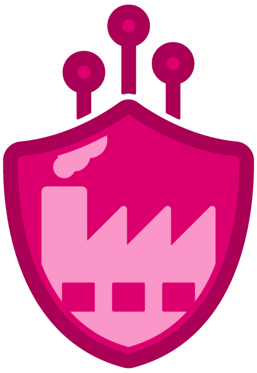
Hes·so VALAIS WALLIS

School of Engineering

OT Security

Graduate Rémi Heredero



Objective

Produce attack scenarios where each includes a vulnerability, an attack using the vulnerability, and a solution to avoid the attack. These scenarios must be usable as the basis for a laboratory experiment for students or industrial partners.

Methods | Experiences | Results

This thesis is divided into 2 scenarios. The first one, a Man in the Middle attack, consists of intercepting the communication between two devices and modifying the packets exchanged. The second scenario is a replay attack on a wireless transmission medium performed with a Flipper Zero.

The first scenario (Man in the Middle Attack) is implemented on a Modbus/TCP communication between a controller and a house's security system. An attacker (a Kali Linux laptop) redirects communication to him to modify the sensor values sent to the controller. It is also possible to sent fake data. This Thesis also shows how securing the communication with certificates (Modbus/TLS) but without certificate validity check can be subject to an attack too. The attacker can intercept the communication in the same way. The thesis concludes that it is important to 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 later to trigger the same effect. Securing such a communication can be simply implemented by using a rolling code or a signature. If each message is unique, an attacker cannot replay it.

Bachelor's Thesis

| 2024 |

Degree programme
Systems Engineering

Field of application
Infotronics

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