# IoT Security

Spring 2024

**Karel Slavicek**
**Vaclav Oujezsky**
**Bacem Mbarek**
**Tomas Pitner**

# Lesson outline

- Aim and goal
- Content and scope of the lecture
- Lecture organization
- Evaluation

# Aim and goal

- Discuss IoT systems security
- Overview of IoT HW used to protect other resources
- Vulnerabilities of communication busses and protocols commonly used in IoT systems
- IoT and cryptography

# Prerequisities

- Basic knowledge of
  - computer architecture
  - operating systems
  - OS Linux
- ABC of programming in C/C++
- ABC of communication and cryptography is advantage

# Content and scope of the lecture

- Focus on lab exercises and hands-on experience
- Lessons for a global overview
- Minimizing the obligatory stuff
- Flexibility in lab design
- Students’ qualification theses upon request

# What this course is about

- Basic properties of IoT devices used for security applications
- Overview of both internal and external busses and its vulnerabilities
- Cryptography support for IoT

# What this course is NOT about

- Physics of the sensors
  - Department of physics at Faculty of Sciences
- Electronics design
  - Faculty of Electrical Engineering and Communication Technology

# Lecture organization

**Lessons**

- 13 weeks of spring term
- 12 lessons + 1 spare
- Up to 10 technical lesson + 2 special - invited lectures / visit at industrial partners
- New lessons and lecturers – please be tolerant to some deficiencies in formal side of the lecture

# Lecture organization

**Lab exercises**

- 1 introductory + 10 regular + OpenLab days
- All necessary SW installed on PCs in KYPO, students own devices supported as well
- Overview of available HW in lab exercises
- Number of participants on lab exercise limited by room size and number of equipment – currently not an issue
- Few times, our room for lab exercises might be occupied by other event – reschedule or cancellation

# Lecture organization

**Studying material** on the web (is.muni.cz + gitlab)

- Slides from presentations
- IDE and supportive SW
- Sample code
- Description and schematics of used HW

# Evaluation

- Colloquium
- Standalone projects optionally solved in groups
- Projects will be discussed during the colloquium

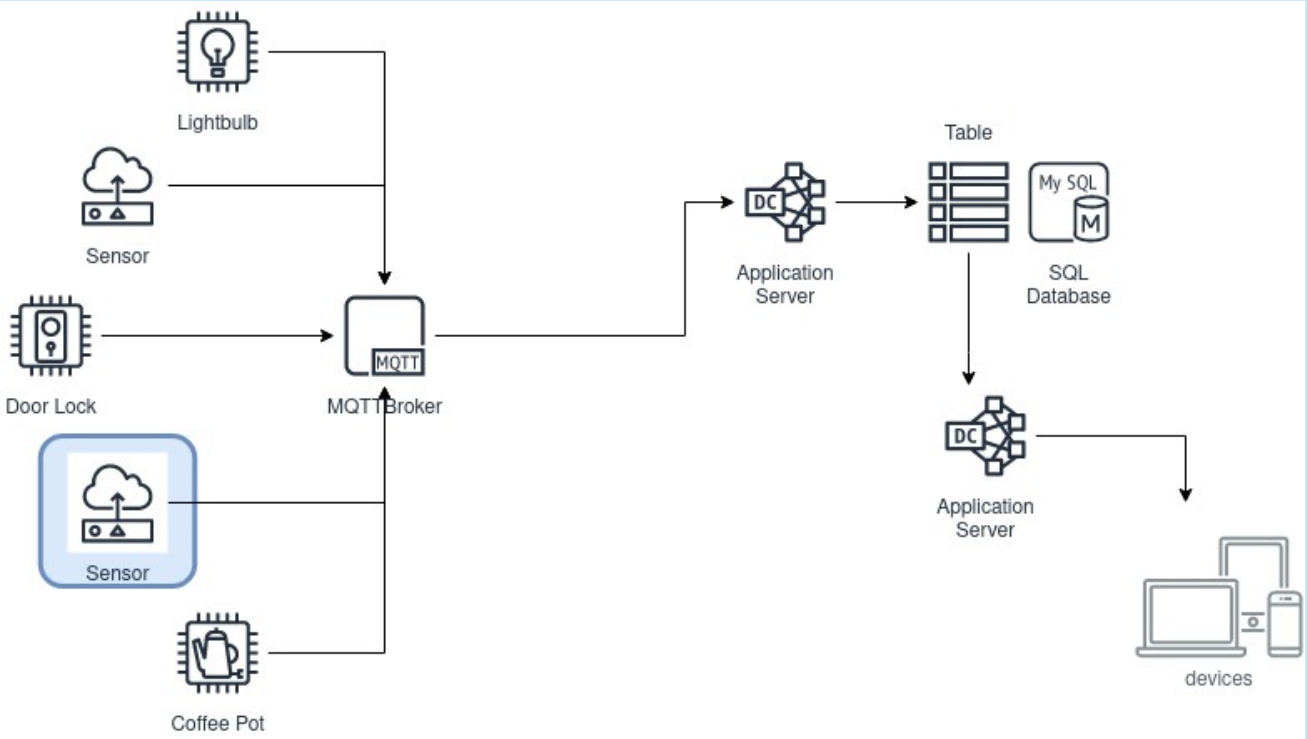
# Lecture organization

**Any questions / comments / requirements ?**

# Summary from the Introduction to IoT

**What is it the IoT ?**

# Structure of an IoT System



# Structure of an IoT System

# Elementary sensors

- **Fingerprint scanner**
- **RFID/NFC card readers**
- Push buttons and switches
- Rotary encoder
- Temperature
- Humidity
- Barometric pressure
- Proximity

# Output devices

- LED diodes and 7-segment displays
- LCD displays
- OLED
- TFT and capacitive touch screens
- E-paper

# Local Data Storage

- uSD
- EEPROM
- FLASH
- eMMC

# Internal busses

- **I2C**
- **SPI**
- 1-Wire
- **UART**

# MCUs and Singleboard Computers

- Bare metal programmable
  - ARM Cortex M – **STM32**, EFM32, ...
  - AtMega (Arduino)
  - AtTiny
  - MSP430
  - **ESP-32**
- Singleboard Computers
  - Raspberry Pi
  - **Rock Pi**
  - Orange Pi
  - Anything Pi

# External busses

- **RS-485 / MODBUS**
- CANBUS
- M-Bus
- FlexRay
- **UART**

# Wireless communication

- WiFi
- Bluetooth
- Sub-Ghz wireless – **868MHz**, 433MHz / SigFox, **LoRa**, …
- ***InfraRed*** communication

# Communication busses

- Similarity with data networks
- ISO-OSI reference model
- Multiple layers: RS-485 / MODBUS
-
- Eavesdropping
- Fake data

# Course plan

- Fingerprint scanner
- RFID/NFC
- DLT, cryptographic algorithms and chips
- LoRa WAN
- Eavesdropping of communication busses

**Thank for your attention!**

**Questions and comments?**