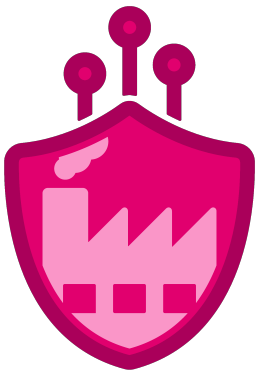
Hes·so VALAIS WALLIS

School of Engineering

OT Security

Graduate Rémi Heredero



Bachelor's Thesis
| 2024 |

Objective
Produce attack scenarios that include an unsecure situation, an attack, and a solution to secure against such attack. These scenarios must be usable as the basis for a laboratory experience for students or industrial partner formation.

Methods | Experiences | Results
This thesis is separated into 2 scenarios. The first one, the Man in the Middle attack, consists of intercepting the communication between two devices and modifying the packets. The second scenario is a replay attack on a wireless transmission medium performed with a flipper zero.

The first scenario (Man in the Middle) is implemented on a modbus/TCP communication between a controller and a house security system. An attacker (a Kali Linux laptop) redirects communication to him to modify the sensor value sent to the controller. He can also send fake data. This Thesis also shows what happens if you secure your communication with certificates (modbus/TLS) but do not check the certificates. The attacker can intercept the communication in the same way. This thesis shows that it is important to always check certificates to guarantee the interlocutor.

The second scenario (Replay) is implemented on a 433MHz basic wireless communication. A flipper zero can record the transmission and replay it to trigger the same effect. Securing it is simple with implementation of a rolling code or signature. If the message is unique, an attacker cannot replay it.

Degree programme
Systems Engineering

Field of application
Infotronics

Supervision professor
Prof. Medard Rieder
medard.reider@hevs.ch