Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

Presentation and choice of attack scenarios

Rémi Heredero

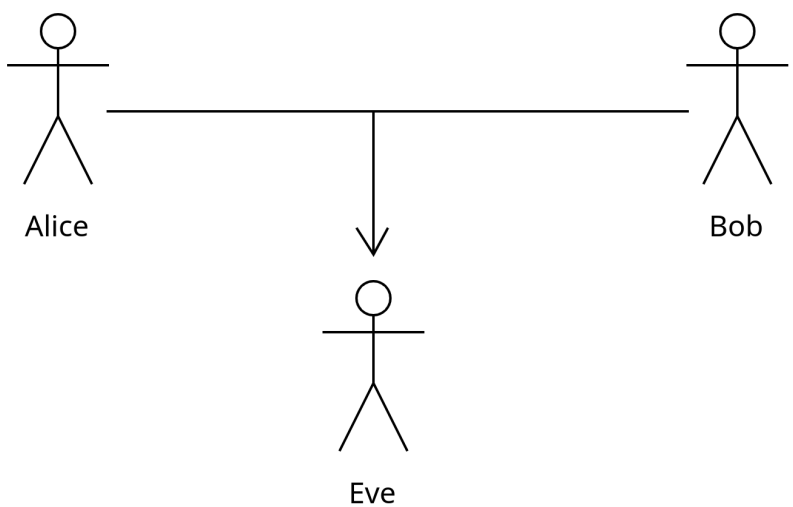
Monday, 3rd of June 2024

OT attacks

Sniffing

- Intercept packets and analyze them
- For other attacks or industrial spying
- Wifi usually with password
  - Or assume password is known

SOL : Use encryption like modbus over TLS



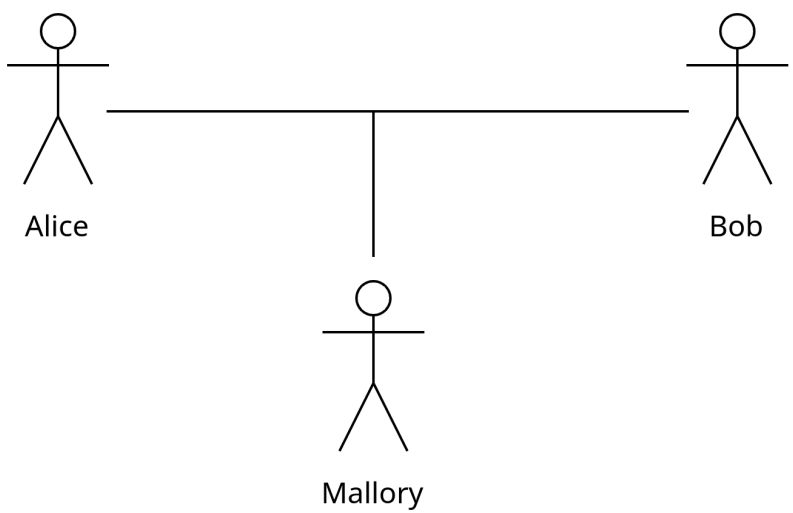
Spoofing

- Create a fake WiFi hotspot
- Easy way for do a get information for succed a MitM
- More IT world

DoS

- Denial of Service
- Spam or Ping of Death
- DDoS more IT world

SOL : Ban IP by the transport layer (or lower)

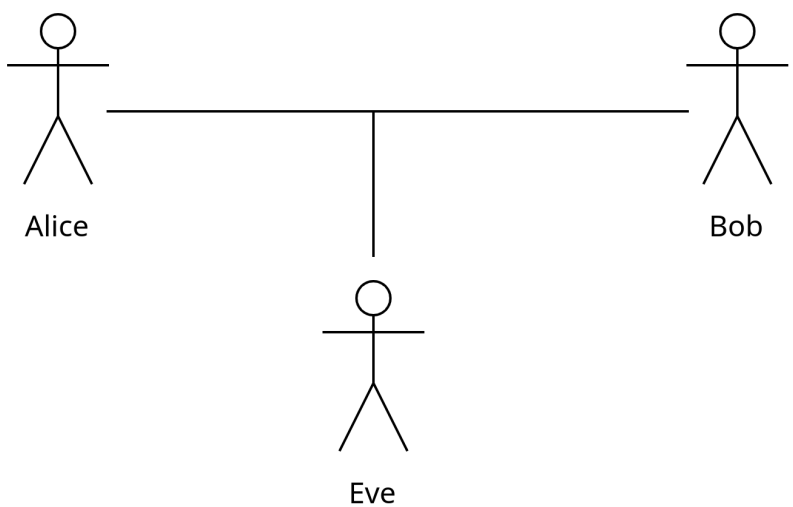


Replay attack

- Replay a packet
- Need sniffing
- Understand or not the packet

SOL : Add a signed timestamp

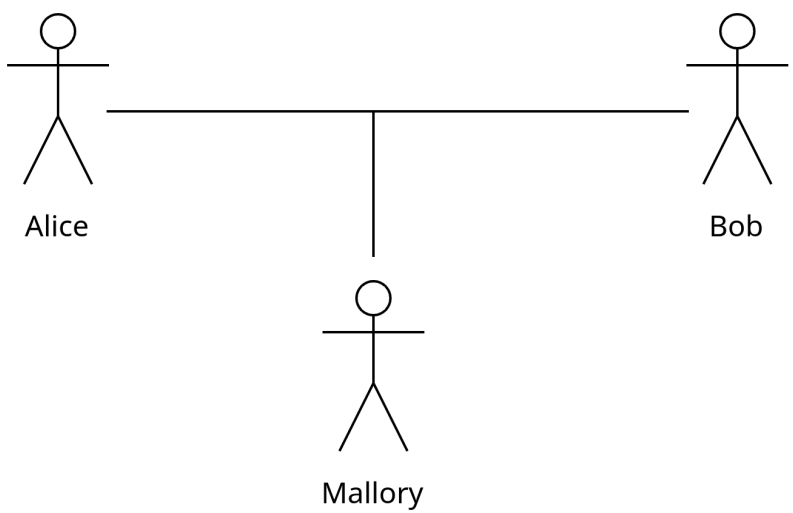
SOL : Rolling code



Man in the middle - Connected

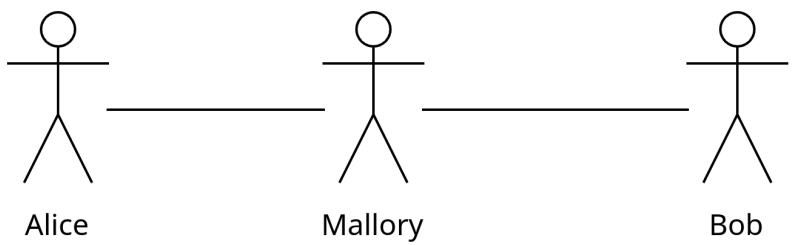
- Send custom packets
- Better with sniffing

SOL : Use encryption with symetric key. Keys exchange with Diffie-Hellman



Man in the middle - Full interception

- Send custom packets
- Intercept everything
- Better with sniffing



SOL : Use encryption like modbus over TLS

Attack scenarios

- DoS by external sensor (external temp by example)
- Wireless Replay attack (433-868 MHz)
- Man in the middle on Modbus over TCP
- Man in the middle on Modbus over TCP with standard encryption

Simulation environnement

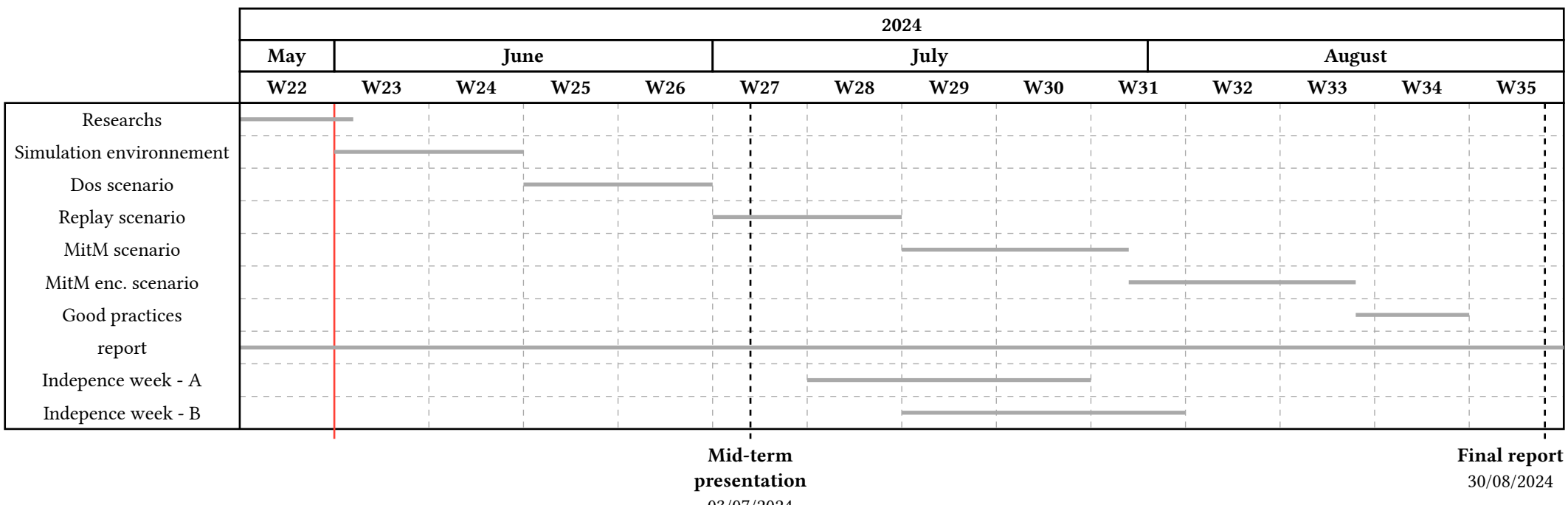
Factory I/O

- Simulation of a factory
- Realistic
- No integreted security

Minecraft

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

Planning


2024
May
June
July
August
W22
W23
W24
W25
W26
W27
W28
W29
W30
W31
W32
W33
W34
W35
Researchs
Simulation environnement
Dos scenario
Replay scenario
MitM scenario
MitM enc. scenario
Good practices
report
Indepence week - A
Indepence week - B
Mid-term presentation
03/07/2024
Final report
30/08/2024