Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

PEN-testing and security about embedded devices

Rémi Heredero

Tuesday the 10th of September 2024

What's OT Security

What's OT Security

OT vs IT

What's OT Security

OT vs IT

- Information Technology (IT)

What's OT Security

OT vs IT

- Information Technology (IT)
- Operational Technology (OT)

What's OT Security

OT vs IT

- Information Technology (IT)
- Operational Technology (OT)
- World of embedded systems

What's OT Security

OT vs IT

- Information Technology (IT)
- Operational Technology (OT)
- World of embedded systems

Security

What's OT Security

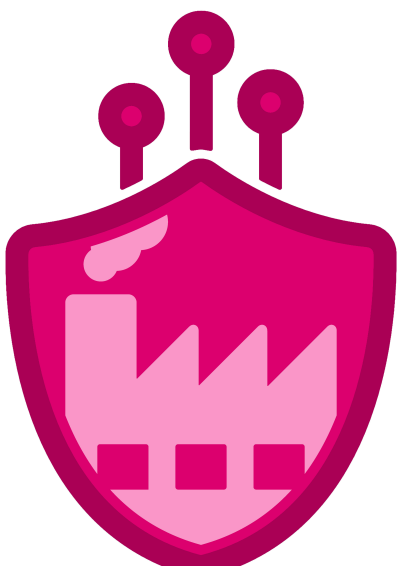
OT vs IT

- Information Technology (IT)
- Operational Technology (OT)
- World of embedded systems

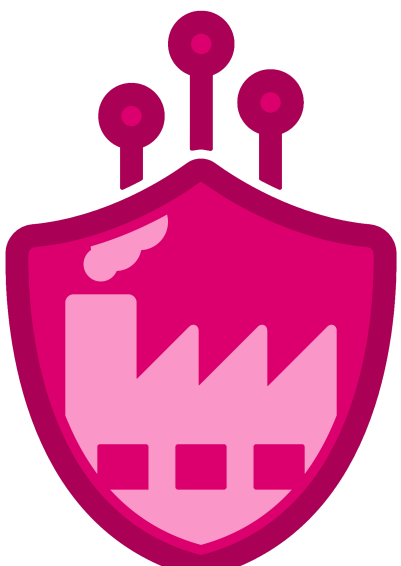
Security

- Before: IT world
- Before: IT world

This thesis

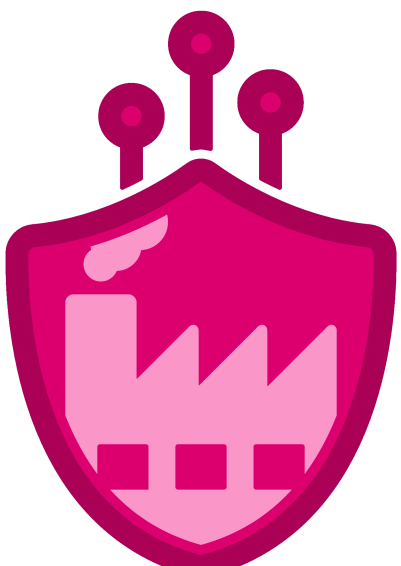


This thesis



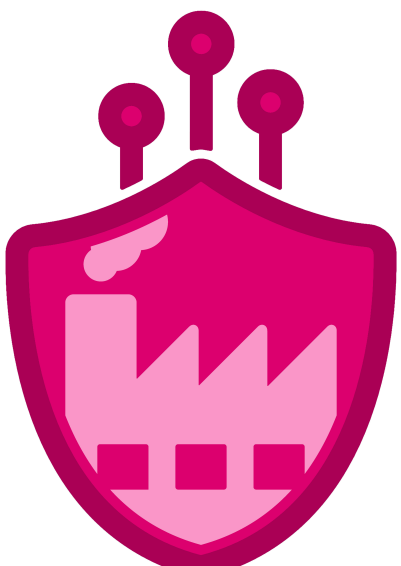
- Labo OT Security - I6

This thesis



- Labo OT Security - I6
- Securitys scenarios
  - Unsecure situation
  - Attack
  - Safe solution

This thesis



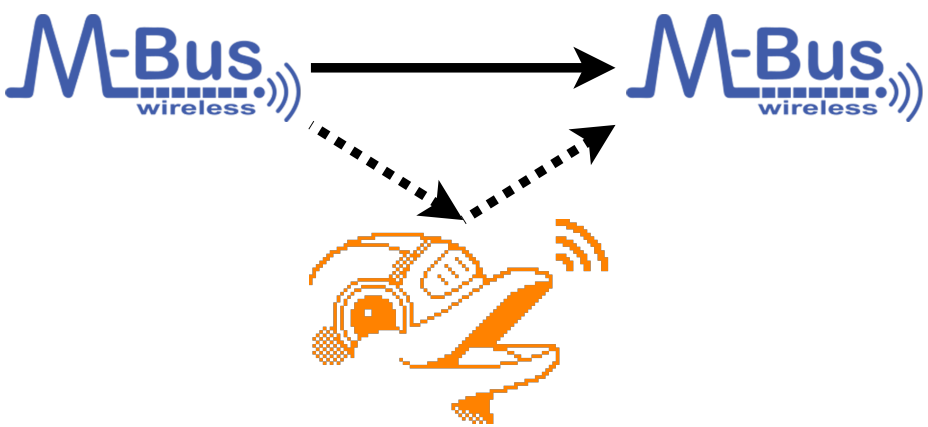
- Labo OT Security - I6
- Securitys scenarios
  - Unsecure situation
  - Attack
  - Safe solution
- Industrial partner training

Replay scenario

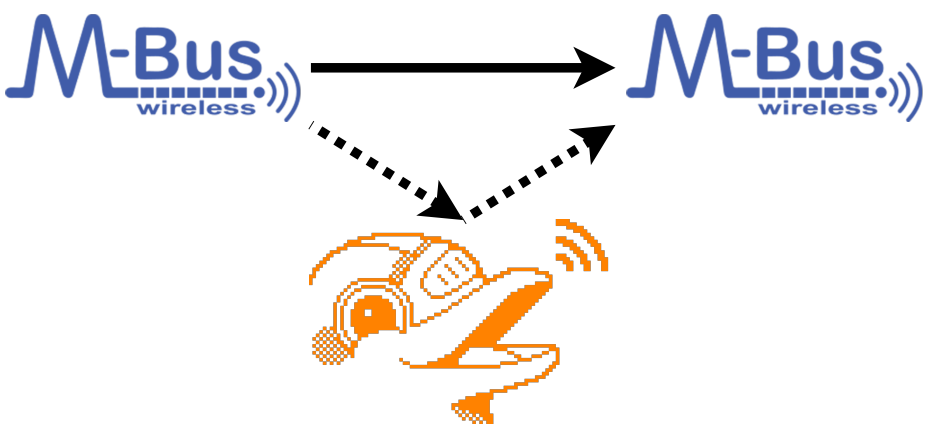
Environnement

Environnement

Environnement



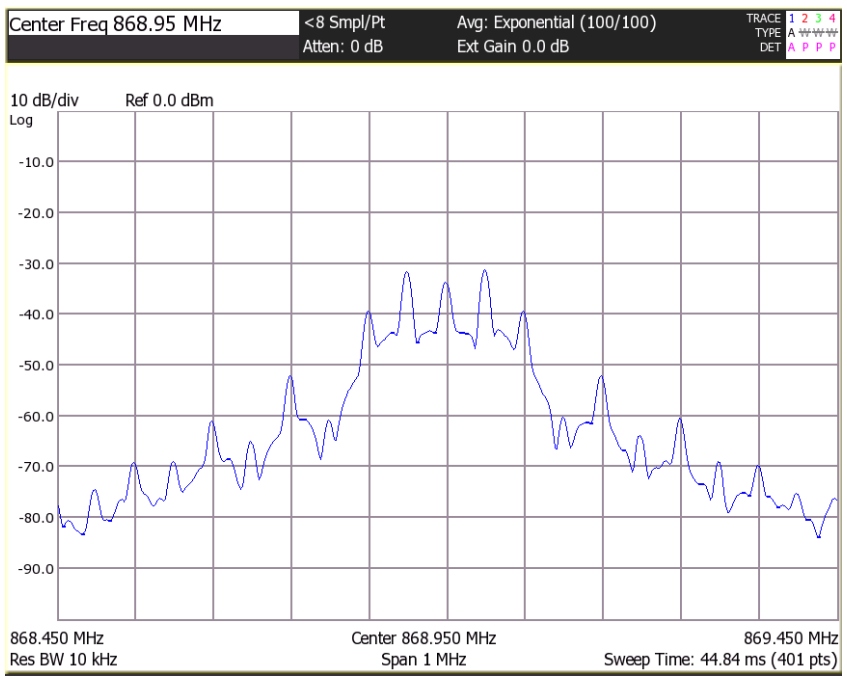
Environnement



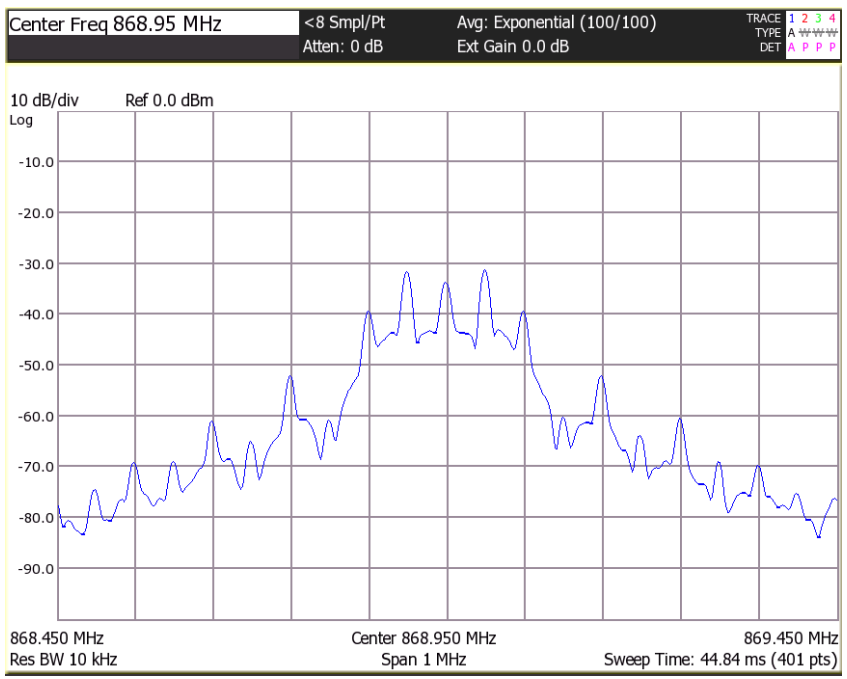
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

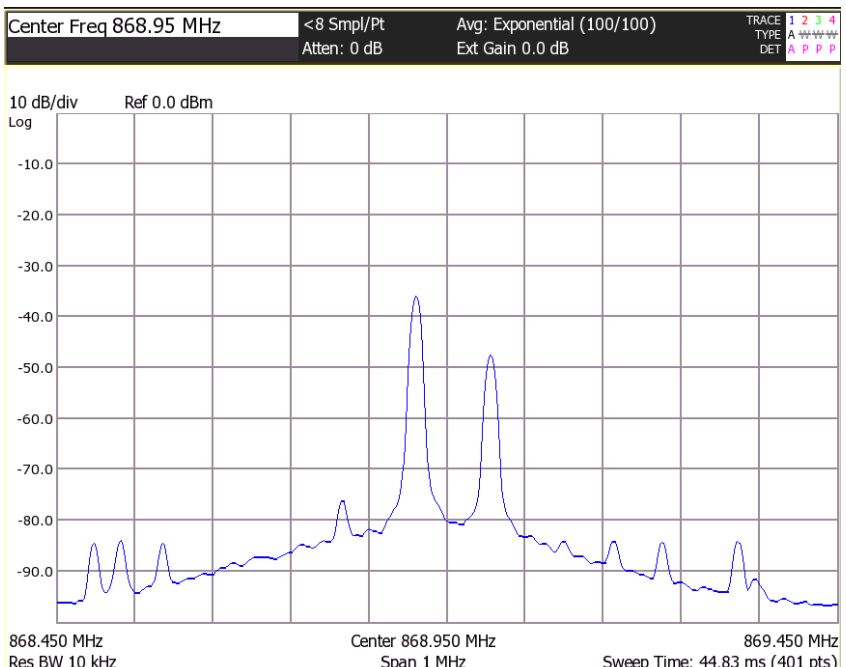
GFSK vs FSK

GFSK vs FSK


Center Freq 868.95 MHz
<8 Smpl/Pt
Atten: 0 dB
Avg: Exponential (100/100)
Ext Gain 0.0 dB
TRACE 1 2 3 4
TYPE A
DET A P P P
10 dB/div
Ref 0.0 dBm
Log
-10.0
-20.0
-30.0
-40.0
-50.0
-60.0
-70.0
-80.0
-90.0
868.450 MHz
Res BW 10 kHz
Center 868.950 MHz
Span 1 MHz
869.450 MHz
Sweep Time: 44.84 ms (401 pts)

GFSK vs FSK


Center Freq 868.95 MHz
<8 Smpl/Pt
Atten: 0 dB
Avg: Exponential (100/100)
Ext Gain 0.0 dB
TRACE 1 2 3 4
TYPE A WWWW
DET A P P P
10 dB/div
Ref 0.0 dBm
Log
-10.0
-20.0
-30.0
-40.0
-50.0
-60.0
-70.0
-80.0
-90.0
868.450 MHz
Res BW 10 kHz
Center 868.950 MHz
Span 1 MHz
869.450 MHz
Sweep Time: 44.84 ms (401 pts)


Center Freq 868.95 MHz
<8 Smpl/Pt
Atten: 0 dB
Avg: Exponential (100/100)
Ext Gain 0.0 dB
TRACE 1 2 3 4
TYPE A WWWW
DET A P P P
10 dB/div
Ref 0.0 dBm
Log
-10.0
-20.0
-30.0
-40.0
-50.0
-60.0
-70.0
-80.0
-90.0
868.450 MHz
Res BW 10 kHz
Center 868.950 MHz
Span 1 MHz
869.450 MHz
Sweep Time: 44.83 ms (401 pts)

Transceiver 433 MHz

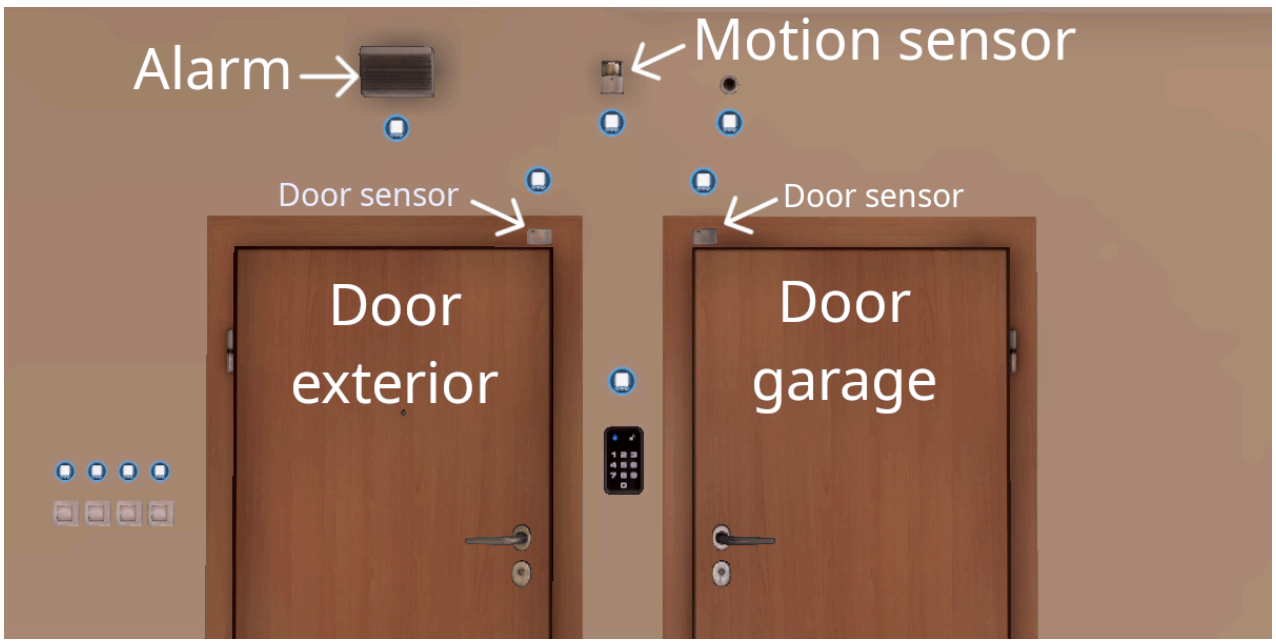
Man in the Middle (MitM) scenario

Home I/O

Home I/O

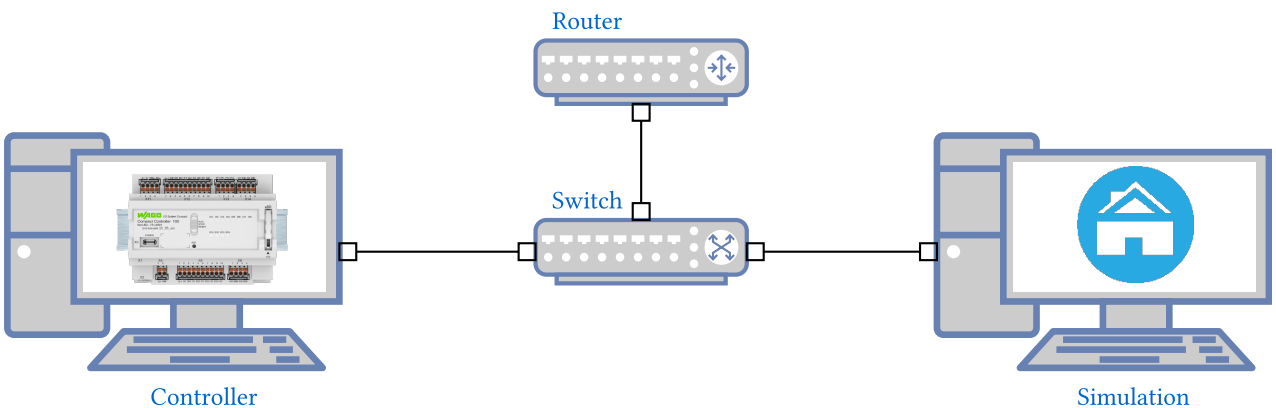

Power 0.000kw
Current Day 0.00 kWh
Last Day 0.00 kWh
Last Week 0.00 kWh
Last Month 0.00 kWh

Home I/O

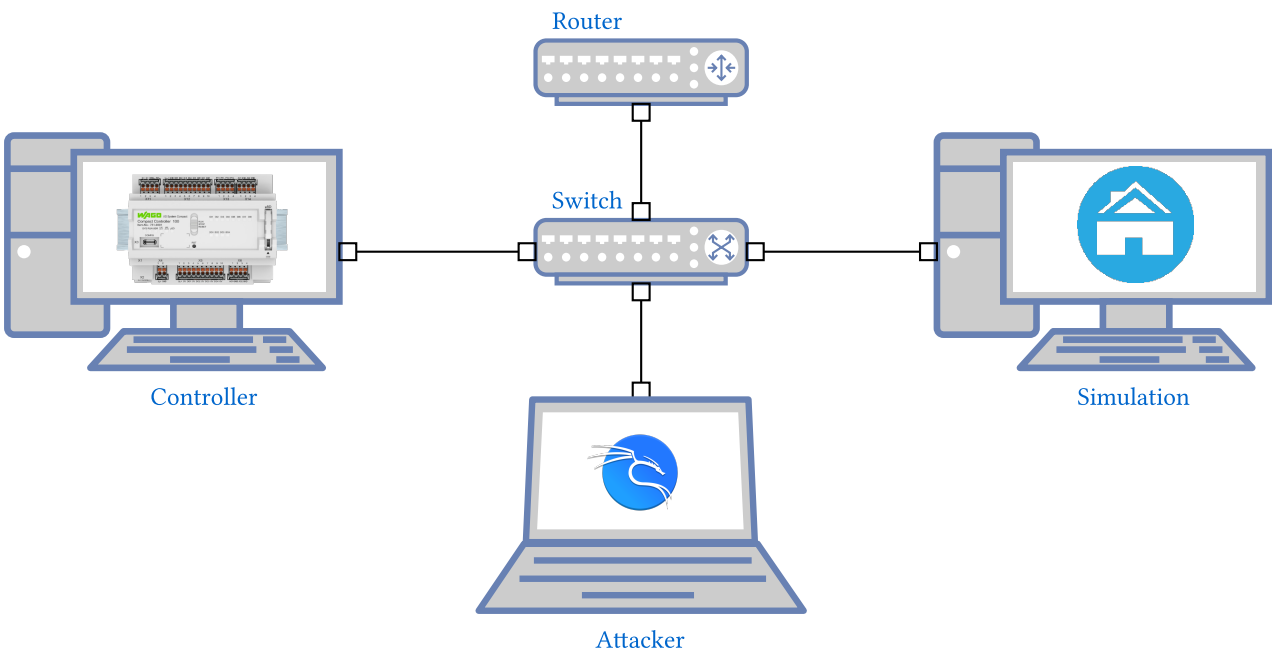

Alarm
Motion sensor
Door sensor
Door sensor
Door exterior
Door garage

Architecture

Architecture

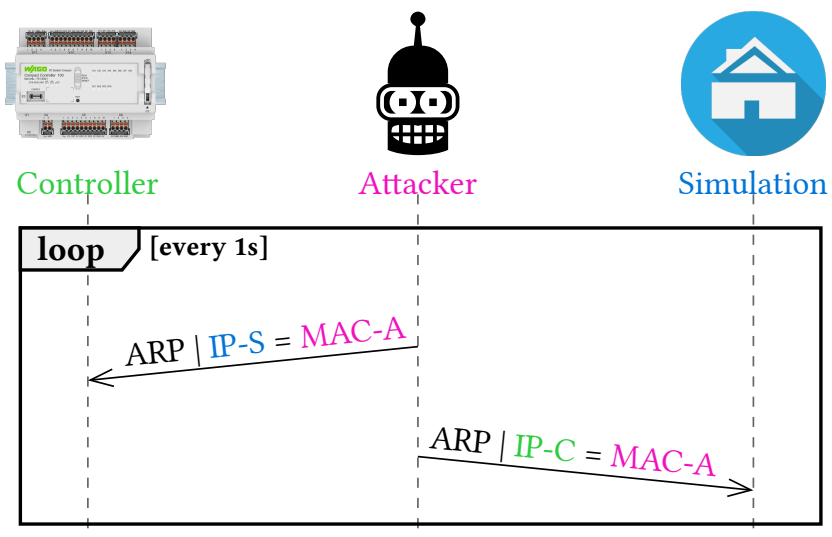


Architecture

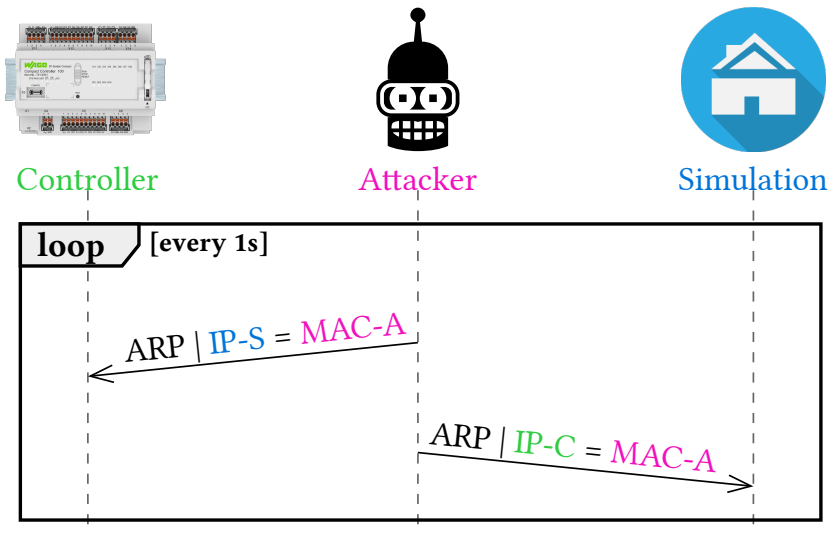


ARP Poisoning

ARP Poisoning



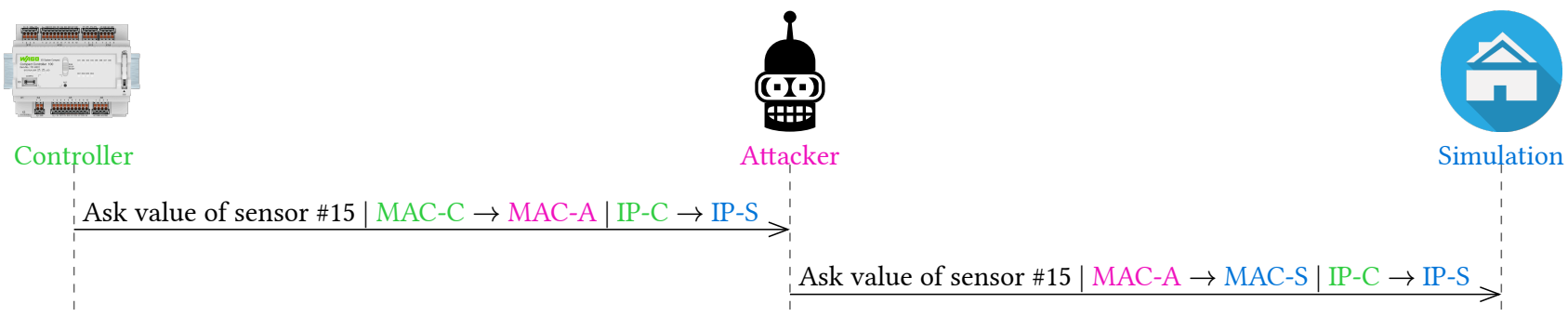
ARP Poisoning



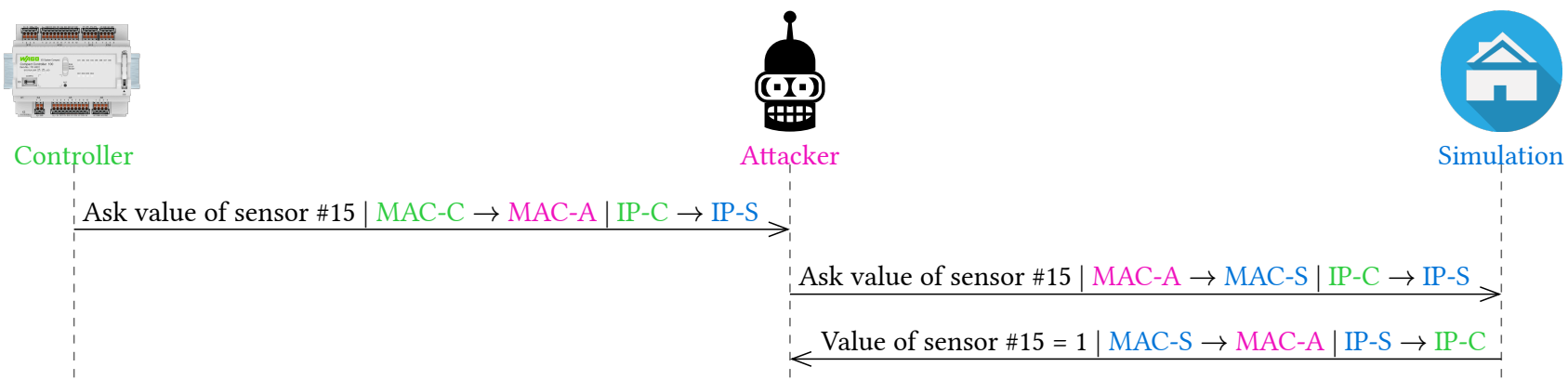
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Attack on Modbus/TCP

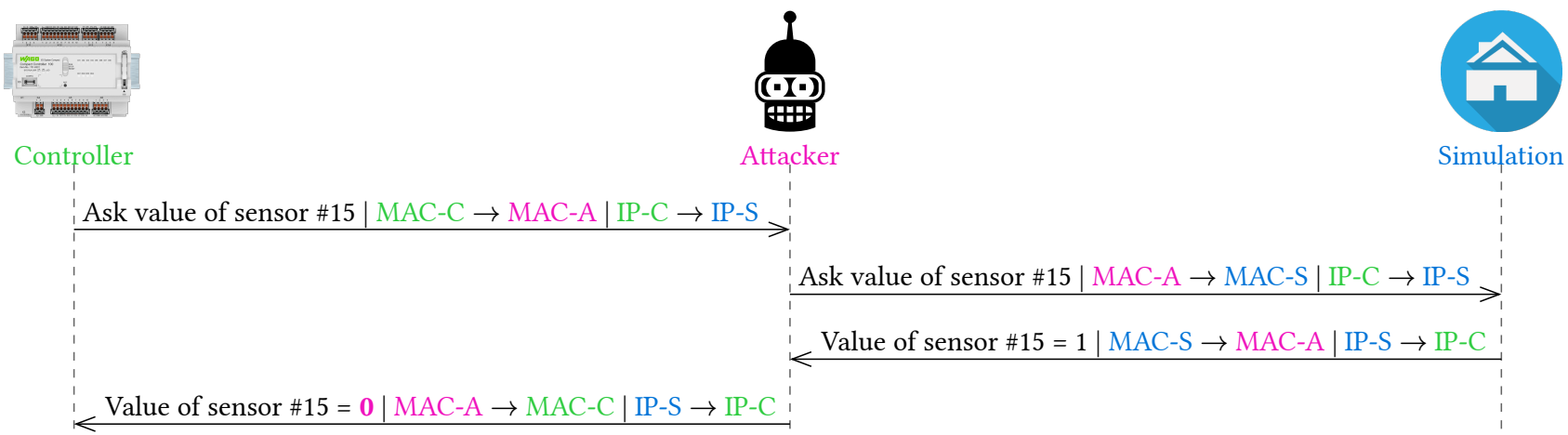
Attack on Modbus/TCP



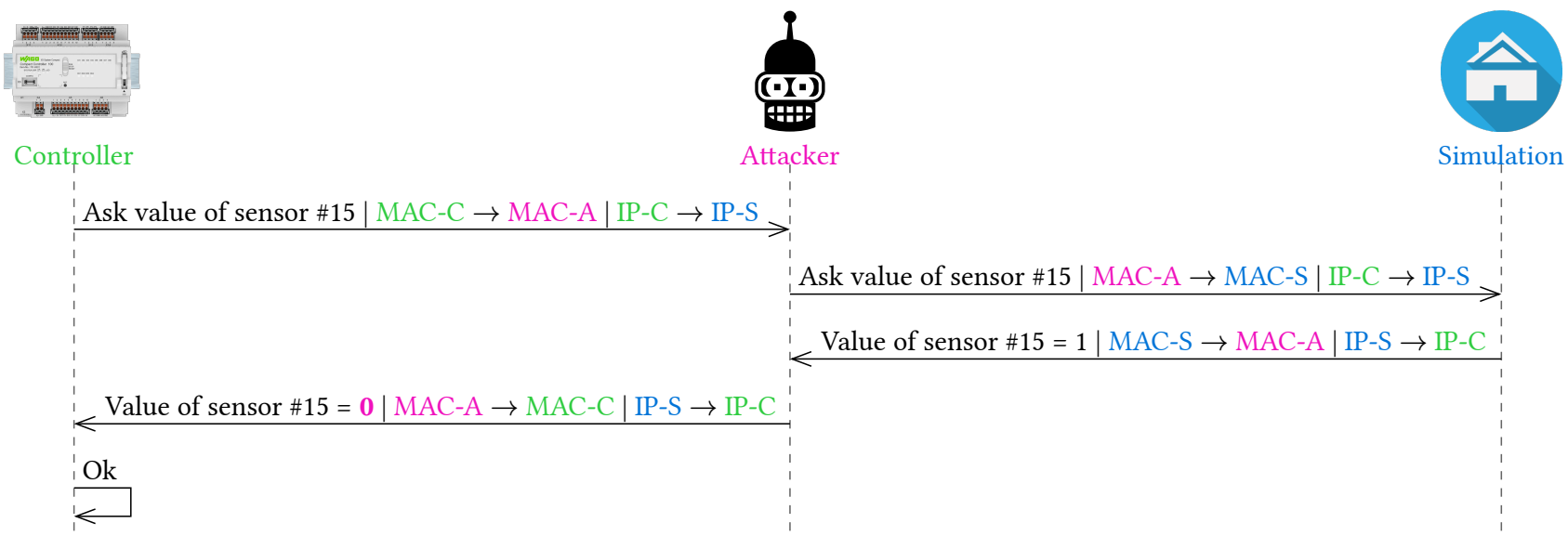
Attack on Modbus/TCP



Attack on Modbus/TCP



Attack on Modbus/TCP



Attack on Modbus/TCP

Summary

Attack on Modbus/TCP

Summary

- On the fly

Attack on Modbus/TCP

Summary

- On the fly
- On TCP layer

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Attack on Modbus/TCP

Summary

- On the fly
- On TCP layer
- No need to decrypt

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

TLS and X.509

TLS and X.509

- Encrypt session

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

TLS and X.509

- Encrypt session

X.509

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

TLS and X.509

- Encrypt session

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

X.509

- Owner
  - Public key

TLS and X.509

- Encrypt session

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

X.509

- Owner
  - Public key
- Certificate authority

TLS and X.509

- Encrypt session

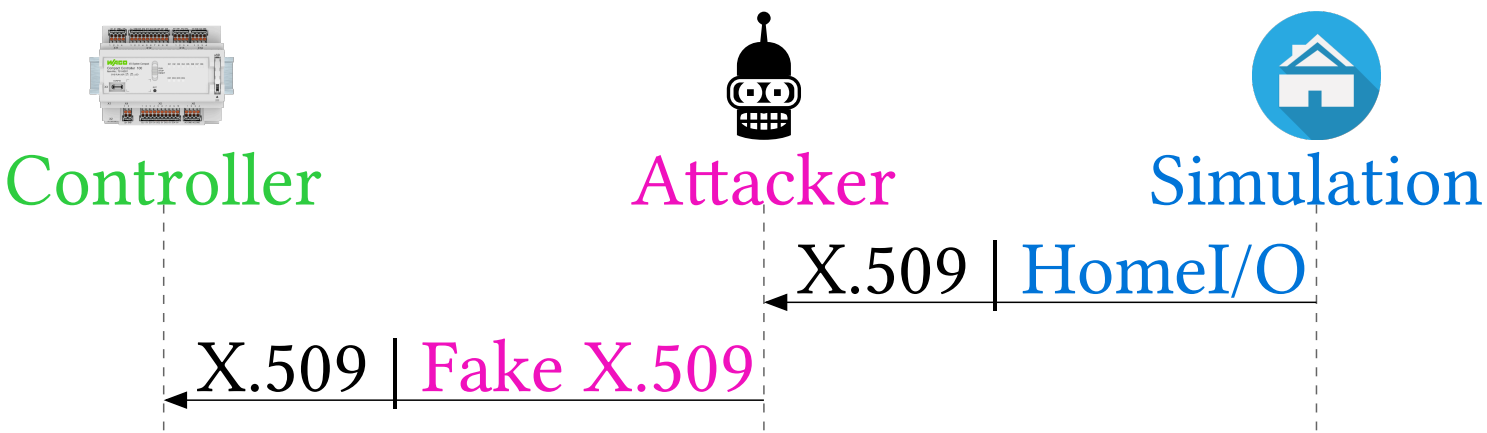
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

X.509

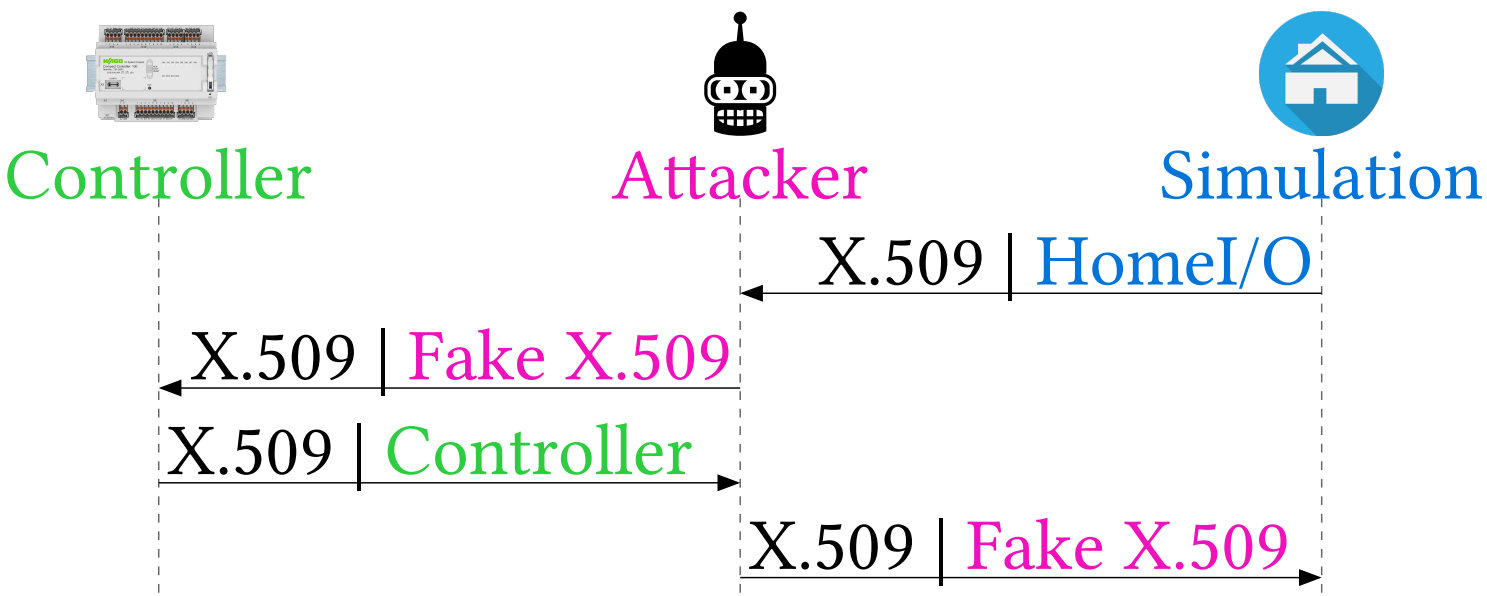
- Owner
  - Public key
- Certificate authority
- Signature

Attack on Modbus/TLS

Attack on Modbus/TLS



Attack on Modbus/TLS



Attack on Modbus/TLS

> The most dangerous code in the world:
> validating SSL certificates in non-browser software
>
> — Martin Georgiev - October 2012

Attack on Modbus/TLS

> The most dangerous code in the world:
> validating SSL certificates in non-browser software
>
> — Martin Georgiev - October 2012

Aapo Oksman prove it still the case **last year**

Attack on Modbus/TLS

> The most dangerous code in the world:
> validating SSL certificates in non-browser software
>
> — Martin Georgiev - October 2012

Aapo Oksman prove it still the case **last year**

Attack on Modbus/TLS

> The most dangerous code in the world:
> validating SSL certificates in non-browser software
>
> — Martin Georgiev - October 2012

Aapo Oksman prove it still the case **last year**

Attack on Modbus/TLS

> The most dangerous code in the world:
> validating SSL certificates in non-browser software
>
> — Martin Georgiev - October 2012

Aapo Oksman prove it still the case **last year**



Questions ?