's expensive (~4300.- lifetime for 10 students). It's possible to create custom scenes. Factory I/O might be interresting for Power & Control. The software can only communicate with Modbus over TCP. The simulation doesn't include anything about security. It have to be implemented by a third soft that interface with Factory I/O for add security layer. Rémi test it on Linux and it work quite well with wine but he couldn't get it to work properly on a docker container (He didn't test a lot).

Scenario would be that the PLC control the palletizer scene. A Wireless sensor could indicate the presence of a truck to be loaded. The Wireless replay attack could be done on this sensor. The DoS attack could be done on the same sensor. The MitM attacks could be made on the Modbus/TCP communication between the PLC and the palletizer and the goal would be to control the clamp.

2.2 Home I/O

Home I/O is made by the same compagny that Factory I/O. It simulate an House with a lot of domotic. It's cheaper than Factory I/O (~300.- lifetime for organization) and can maybe used by ETE students too. Home I/O need another software (Connect I/O) for communicate with Modbus. A third software have to be used for add security layer. Rémi tried it a bit on Linux and although Home I/O works perfectly well, he wasn't able to get Connect I/O to work. This soft need to be used on Windows.

Scenario would be that the PLC control the alarm and acces system with main door and garage. The garage door could be open by a wireless remote. The Wireless replay attack could be done on this remote. A external presence detector on front of the main door could be use for the DoS attackremote. The MitM attacks could be made on the Modbus/TCP communication between the PLC and the alarm system and the goal would be to open the main door.

2.3 Minecraft

Rémi suggest to use the Electrical age world of Minecraft that was used on 2th year with Christopher. This goal of this lab was to control a Factory and a energy system for produce the most as possible. It can be interresting for student to continue this lab for attack / secure the communication. On Minecraft it also possible to do security with Open Computer or even create a extension mod in Electrical age for Modbus over TLS (maybe more simple than use Open Computer on Lua).

Scenario would be to reused the PLC made on the last lab that control everything. It can be interresting to build a physical HMI part that set Factory and Coal production in the same way as the HTML page we had on the last lab. A wind wireless sensor could be added. The Wireless replay attack and DoS attack could be done on this sensor. The MitM attacks could be made on the Modbus/TCP communication between the PLC and the Factory and the goal would be to control the Factory.