



---

# OT Security

PEN-testing and security about embedded devices

---

Rémi Heredero

Tuesday, September 10 2024

# What's OT Security

# What's OT Security

## OT vs IT

# What's OT Security

## OT vs IT

- Information Technology (IT)  
= CPU

# What's OT Security

## OT vs IT

- Information Technology (IT)  
= CPU
- Operational Technology (OT)  
= MCU

# What's OT Security

## OT vs IT

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

# What's OT Security

## OT vs IT

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

## Security

# What's OT Security

## OT vs IT

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

## Security

- Before: IT wall



# 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

# What's OT Security

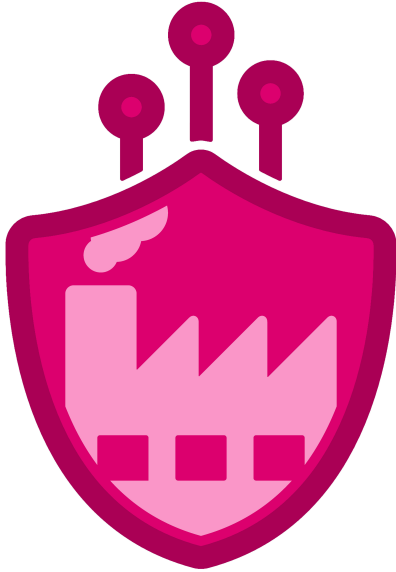
## OT vs IT

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

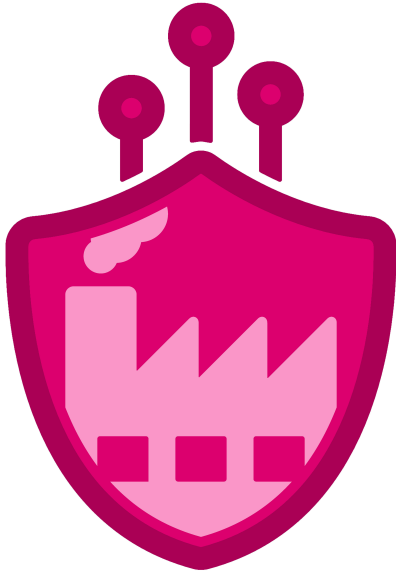
## Security

- Before: IT wall
  - Now: IoT everywhere
- ⇒ Time to put Security in OT

# This thesis

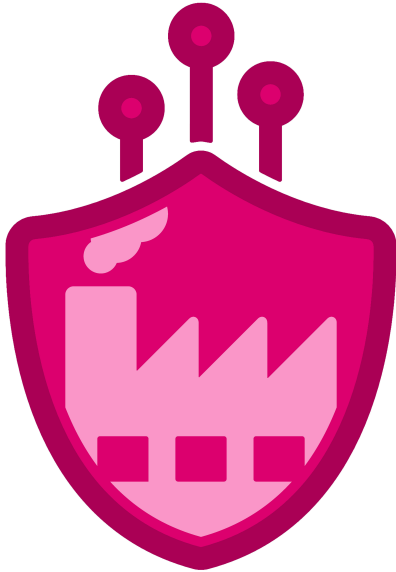


# This thesis



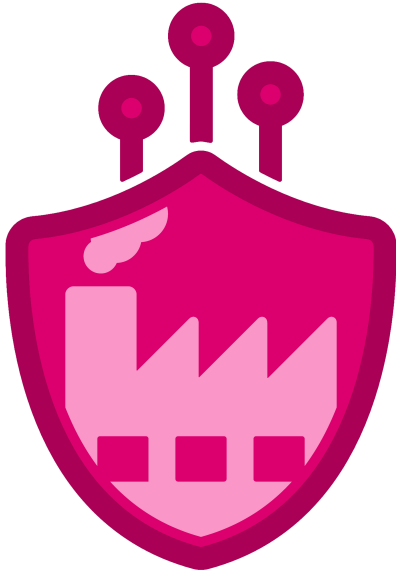
- Labo OT Security - I6

# This thesis



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

# This thesis



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

# Replay scenario

---

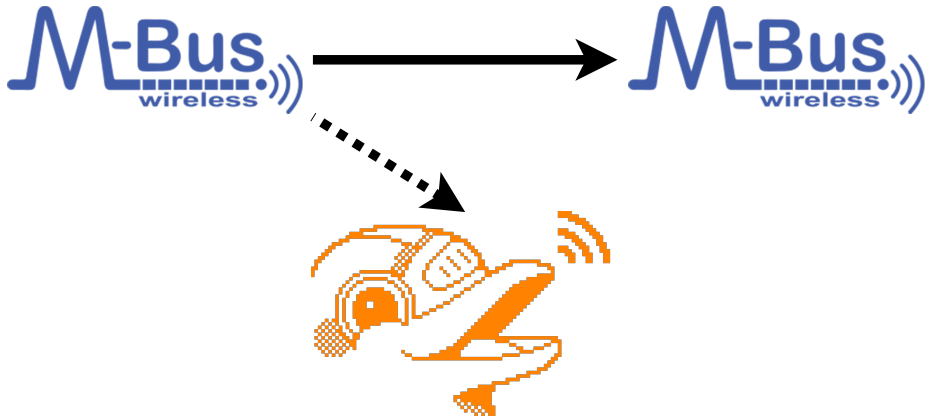
# Environment



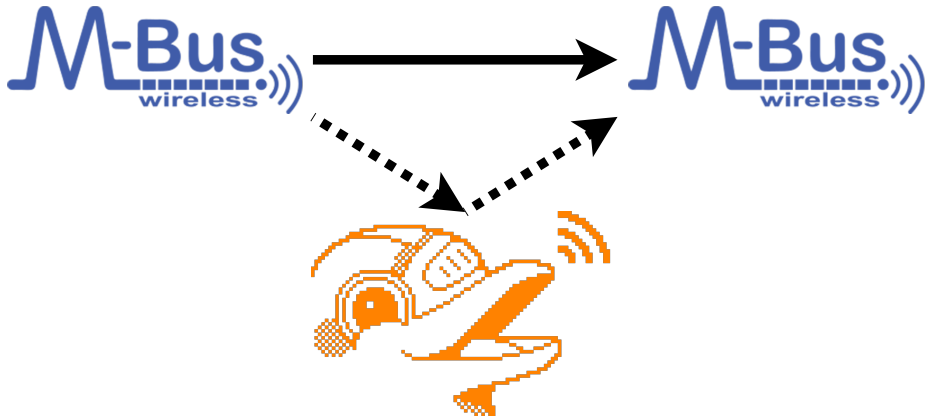
# Environment



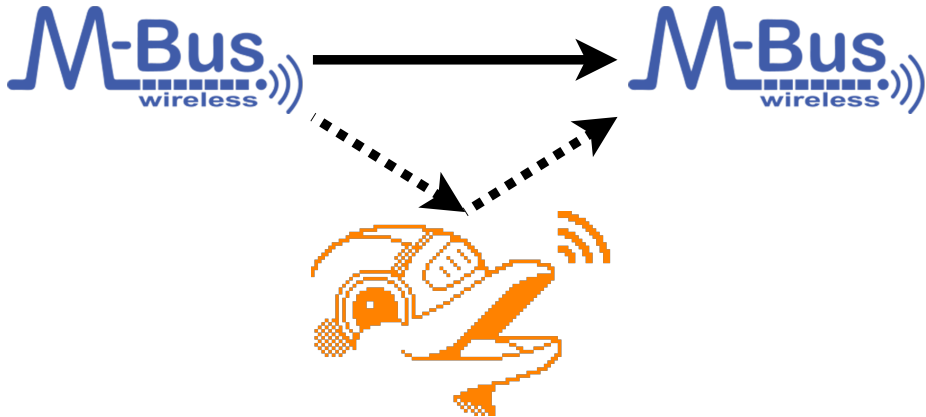
# Environment



# Environment



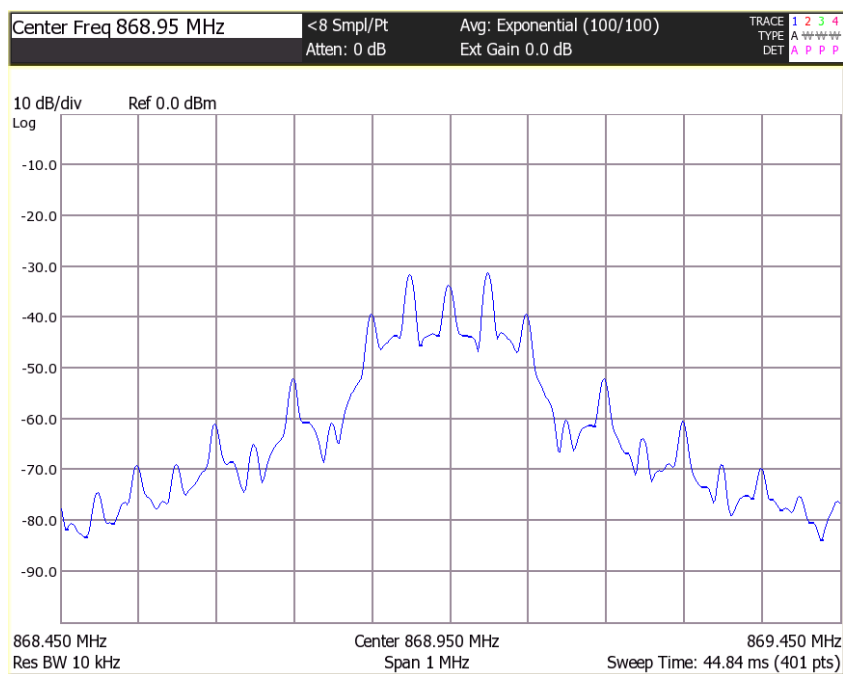
# Environment



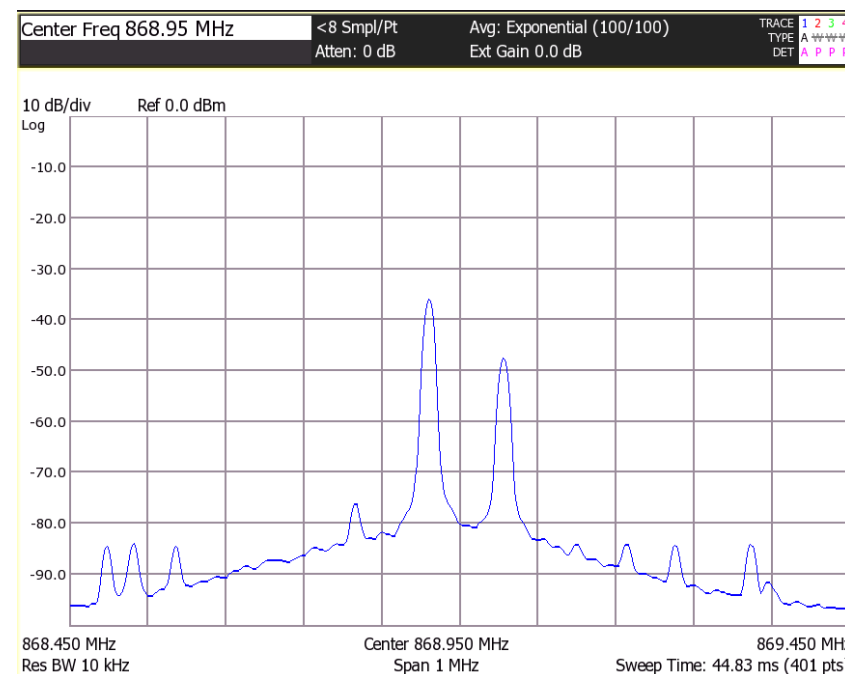
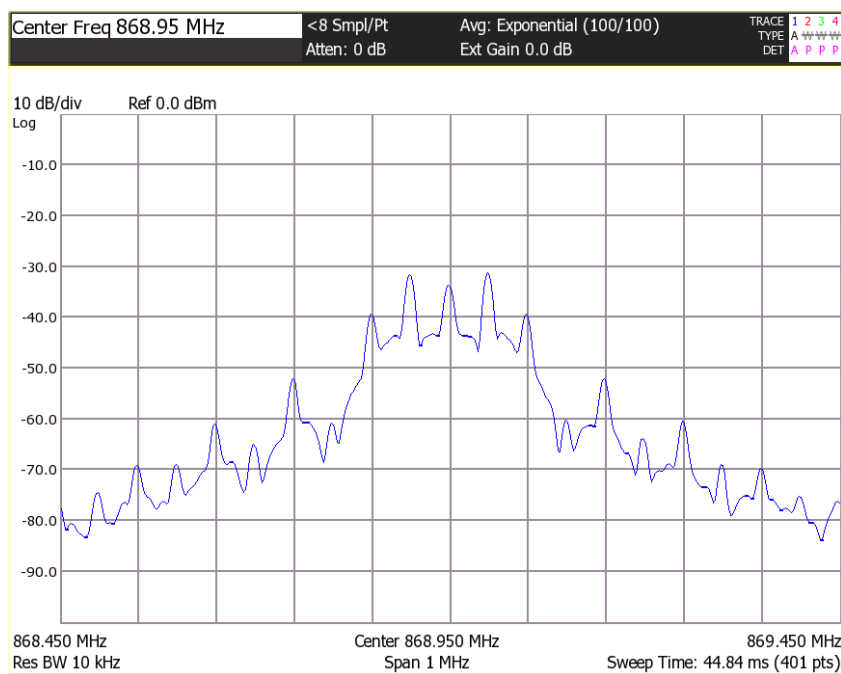
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

# The Flipper modulation

# The Flipper modulation



# The Flipper modulation



# Plan B & Security



# Plan B & Security

## Transceiver 433 MHz

# Plan B & Security

## Transceiver 433 MHz

- OOK

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

## Security

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

## Security

- Different messages

# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

## Security

- Different messages
- Rolling code



# Plan B & Security

## Transceiver 433 MHz

- OOK
- Serial
- Preamble
- Start & Stop characters

## Security

- Different messages
- Rolling code
- Signature

# **Man in the Middle (MitM) scenario**

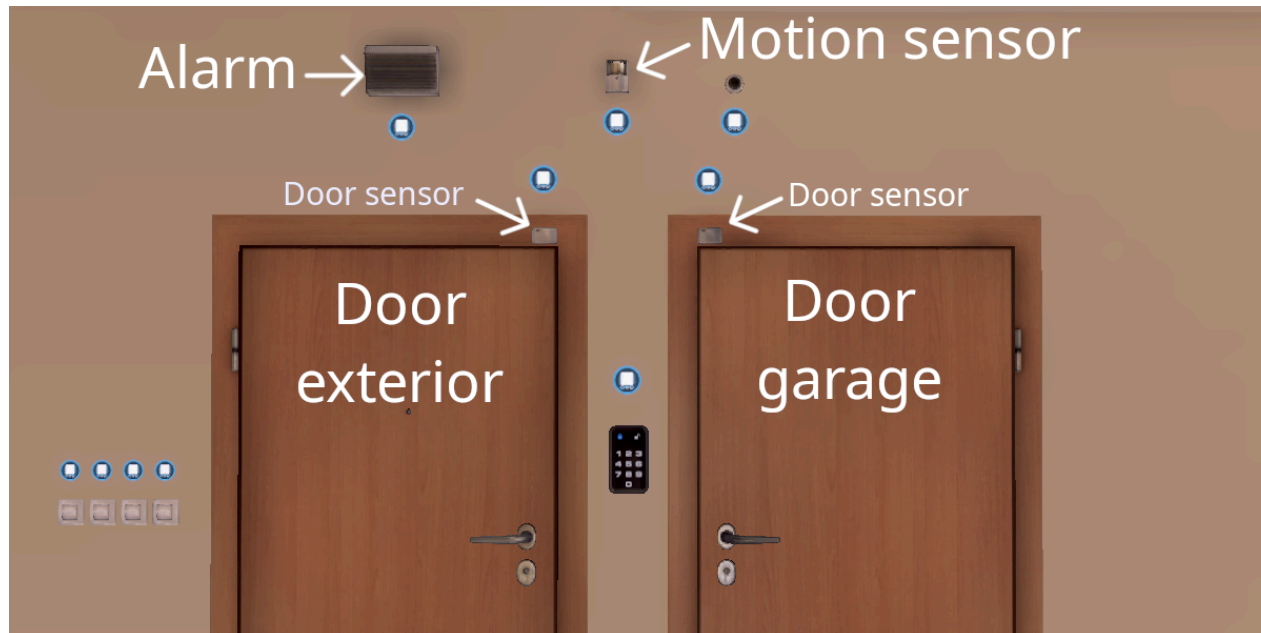
---

# Home I/O

# Home I/O

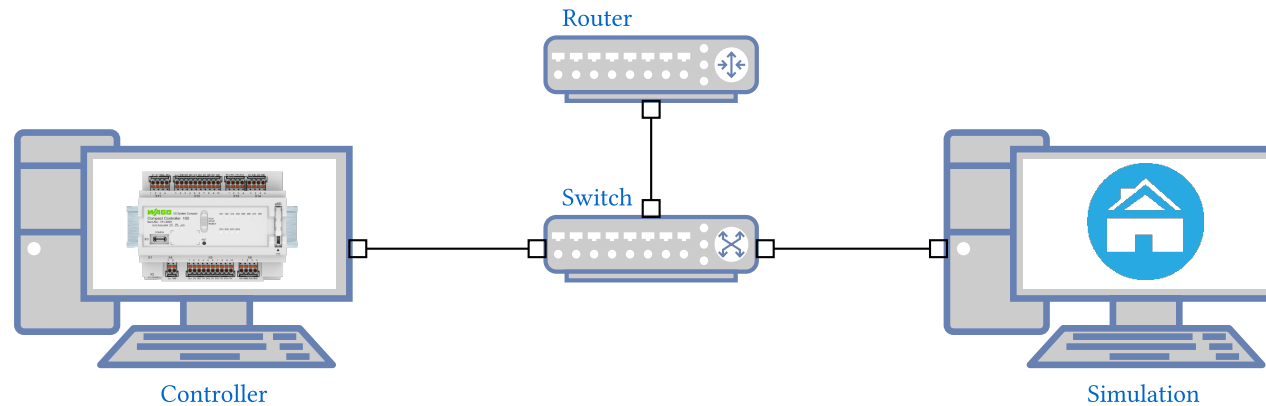


# Home I/O

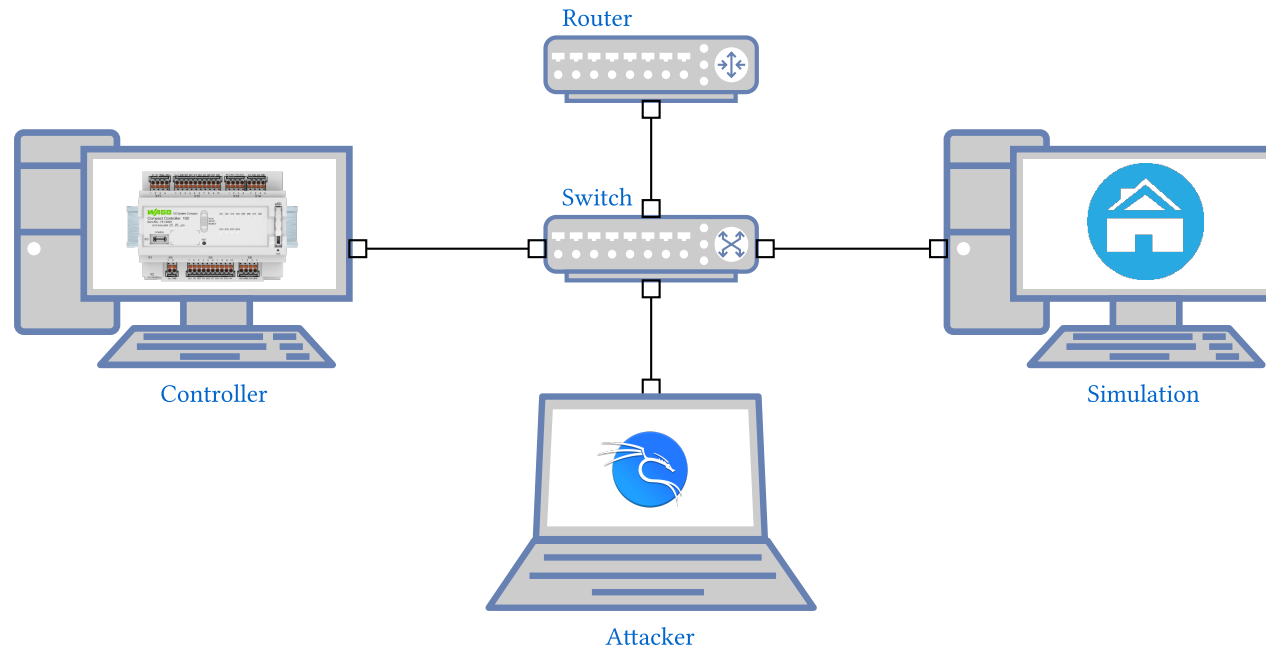


# Architecture

# Architecture



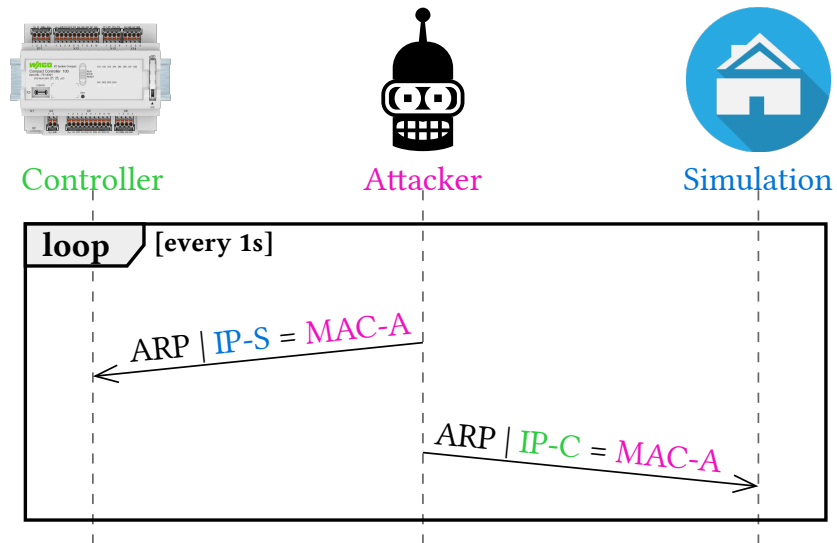
# Architecture



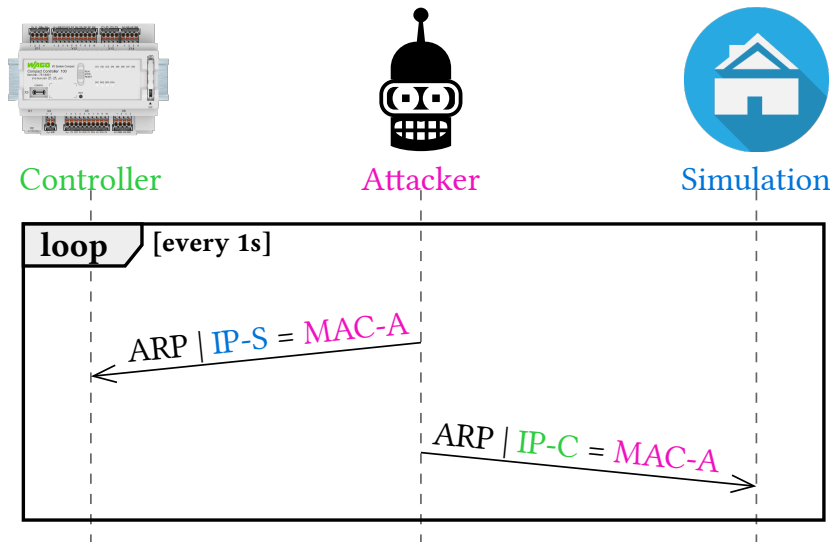


# ARP Poisoning

# ARP Poisoning



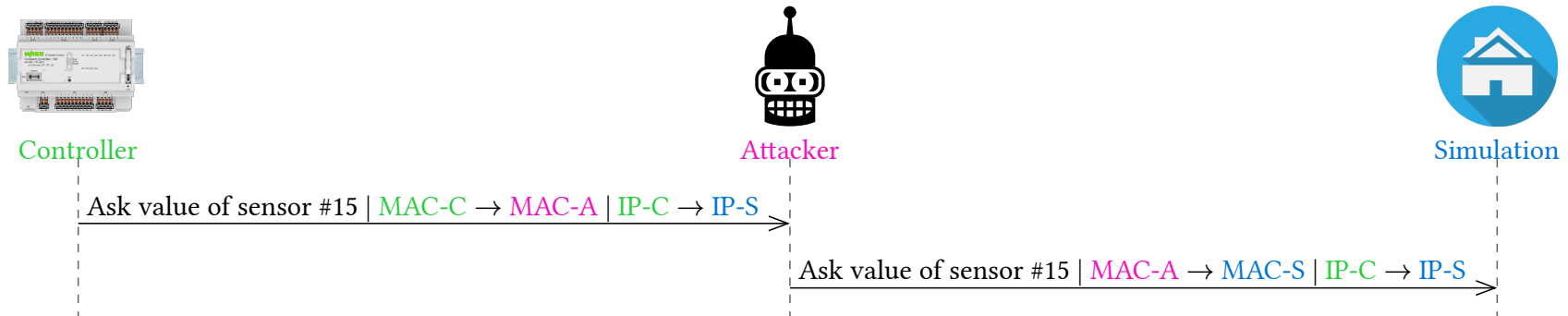
# ARP Poisoning



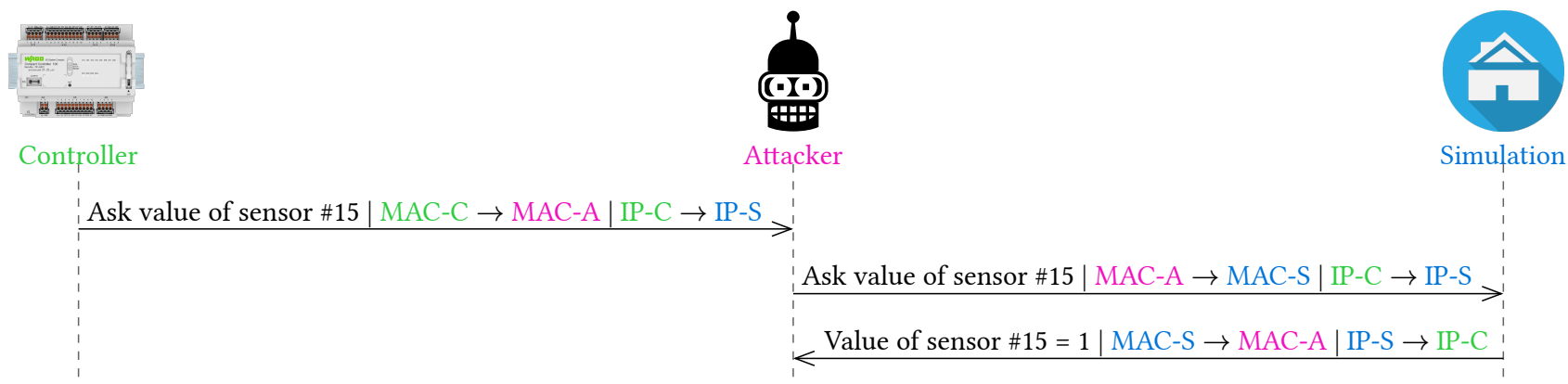
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

# Attack on Modbus/TCP

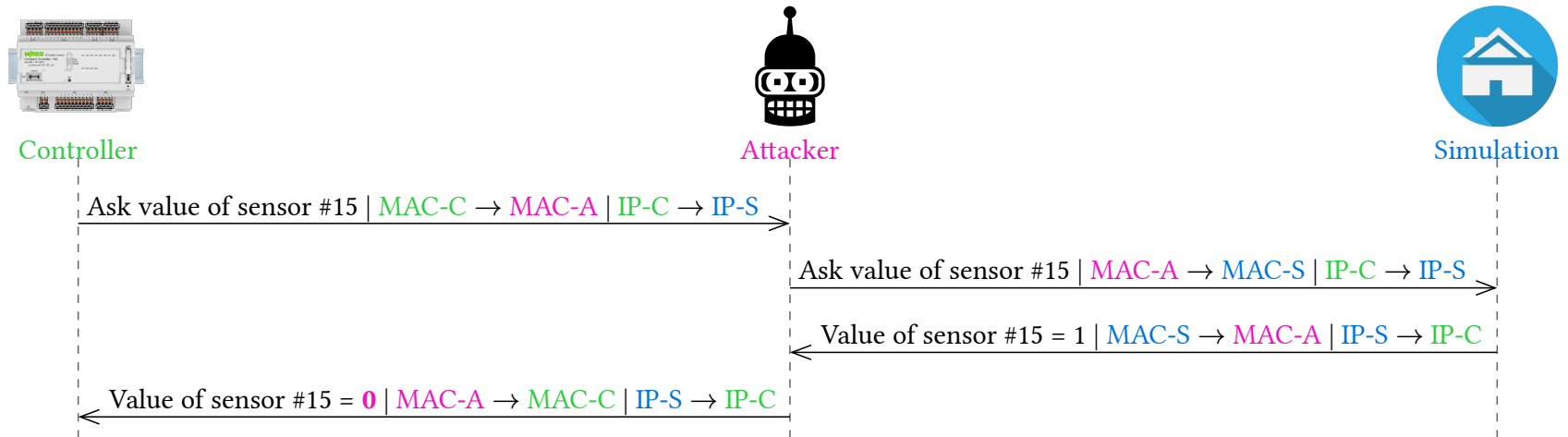
# Attack on Modbus/TCP



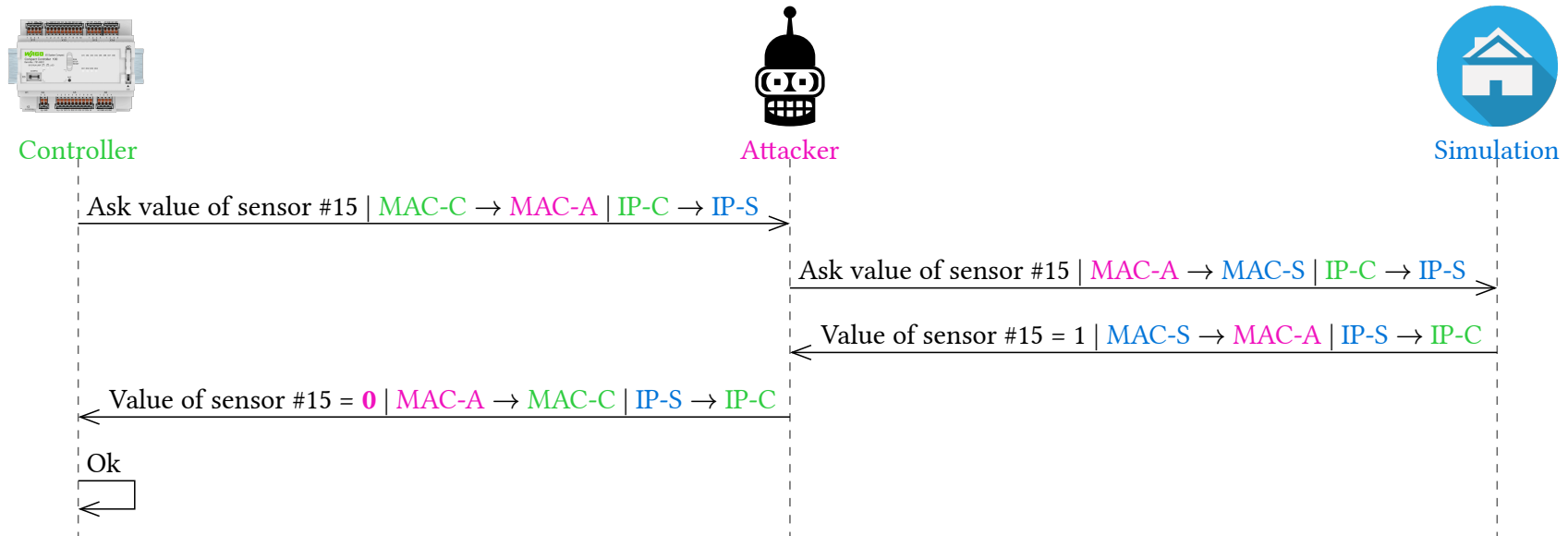
# Attack on Modbus/TCP



# 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 & X.509

# TLS & X.509

- Encrypt session

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

# TLS & X.509

- Encrypt session

## X.509

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



# 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

# TLS & X.509

- Encrypt session

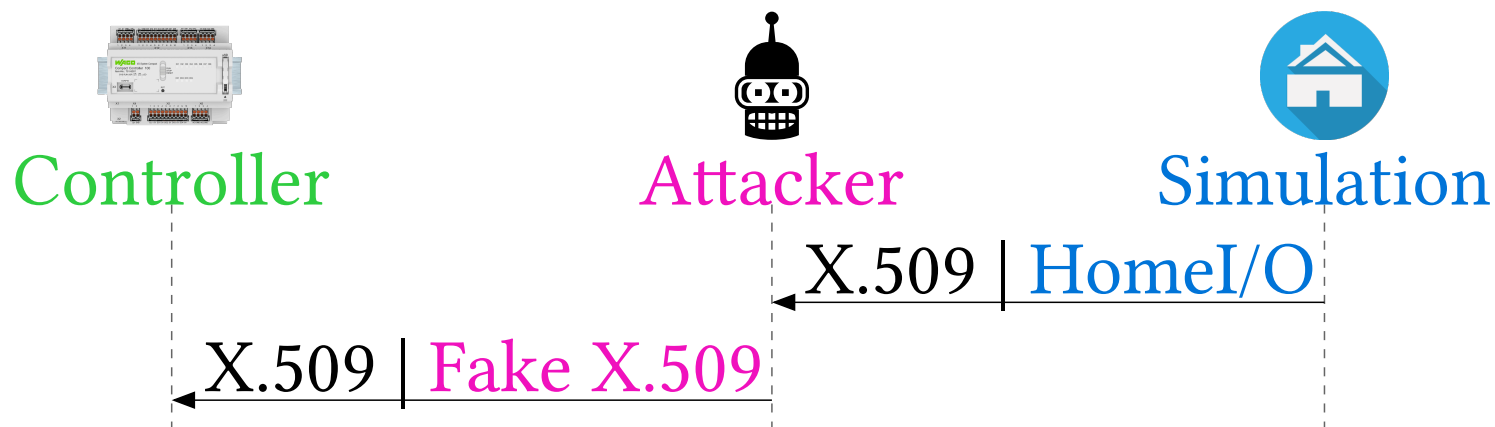
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

## X.509

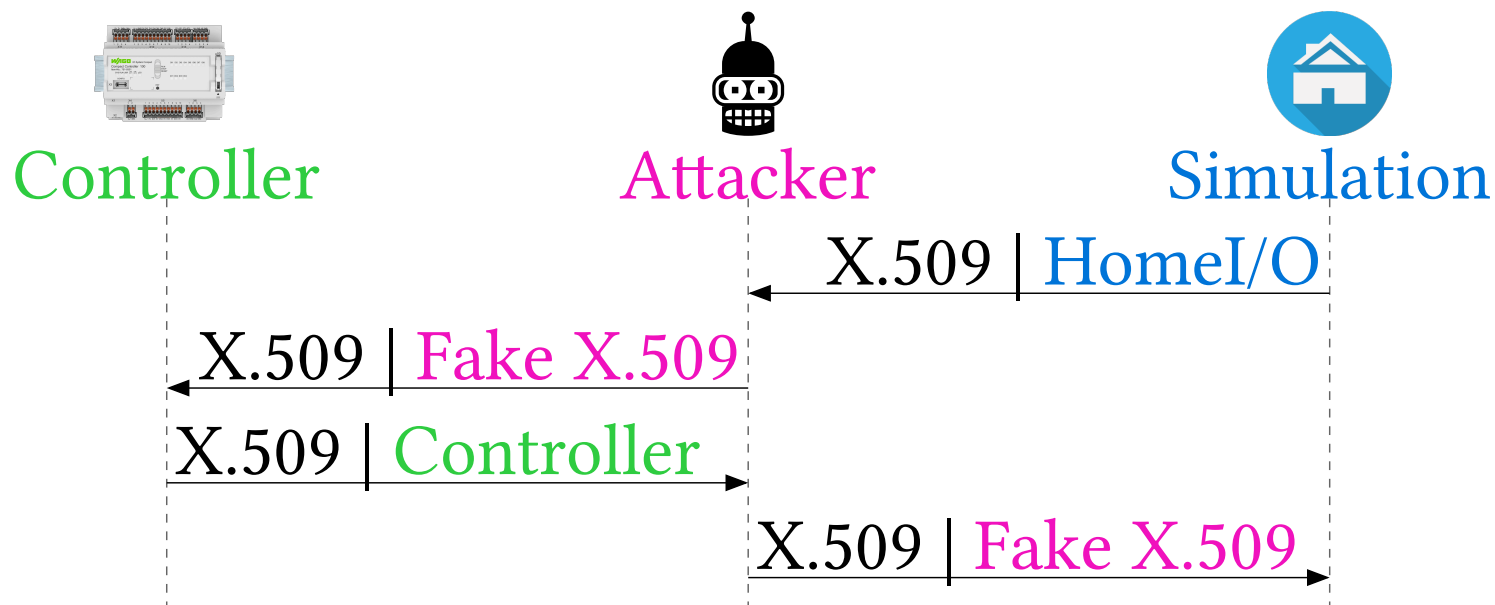
- Owner
  - Public key
- Certificate authority
- Signature

# Attack on Modbus/TLS

# Attack on Modbus/TLS



# Attack on Modbus/TLS



# Warning about TLS

# Warning about TLS

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

— Martin Georgiev - 2012

# Warning about TLS

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

— Martin Georgiev - 2012

Aapo Oksman proved it still holds



# Warning about 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**

# Warning about 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**



# Warning about 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**



# Warning about 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?