Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

Presentation and choice of simulations scenarios

Rémi Heredero

Monday, 10th of June 2024

Attacks

- *Wireless* Replay (Zigbee or wM-Bus)
- Dos by **external** sensor with valid packet
- MitM on Modbus over TCP
- MitM on Modbus over TCP with standard encryption

Factory I/O

- PLC manage palletizer
- *Wireless* **external** sensor for truck detection
- MitM on clamp

➕ Realism

➖ ~4300.-

➕ Customization

Security by third party

Home I/O

- PLC manage garage and door
- ***Wireless*** remote for garage
- **External** sensor for presence detection (door)
- MitM for opening door

➕ ~300.-

➖ Customization

Security by third party

Minecraft

- PLC already exist with Java lab
- Wireless wind sensor
- Add Physical HMI for setter (MitM on it)

➕ Pursuite of a lab

➕ Already got it

➕ Full customization

Security by OC or new mod

Summary

	Price	Security	Customization	Cross-patform
Factory I/O	~4300.-	by third soft	yes	no
Home I/O	~300.-	by third soft	no	no
Minecraft	-	OC or new mod	full	yes