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

PV kickoff

Date : 27/05/2024
Houre : 9h55 → 10h30
Participants : M. Rieder, M. Clausen, (D. Gabioud) et R. Heredero
Next meeting : 03/06/2024 - PM

Small takl before meeting

Small talk with D. Gabioud. He said that 862 MHz is used in use in buildings. It is a standard that is not encrypted and is considered to be used only in a "safe" environment. He also said that the wago PLCs do not have wireless communication natively.

Presentation of the project

M. Rieder explain the project to M. Clausen. He really want a physical part in the interception. The goal is to show a problem, exploit it and propose a solution. It should be more on the communication side. Wiring modbus and wireless 862 MHz look that the main axes of the project. It asked to have at least a scenario of attack:

- Denial of service (DoS)
- Man in the middle

M. Clausen also said that it can be interessant to hack a zigbee radio.

Discussion about simulation

M. Clausen didn't really like Winter Resort Simulator Pro. He proposed to use Factory io instead. It is a game that is made to be controlled by sps. It is also possible to simulate and interface with modbus. I still ask for a license to Winter Resort Simulator Pro.

Tasks

For next week, propose scenarios of attacks. Think to solutions.

For the next 2 weeks (10 June), propose 4 scenarios of attack with idea of solution. Also propose scenarios for simulation.