Hes·so VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

OT Security

PEN-testing and security about embedded devices

Rémi Heredero

Tuesday, September 10 2024

What's OT Security

OT vs IT

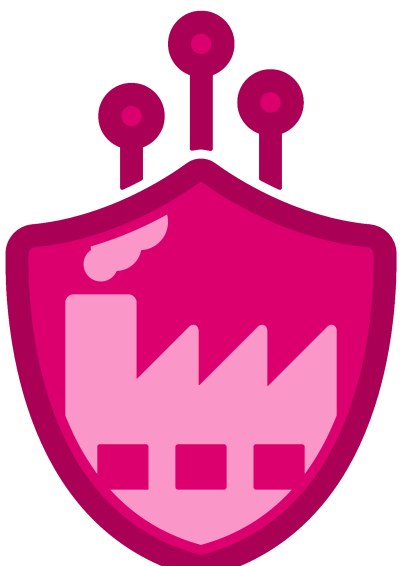
- Information Technology (IT)
  = CPU
- Operational Technology (OT)
  = MCU
- World of embedded systems

Security

- Before: IT wall
- Now: IoT everywhere

$\Rightarrow$ Time to put Security in OT

This thesis



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

Replay scenario

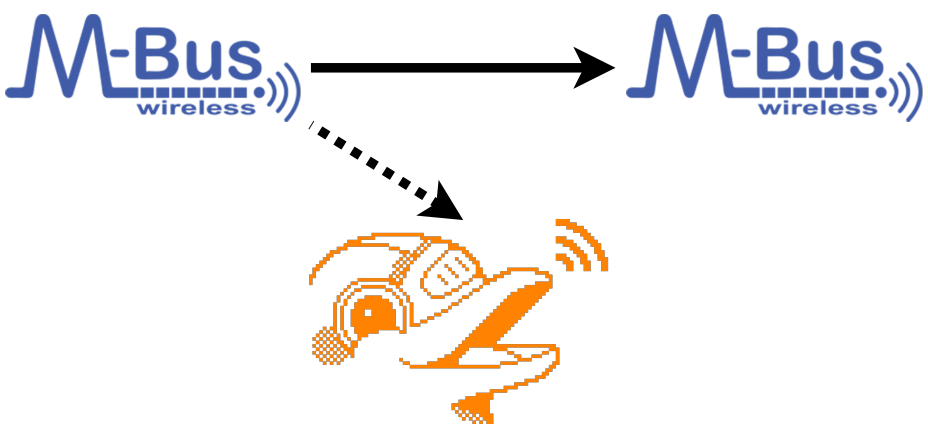
Environment

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

Environment

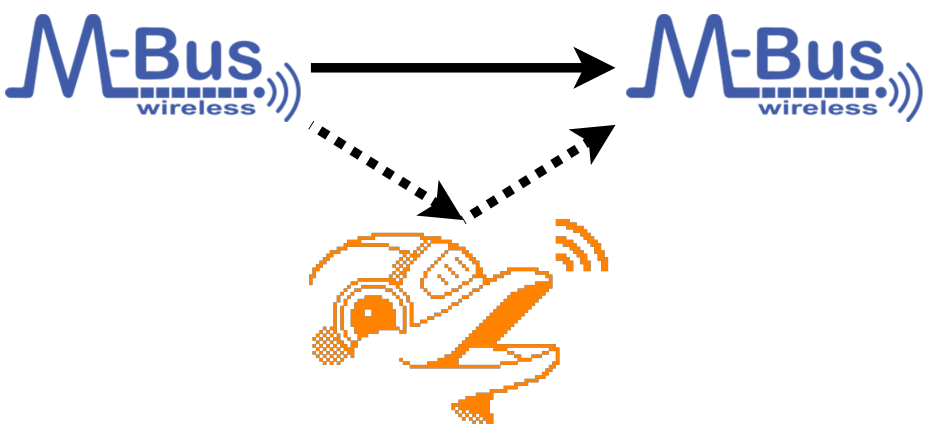
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Environment



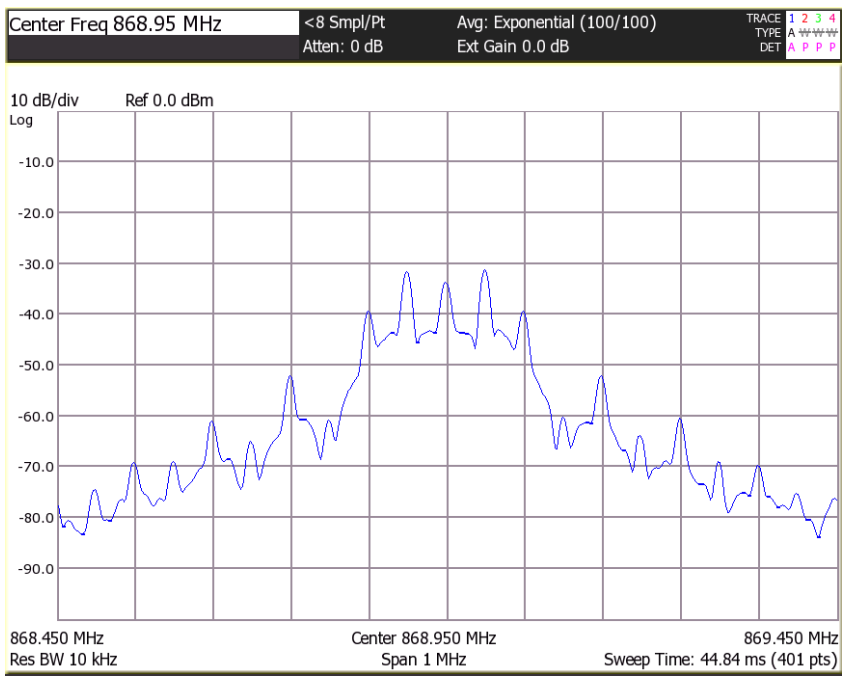
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

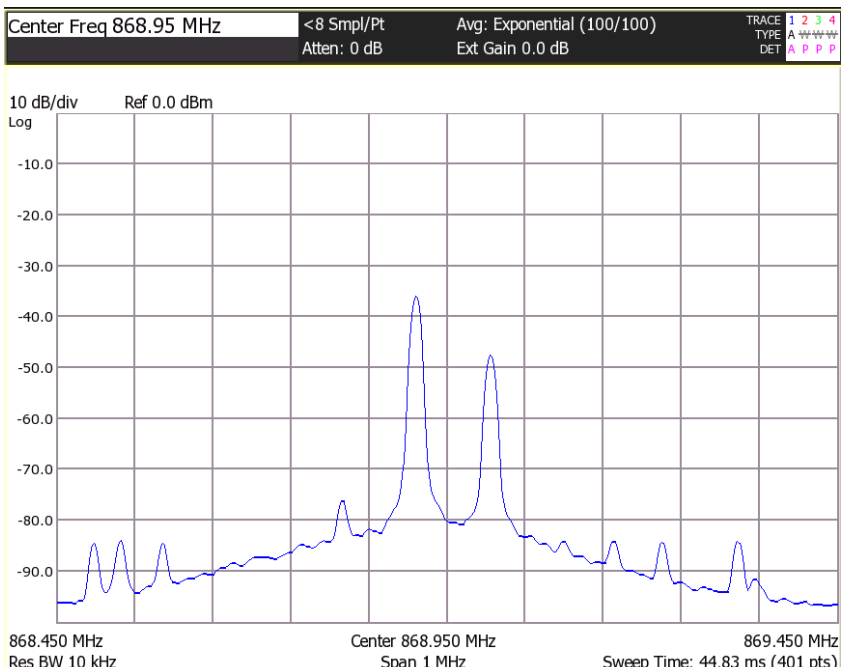
Environment



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

The Flipper modulation





Plan B & Security

Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

Security

- Different messages
- Rolling code
- Signature

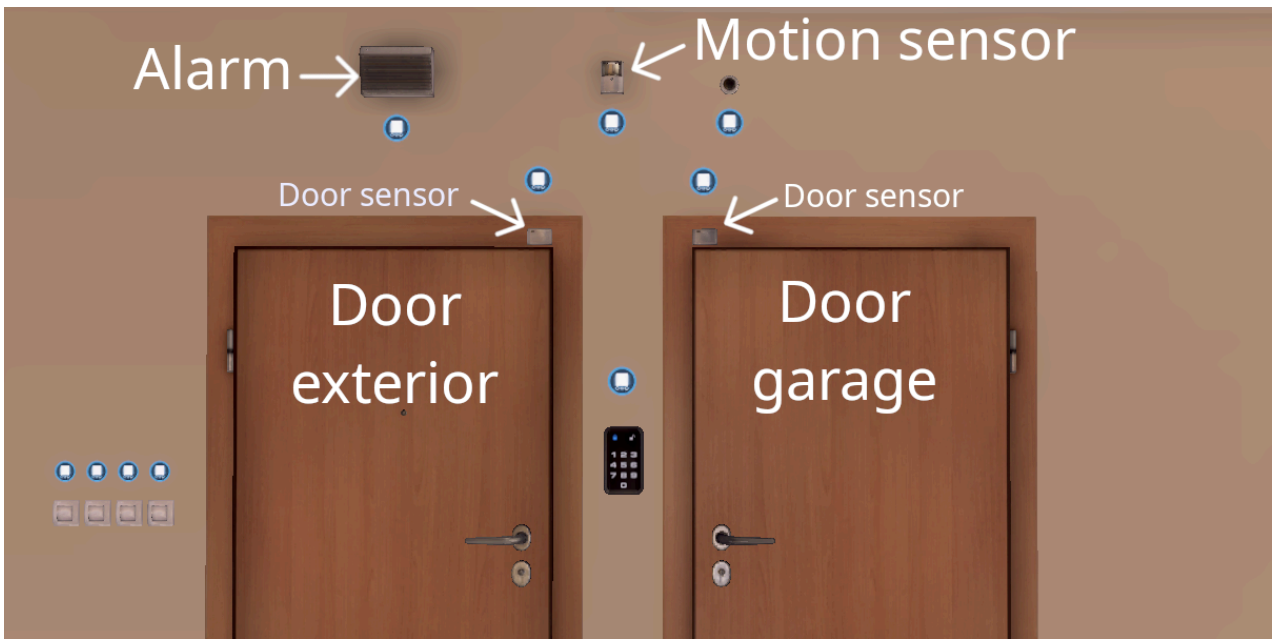
Man in the Middle (MitM) scenario

Home I/O

Home I/O

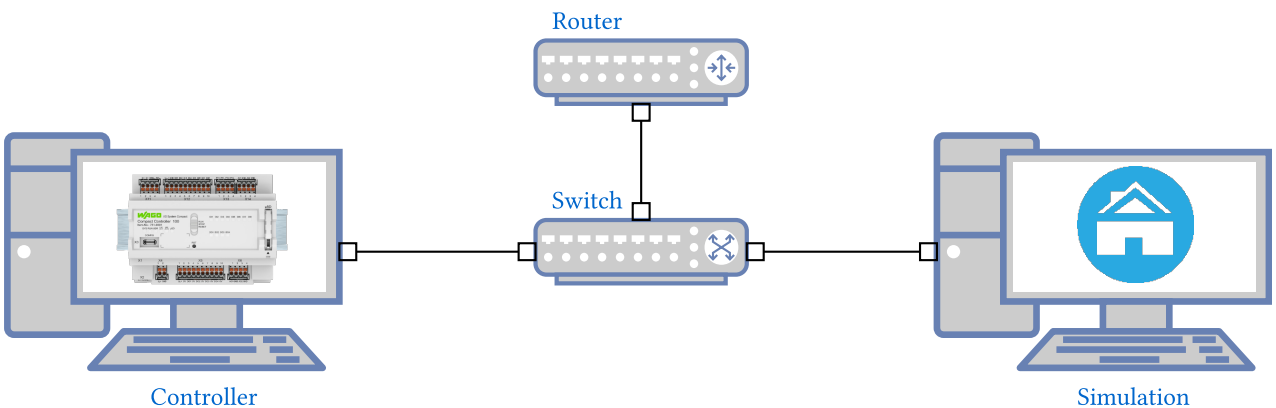

Power 0.000kw
Current Day 0.00 kWh
Last Day 0.00 kWh
Last Week 0.00 kWh
Last Month 0.00 kWh

Home I/O

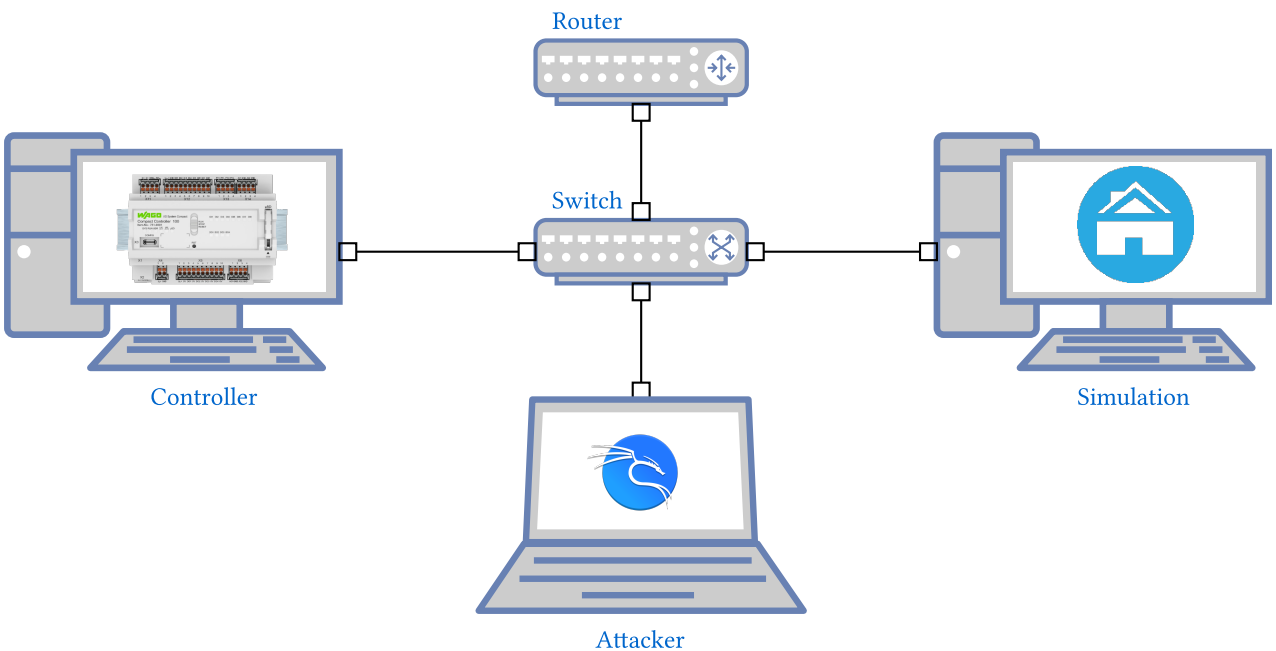

Alarm
Motion sensor
Door sensor
Door sensor
Door exterior
Door garage

Architecture

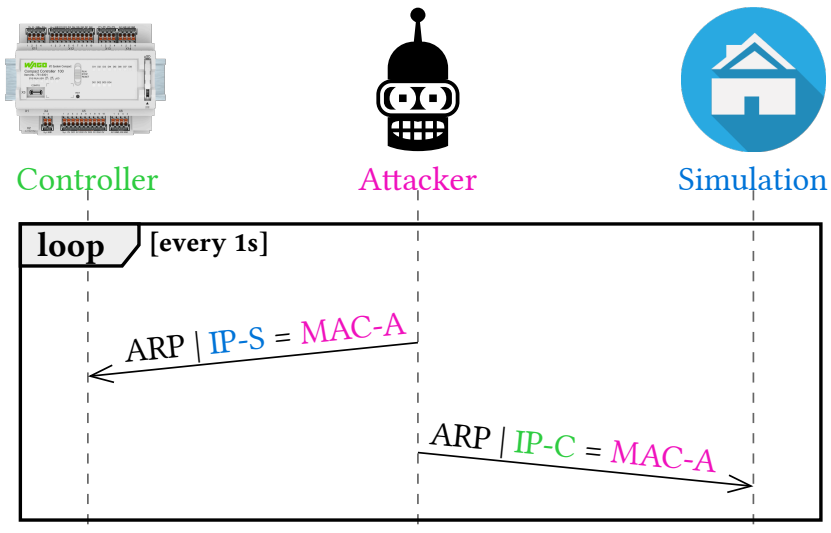
Architecture



Architecture



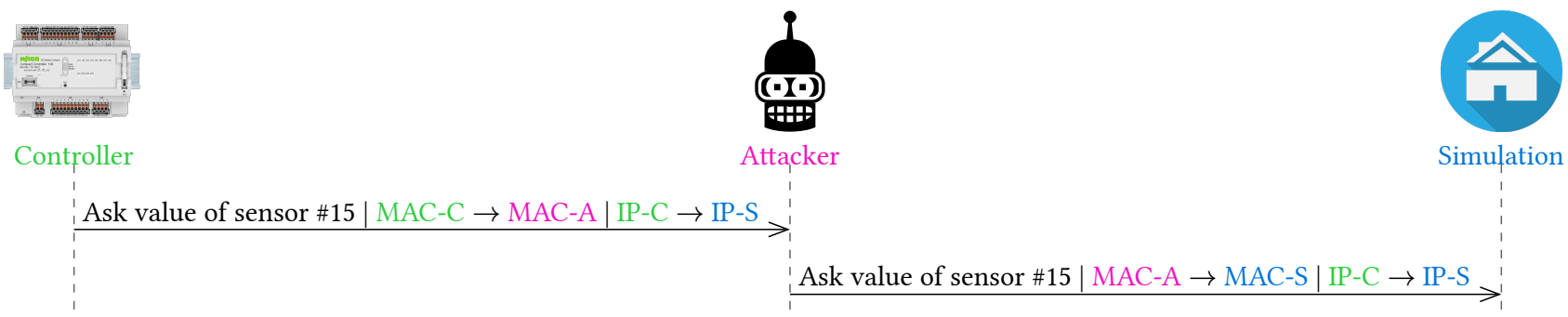
ARP Poisoning



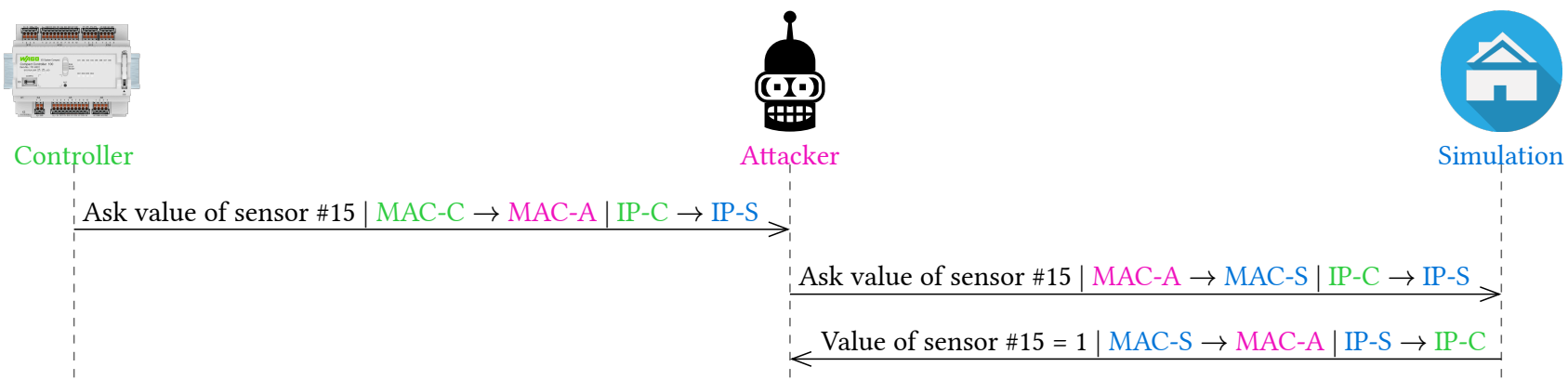
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Attack on Modbus/TCP

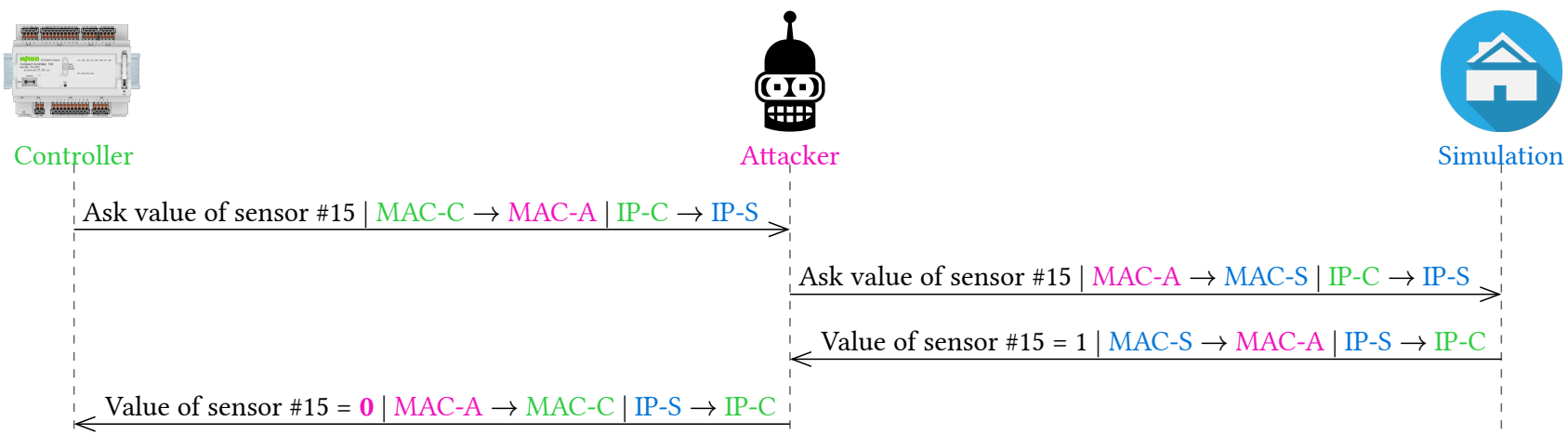
Attack on Modbus/TCP



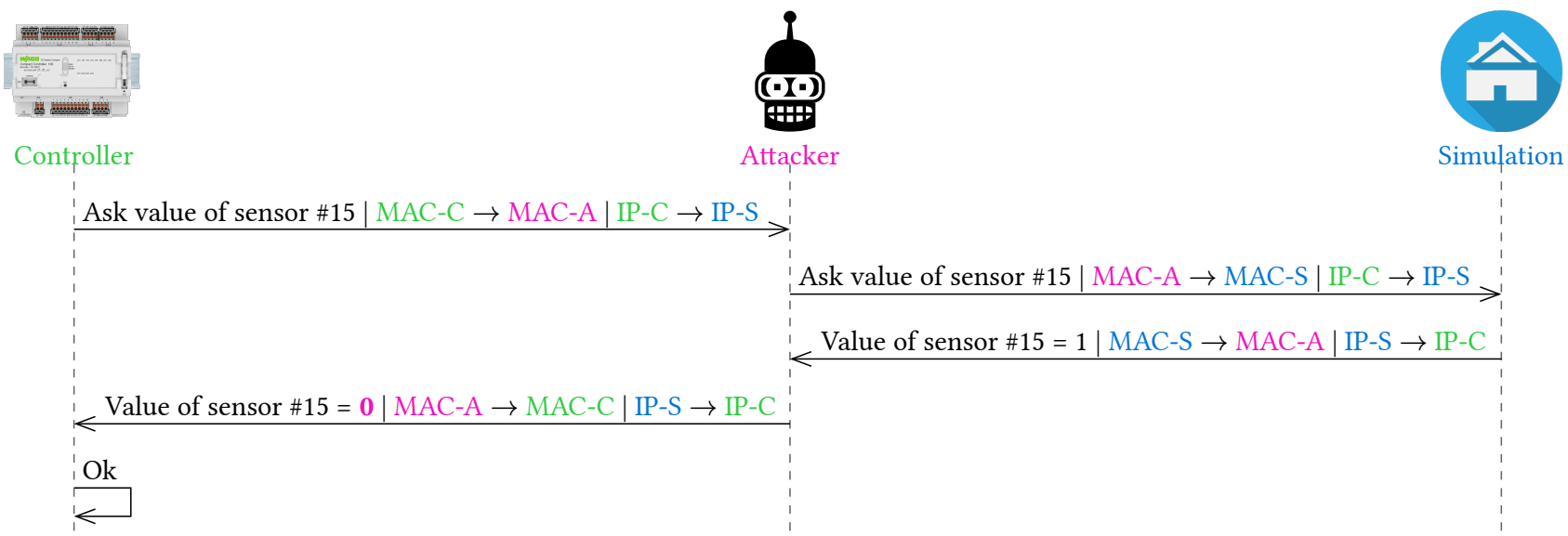
Attack on Modbus/TCP



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 & X.509

- Encrypt session

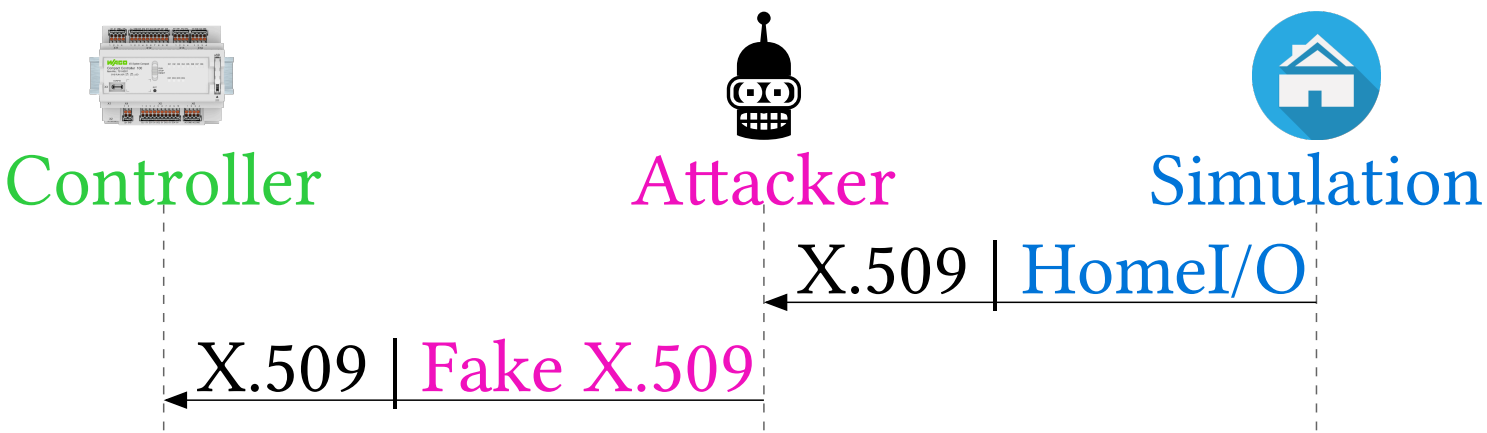
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

X.509

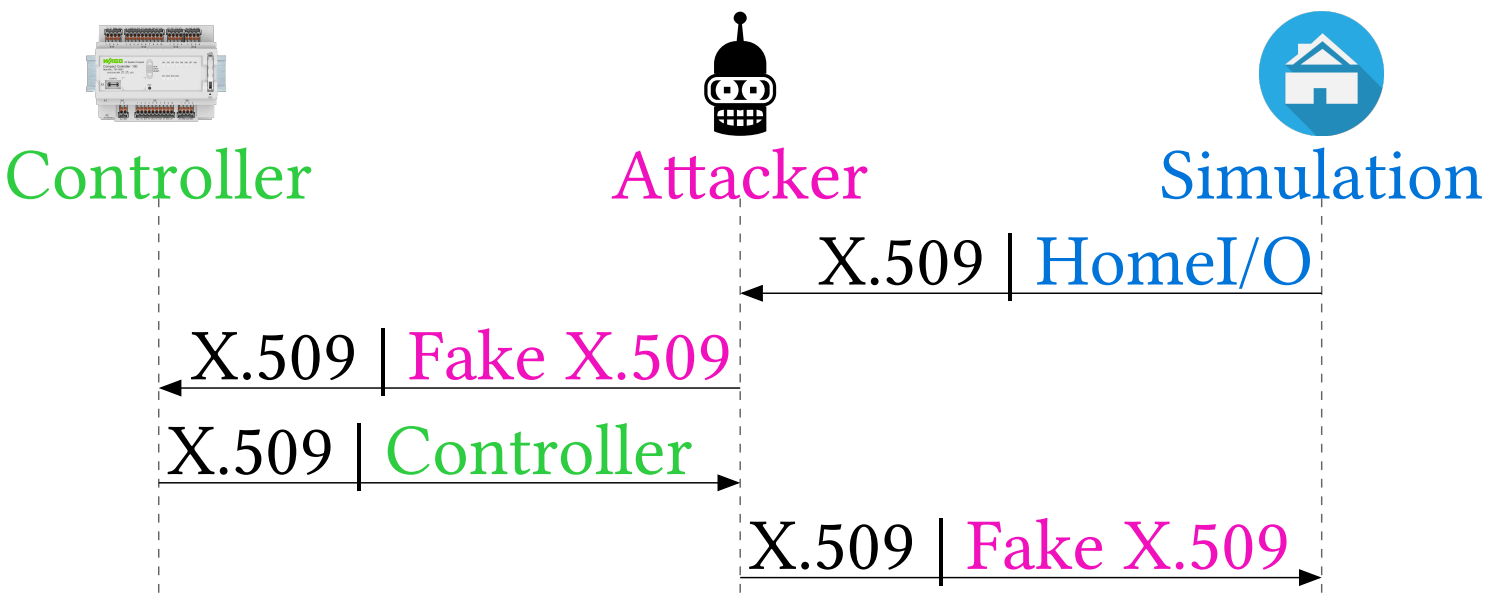
- Owner
  - Public key
- Certificate authority
- Signature

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 - 2012

Attack on Modbus/TLS

The most dangerous code in the world:
validating SSL certificates in non-browser software

— Martin Georgiev - 2012

Aapo Oksman proved it still holds **last year**



Questions?