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 chosen during the last meeting.

1. A wireless replay attack on Zigbee or wireless M-Bus. Rémi prefers Zigbee, but wM-Bus is completely relevant 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 suggests using Can Bus for this scenario)
3. A Man in the Middle attack on Modbus/TCP without encryption. An example of how easy it is to impersonate 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 symmetric 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 impersonate 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 interesting for Power & Control. The software can only communicate with Modbus over TCP. The simulation doesn't include anything about security. It has to be implemented by a third soft that interface with Factory I/O to add a security layer. Rémi tested it on Linux, and it works quite well with wine, but he couldn't make it work properly on a docker container (He didn't test a lot).

The scenario would be that the PLC controls 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 company that Factory I/O. It simulates 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 needs another software (Connect I/O) to communicate with Modbus. A third software had to be used to add a 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 needs to be used on Windows.

The scenario would be that the PLC controls the alarm and access 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. An external presence detector on in front of the main door could be used for the DoS attack. 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, suggests using the Electrical age world of Minecraft that was used in 2nd year with Christopher. The goal of this lab was to control a Factory and an energy system for produce the most as possible. It can be interesting for students to continue this lab to attack / secure the communication. On Minecraft, it is also possible to do security with Open Computer or even create an extension mod in Electrical age for Modbus over TLS (maybe more simple than using Open Computer on Lua).

The scenario would be to reuse the PLC made in the last lab that controls everything. It can be interesting to build a physical HMI part that set Factory and Coal production in the same way as the HTML page we had in 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.