Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

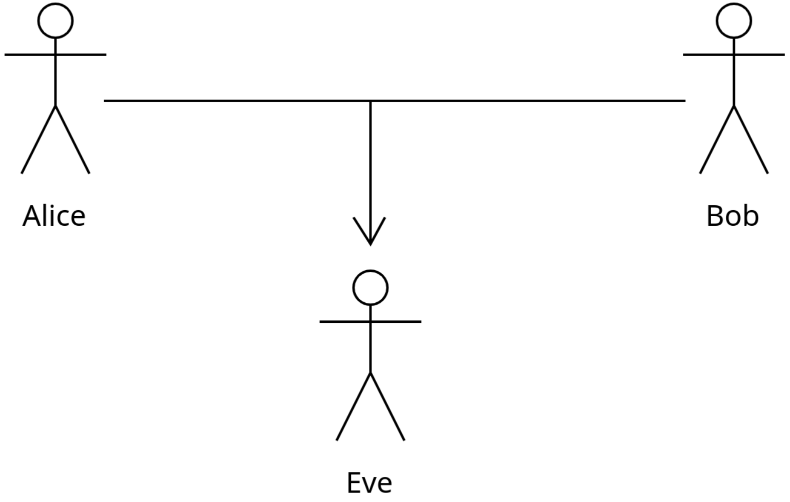
Presentation and choice of attack scenarios

Rémi Heredero

Monday, 3rd of June 2024

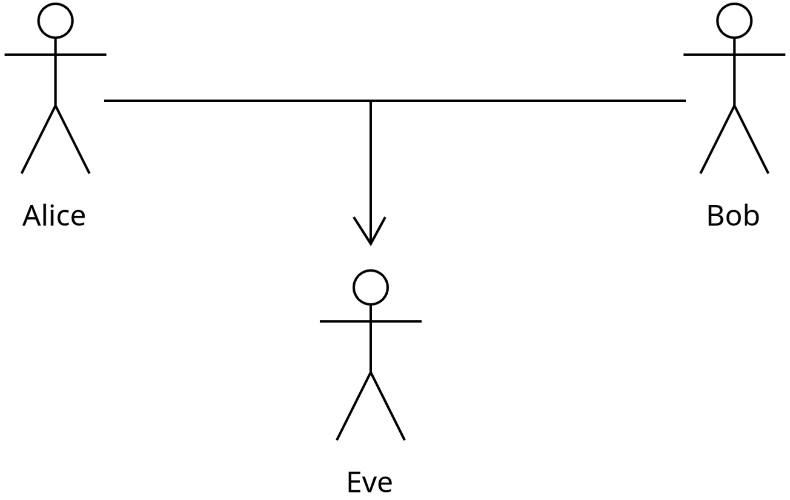
Sniffing

- Intercept packets and analyze them



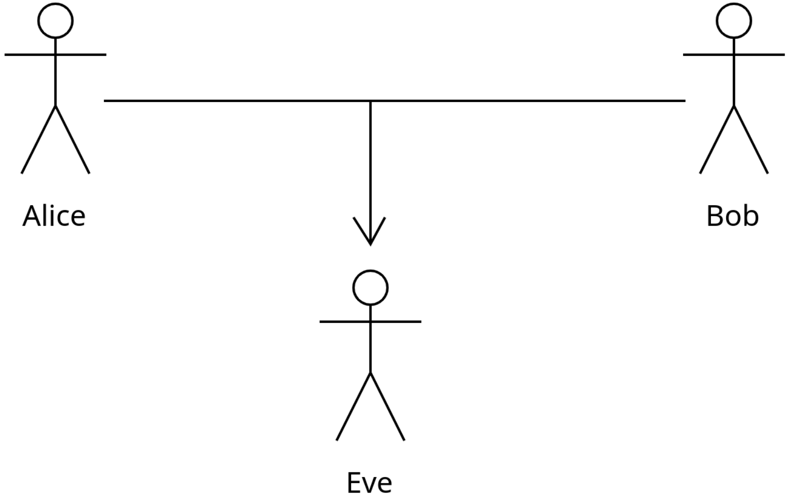
Sniffing

- Intercept packets and analyze them
- For other attacks or industrial spying



Sniffing

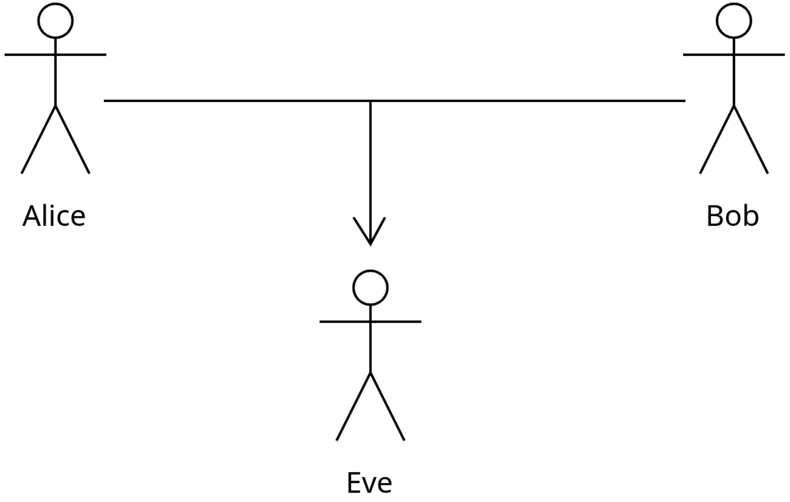
- Intercept packets and analyze them
- For other attacks or industrial spying
- Wifi usually with password
  - Or assume password is known



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

Spoofing

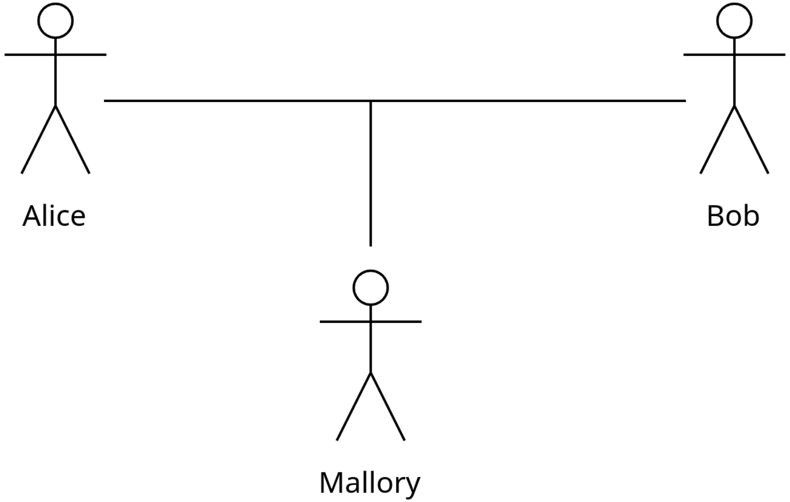
- Create a fake WiFi hotspot
- Easy way for do a get information for succed a MitM

Spoofing

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

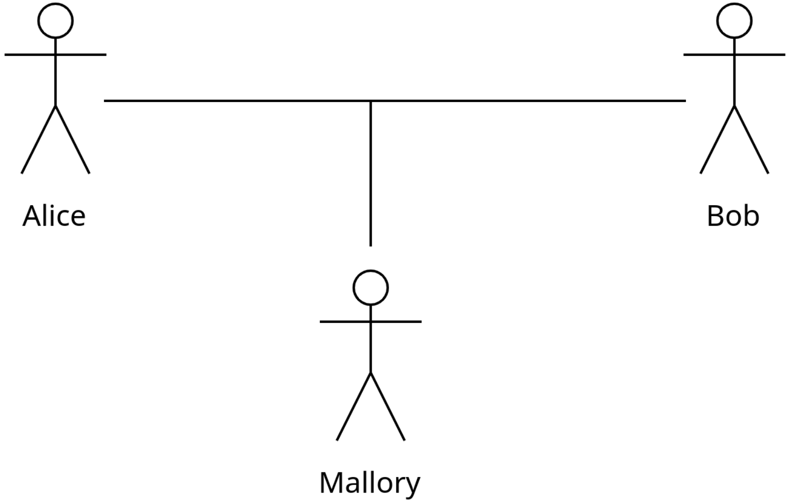
DoS

- Denial of Service



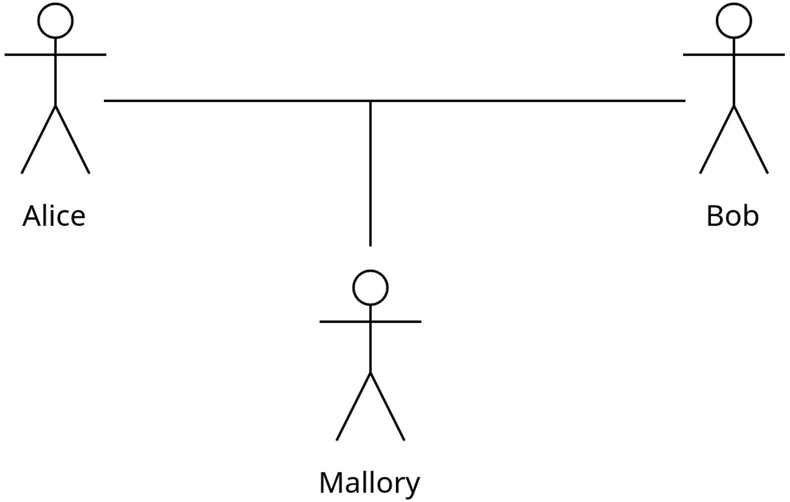
DoS

- Denial of Service
- Spam or Ping of Death



DoS

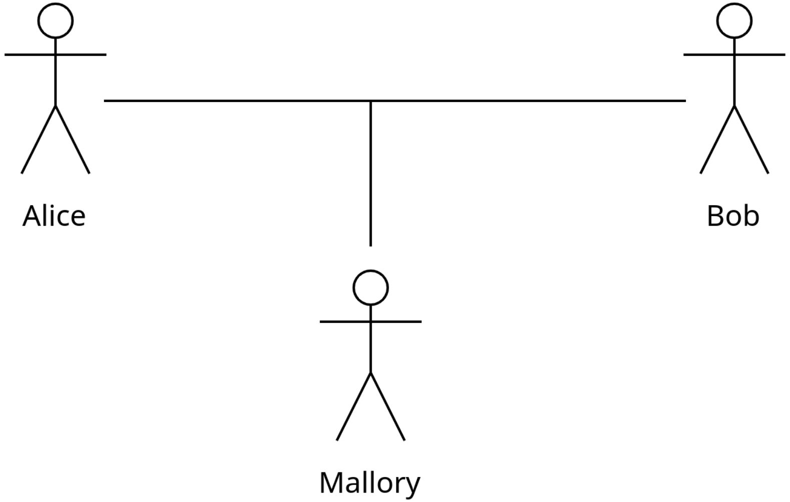
- Denial of Service
- Spam or Ping of Death
- DDoS more IT world



DoS

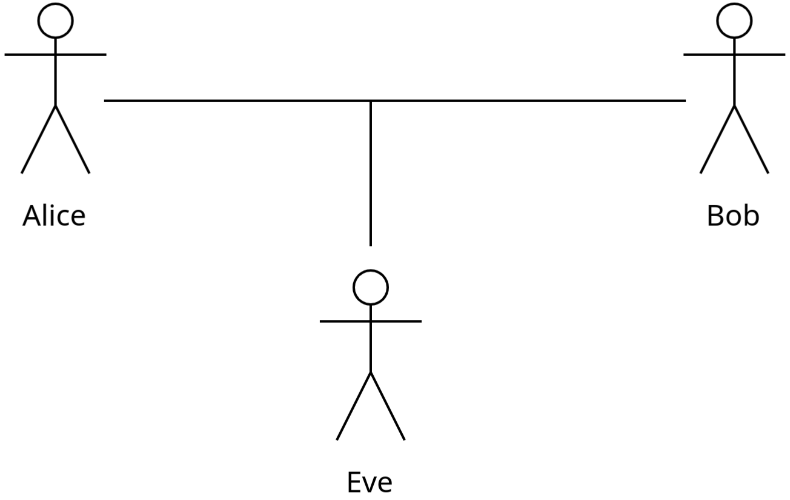
- Denial of Service
- Spam or Ping of Death
- DDoS more IT world

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



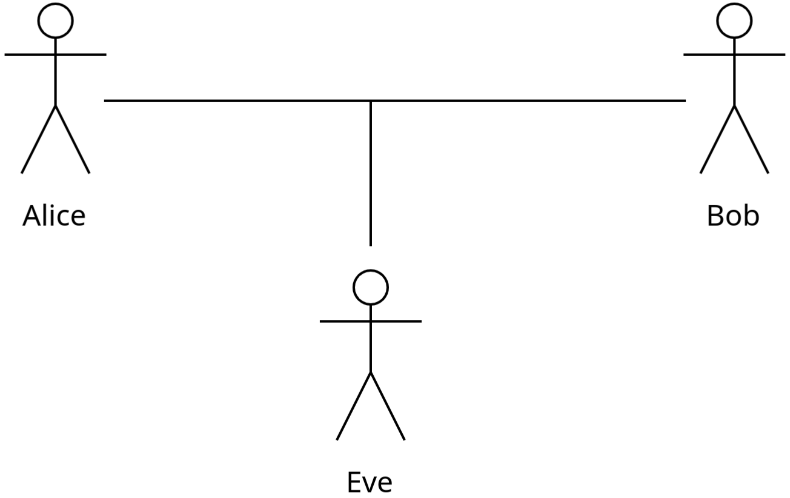
Replay attack

- Replay a packet



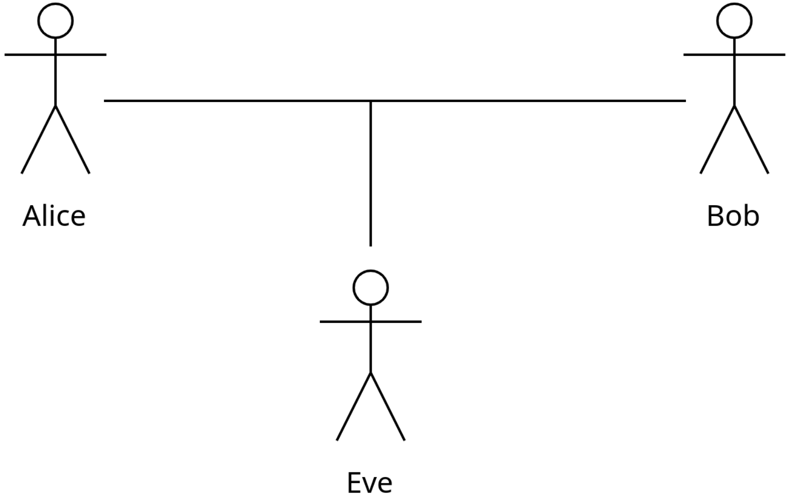
Replay attack

- Replay a packet
- Need sniffing



Replay attack

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

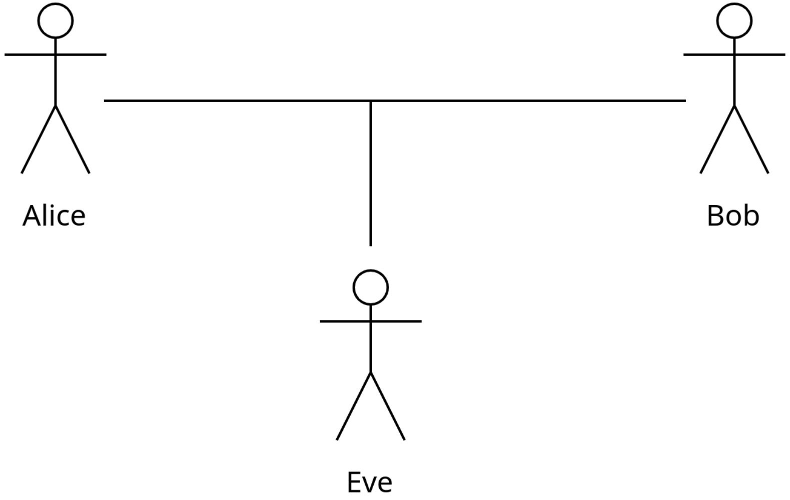


Replay attack

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

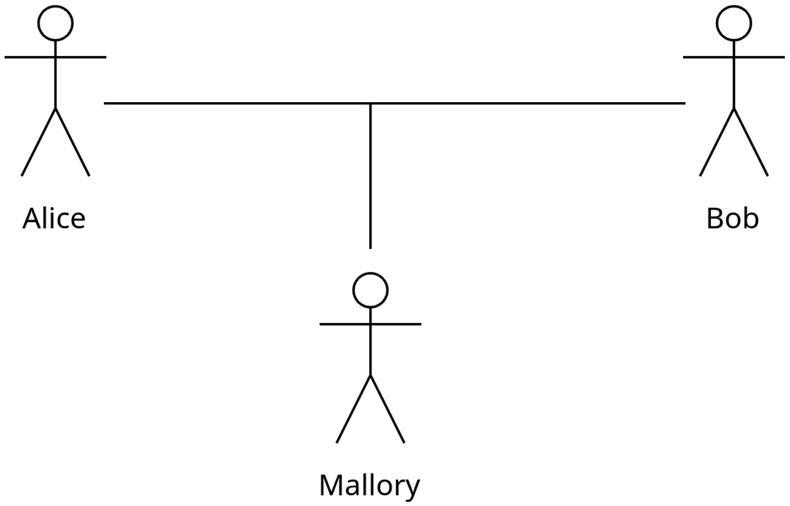
SOL : Add a signed timestamp

SOL : Rolling code



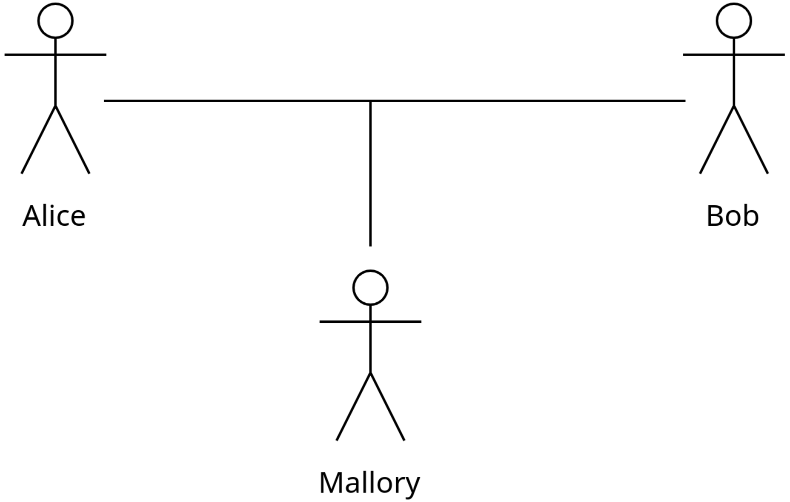
Man in the middle - Connected

- Send custom packets



Man in the middle - Connected

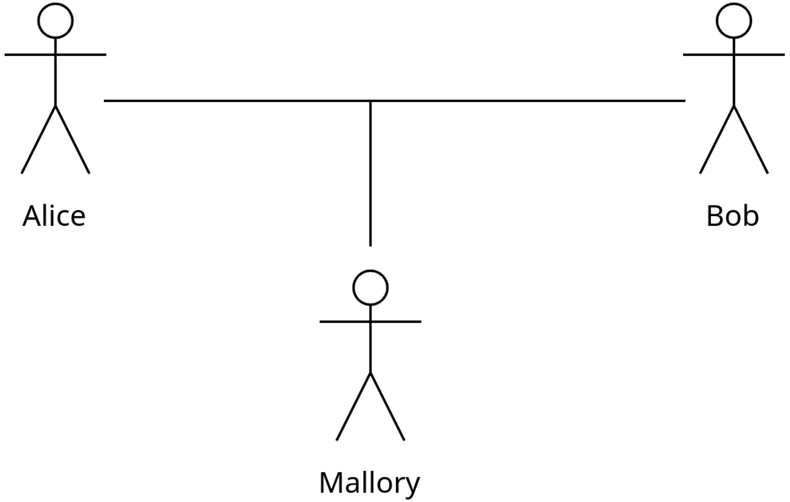
- Send custom packets
- Better with sniffing



Man in the middle - Connected

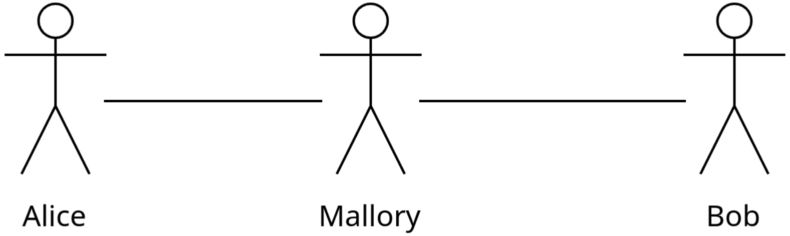
- Send custom packets
- Better with sniffing

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



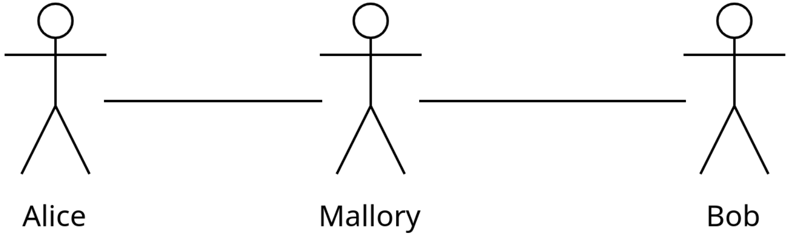
Man in the middle - Full interception

- Send custom packets



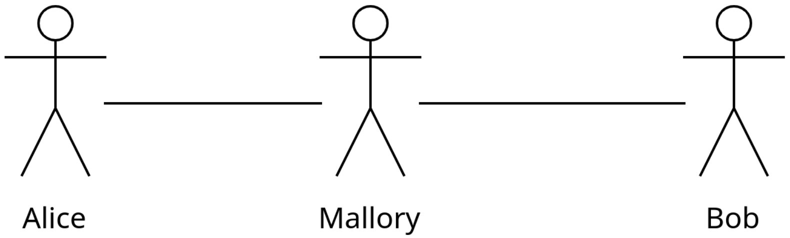
Man in the middle - Full interception

- Send custom packets
- Intercept everything



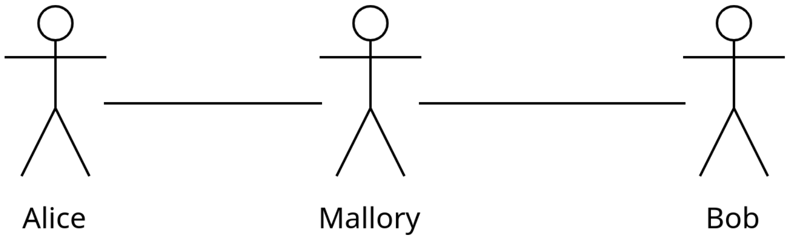
Man in the middle - Full interception

- Send custom packets
- Intercept everything
- Better with sniffing



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)

Attack scenarios

- DoS by external sensor (external temp by example)
- Wireless Replay attack (868 MHz)

Attack scenarios

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

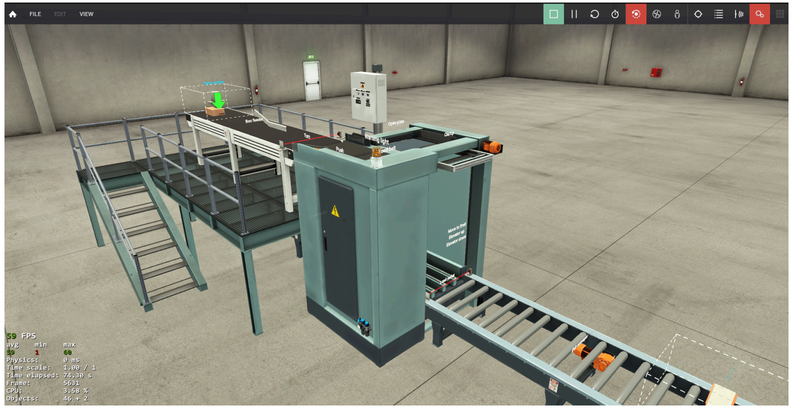
Attack scenarios

- DoS by external sensor (external temp by example)
- Wireless Replay attack (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
- Some scenes already prepared



```
59 FPS
avg     min     max
59      1       60
Physics:        0 ms
Time scale:     1.00 / 1
Time elapsed:   74.30 s
Frame:          5631
CPU:            3.58 %
Objects:        46 + 2
```

Minecraft

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