Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

PEN-testing and security about embedded devices

Mid-term presentation

Rémi Heredero

Tuesday the 2nd of July 2024

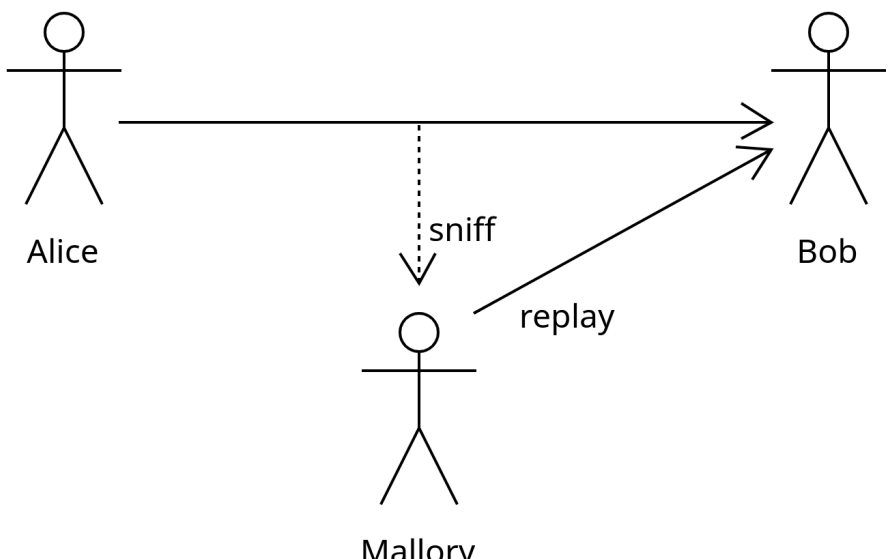
This thesis

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

Attacks

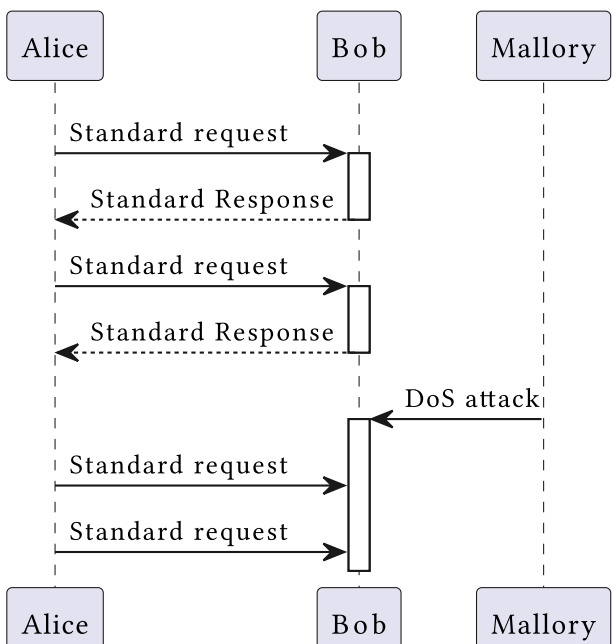
Replay

- On wireless
- On physical layer



Denial of Service (DoS)

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

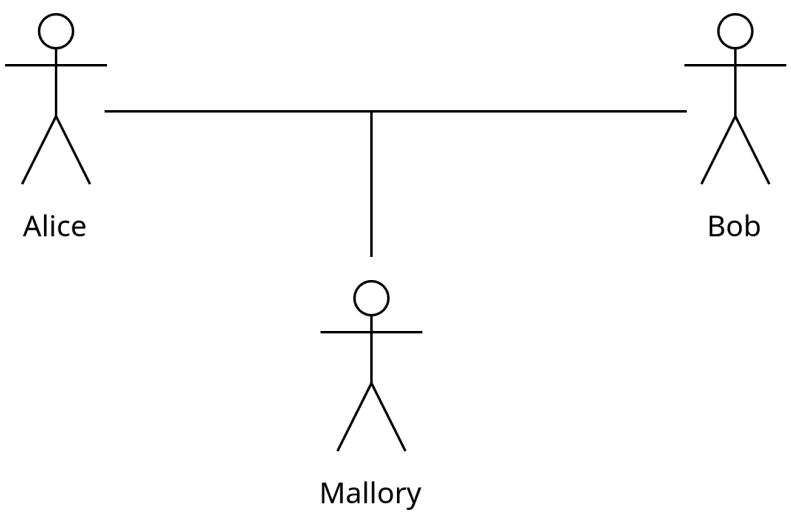


Man in the Middle (MitM)

- Intercept, modified or inject
- 2 phases

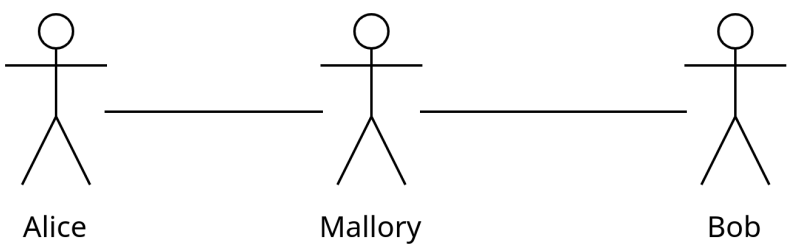
MitM - connected

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



MitM - full interception

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



Simulation environment

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

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

Communication media

Modbus

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

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

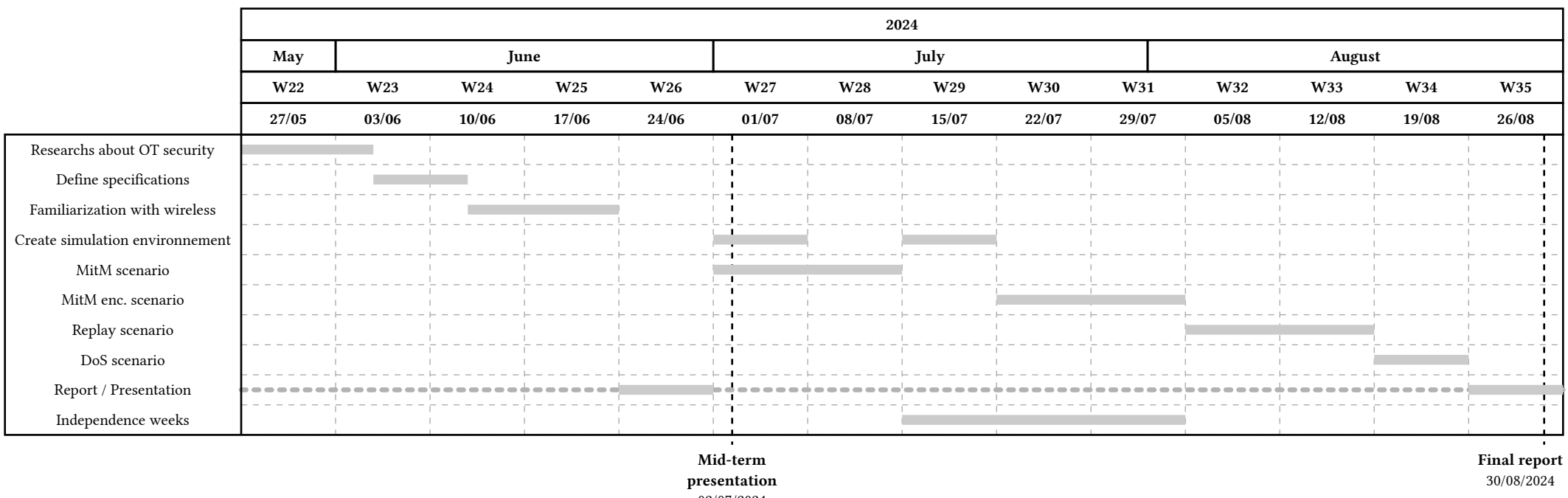
↓

Replay

DoS

- Presence detector

Planning


2024
May
June
July
August
W22
W23
W24
W25
W26
W27
W28
W29
W30
W31
W32
W33
W34
W35
27/05
03/06
10/06
17/06
24/06
01/07
08/07
15/07
22/07
29/07
05/08
12/08
19/08
26/08
Researchs about OT security
Define specifications
Familiarization with wireless
Create simulation environnement
MitM scenario
MitM enc. scenario
Replay scenario
DoS scenario
Report / Presentation
Independence weeks
Mid-term presentation
02/07/2024
Final report
30/08/2024