



OT Security

PEN-testing and security about embedded devices

Mid-term presentation

Rémi Heredero

Tuesday the 2nd of July 2024

This thesis

This thesis

- Labo OT Security - I6

This thesis

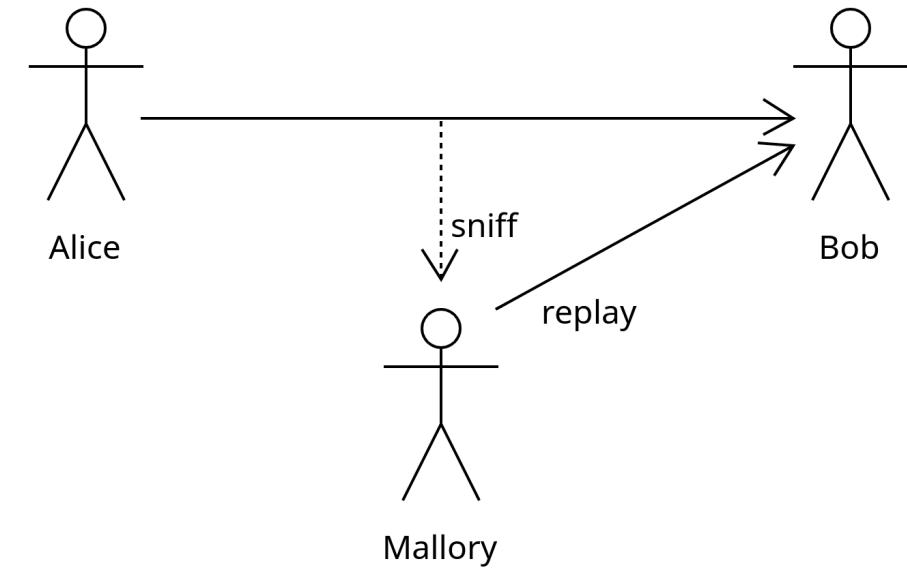
- Labo OT Security - I6
- 3-4 security scenarios

This thesis

- Labo OT Security - I6
- 3-4 security scenarios
- Industrial partner training

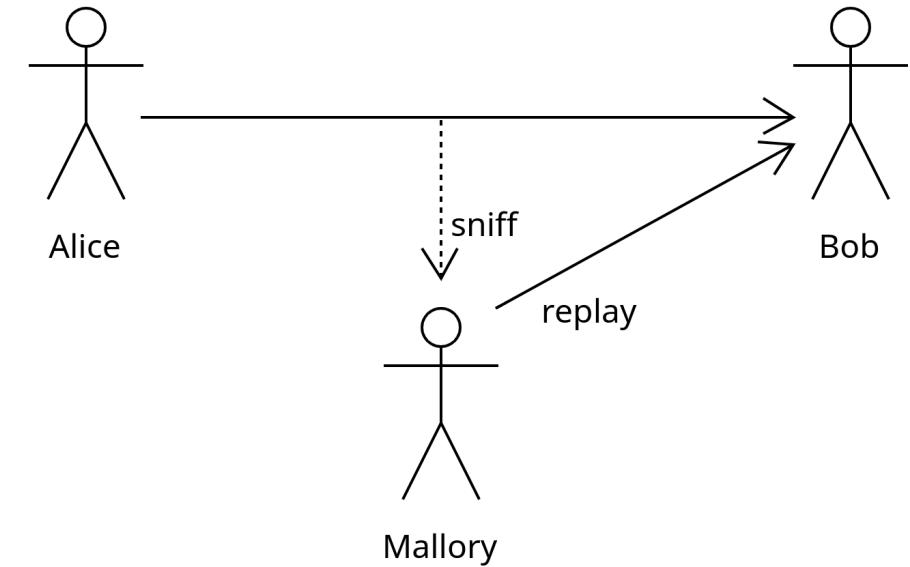
Attacks

Replay



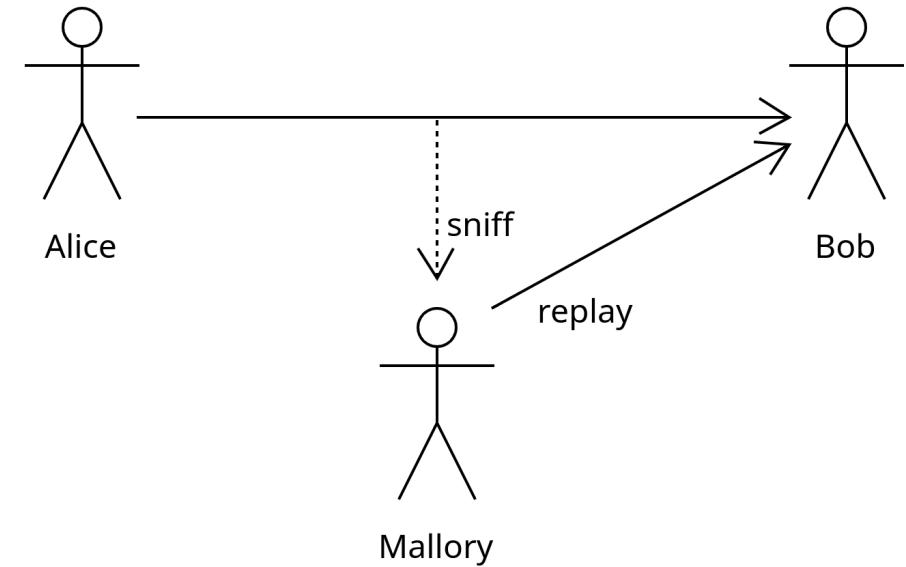
Replay

- On wireless

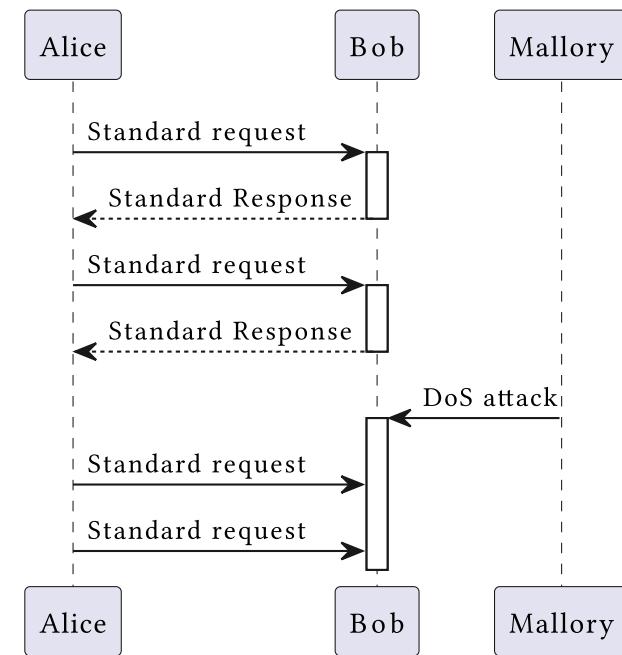


Replay

- On wireless
- On physical layer

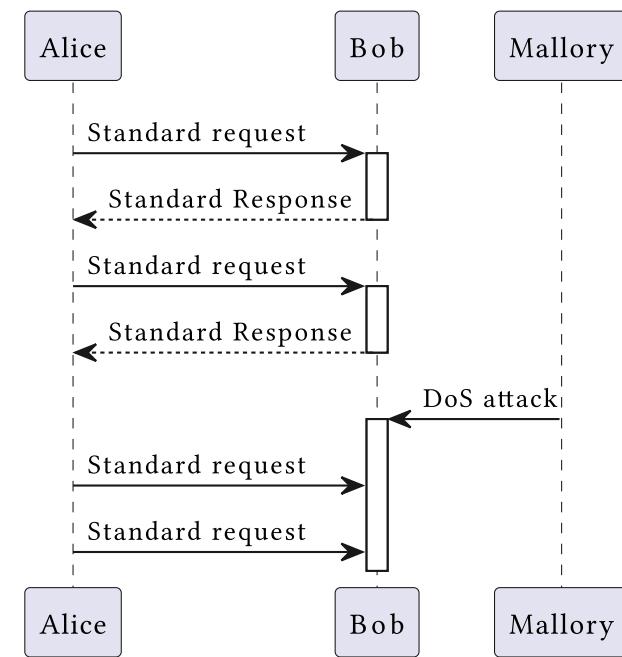


Denial of Service (DoS)



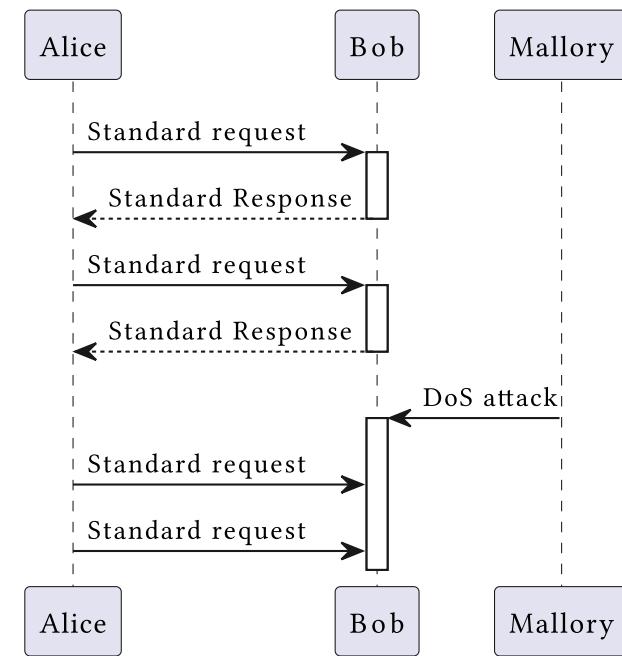
Denial of Service (DoS)

- Too many requests



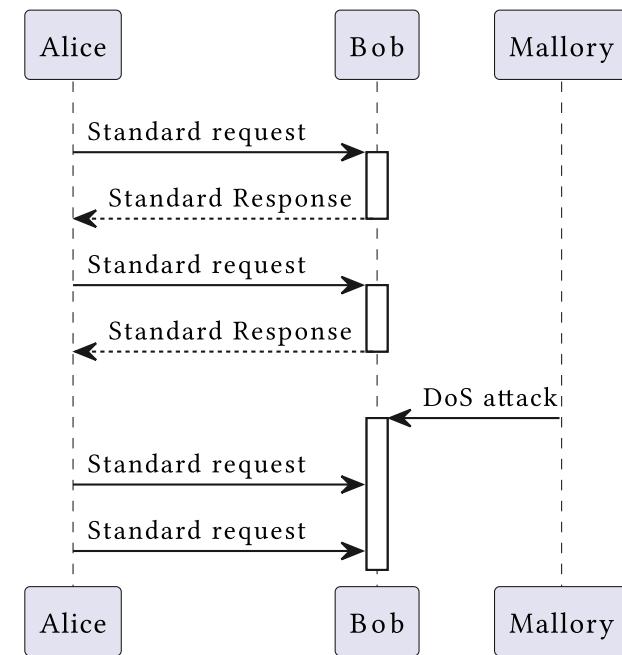
Denial of Service (DoS)

- Too many request
- Overload controller not network



Denial of Service (DoS)

- Too many requests
- Overload controller not network
- Valid request



Man in the Middle (MitM)

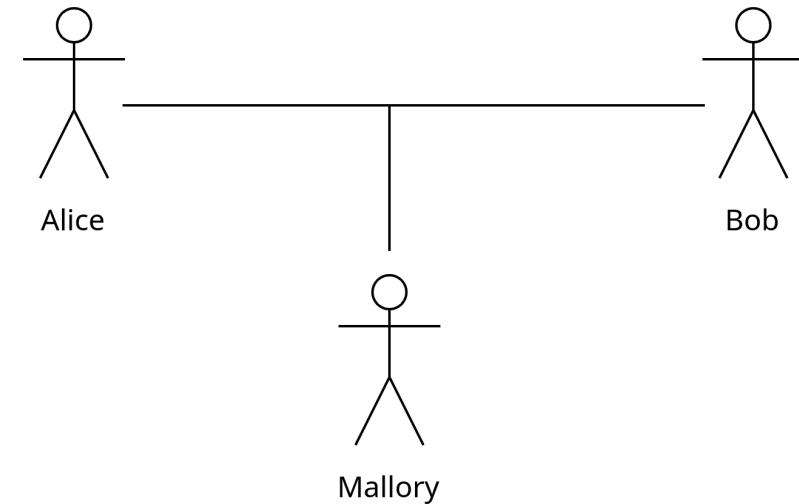
Man in the Middle (MitM)

- Intercept, modified or inject

Man in the Middle (MitM)

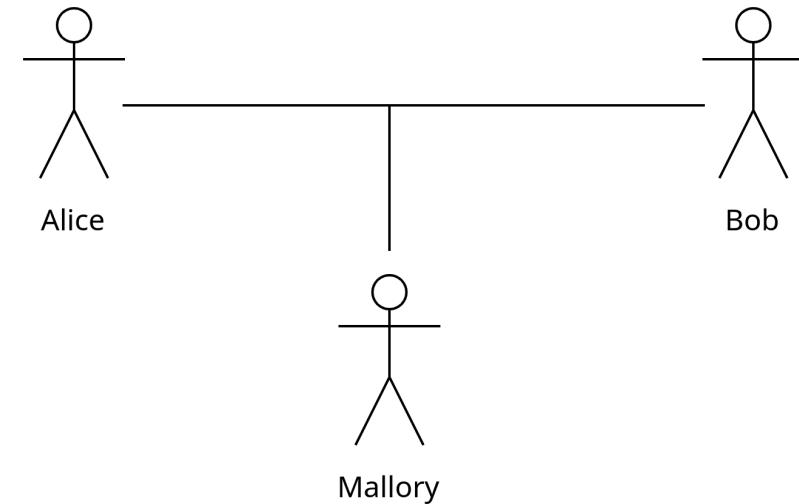
- Intercept, modified or inject
- 2 phases

MitM - connected



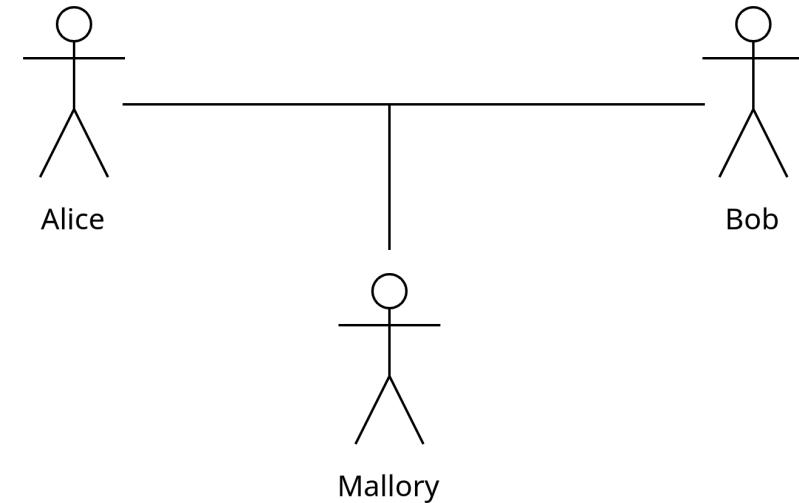
MitM - connected

- Unsecure communication



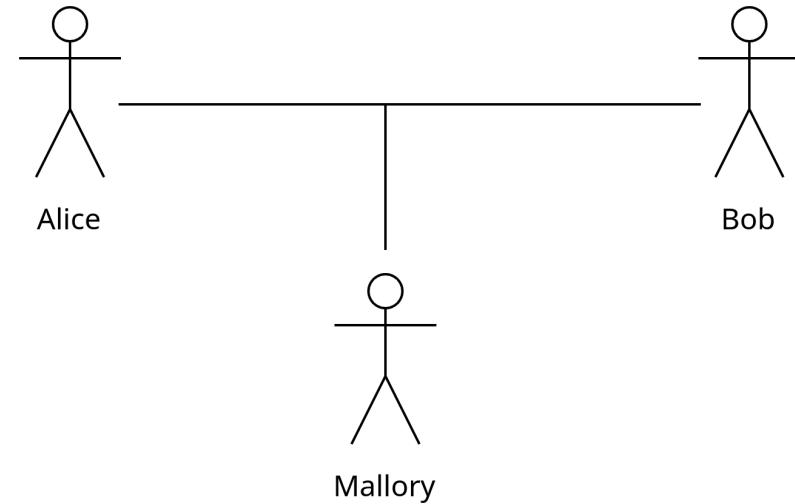
MitM - connected

- Unsecure communication
- Send fake message

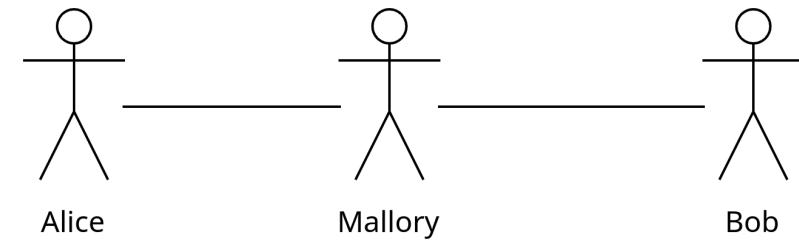


MitM - connected

- Unsecure communication
- Send fake message
- Encryption with symmetric key
(Diffie-Hellman)

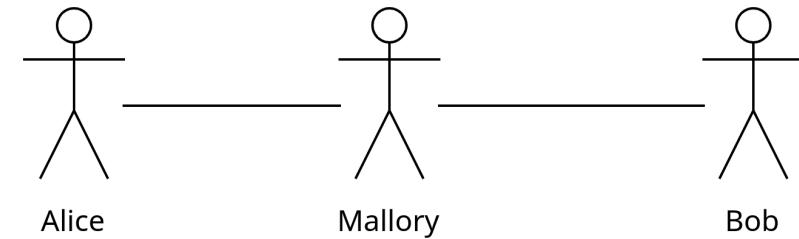


MitM - full interception



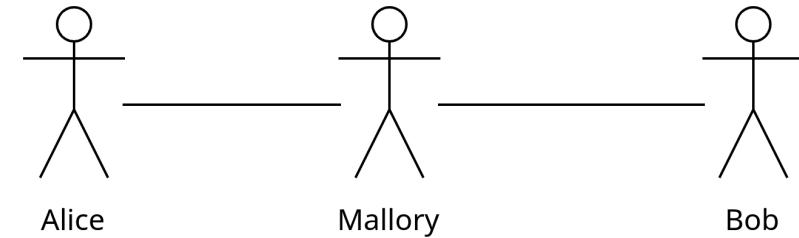
MitM - full interception

- From Diffie-Hellman



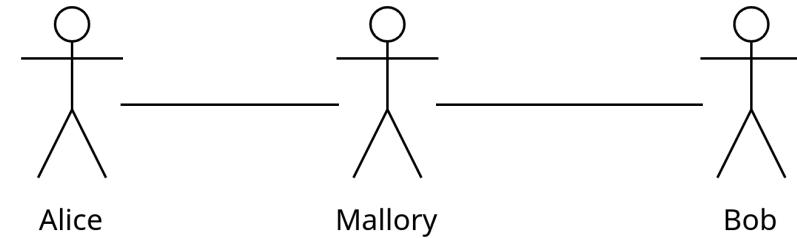
MitM - full interception

- From Diffie-Hellman
- Impersonnate key



MitM - full interception

- From Diffie-Hellman
- Impersonnate key
- Use modbus over TLS



Simulation environment

Other choices

Factory I/O



Other choices

Factory I/O



- Simulation of a factory

Other choices

Factory I/O



- Simulation of a factory
- Realistic

Other choices

Factory I/O



- Simulation of a factory
- Realistic
- Some scenes already prepared

Other choices

Factory I/O



- Simulation of a factory
- Realistic
- Some scenes already prepared

Minecraft



Other choices

Factory I/O



- Simulation of a factory
- Realistic
- Some scenes already prepared

Minecraft



- Simulation of anything

Other choices

Factory I/O



- Simulation of a factory
- Realistic
- Some scenes already prepared

Minecraft



- Simulation of anything
- Cross platforms

Other choices

Factory I/O



- Simulation of a factory
- Realistic
- Some scenes already prepared

Minecraft



- Simulation of anything
- Cross platforms
- Security in Open Computer

Home I/O



Home I/O

- House with domotic



Home I/O

- House with domotic
- Also for ETE students



Home I/O

- House with domotic
- Also for ETE students
- Garage and solar panels by M. Clausen



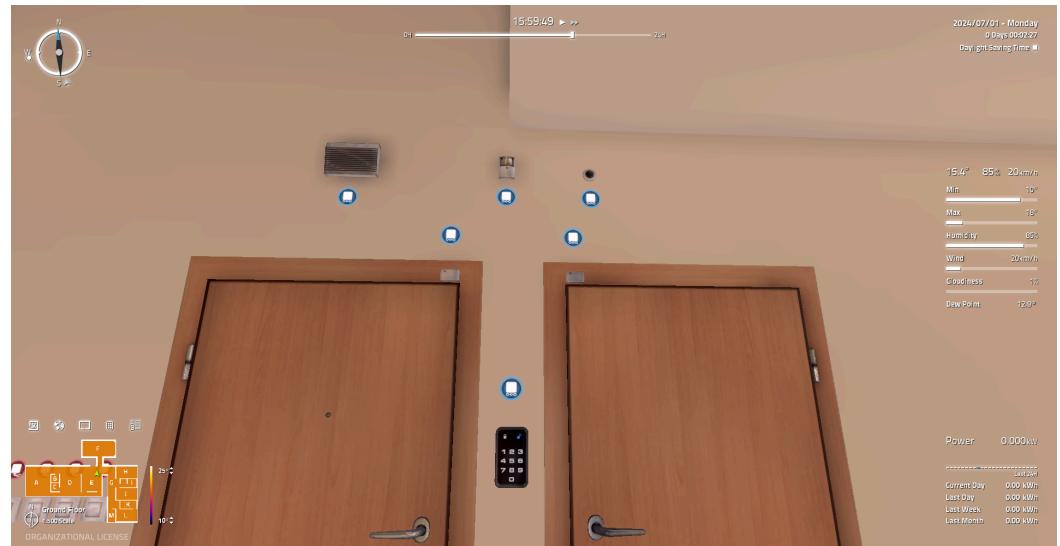
Communication media

Modbus



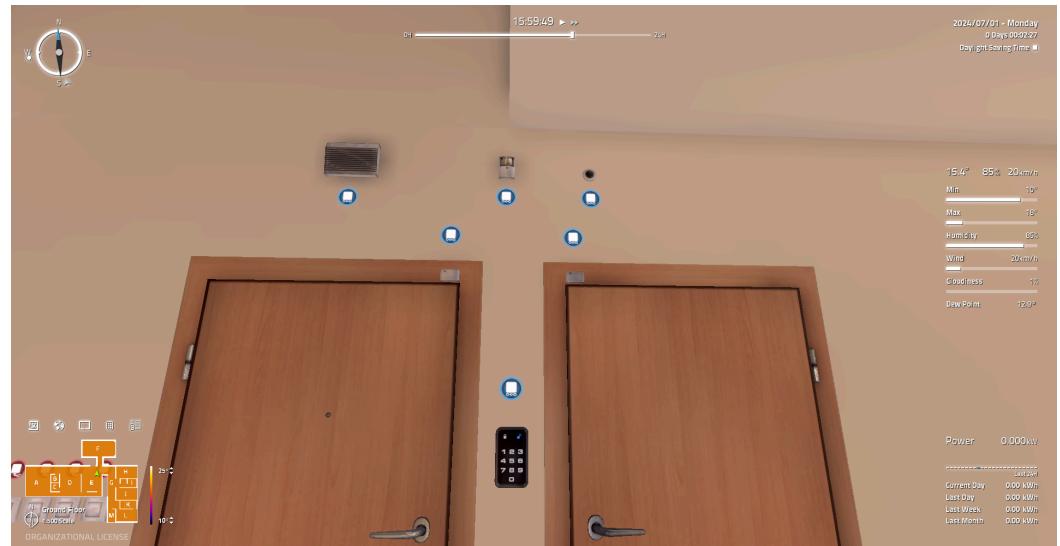
Modbus

- RTU - TCP



Modbus

- RTU - TCP
- For Man in the Middle
→ deactivate alarms



Wireless M-Bus (wM-Bus)

Wireless M-Bus (wM-Bus)

- Use Flipper Zero

Wireless M-Bus (wM-Bus)

- Use Flipper Zero
- No frequency hopping

Wireless M-Bus (wM-Bus)

- Use Flipper Zero
- No frequency hopping
- Europe for meters

Wireless M-Bus (wM-Bus)

- Use Flipper Zero
- No frequency hopping
- Europe for meters
- Mode T / mono-directional

Wireless M-Bus (wM-Bus)

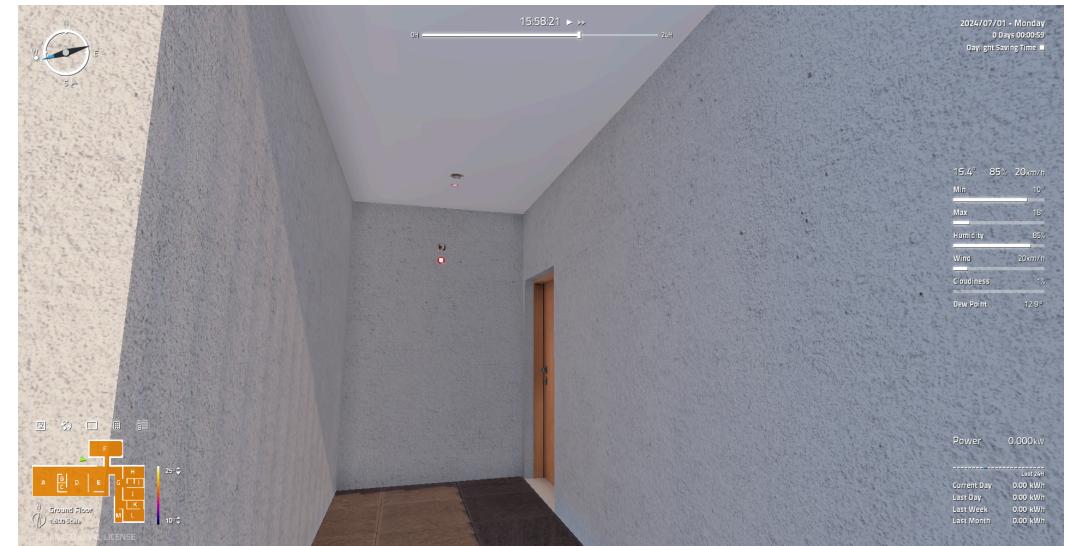
- Use Flipper Zero
- No frequency hopping
- Europe for meters
- Mode T / mono-directional
- On electricity meter

Wireless M-Bus (wM-Bus)

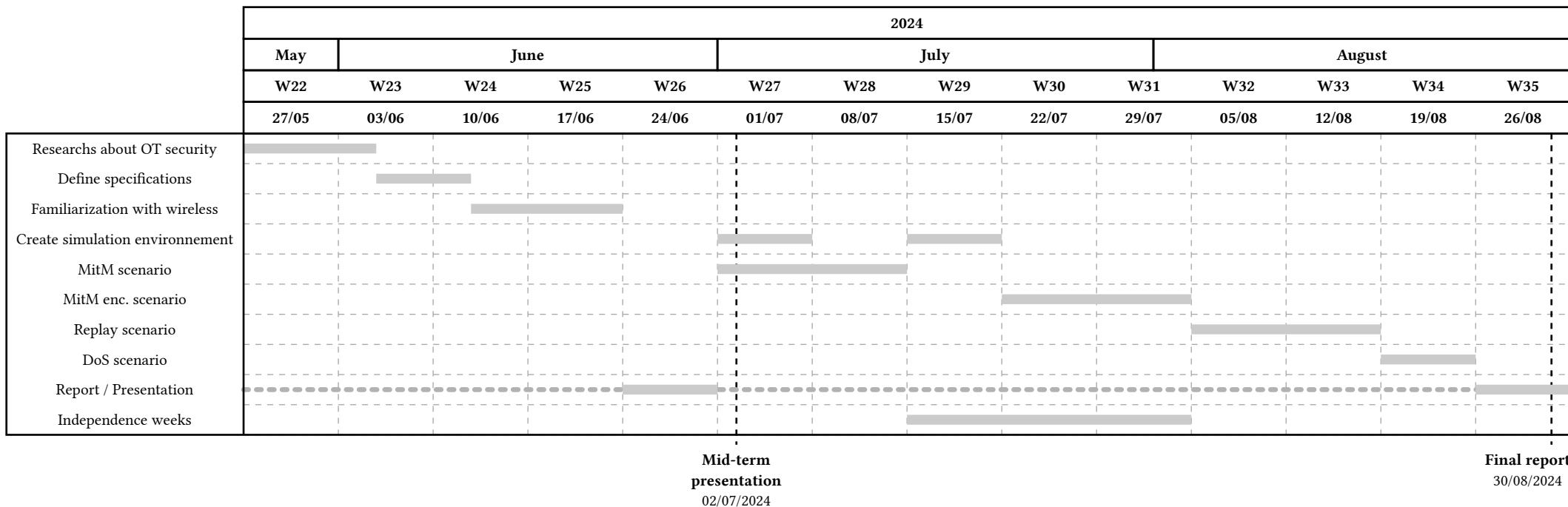
- Use Flipper Zero
- No frequency hopping
- Europe for meters
- Mode T / mono-directional
- On electricity meter
Sniff low consumption
↓
Deactivate meter
↓
Replay

DoS

- Presence detector



Planning



Questions ?