Introduction to the Internet of Things

MCIoT Session 15

Ulrich Norbisrath
Outline Today

• RGB Strips
• The Internet of Broken Things
• IoT in Estonia
• Summary, Reflection (, and more)
Reminder: remaining deadlines

• 13.12 Project presentations
  • More on next slide

• 19.12
  • Deadline for IoT labs portfolio
  • Deadline for finishing Project GitLab
    • Bug fixes, Readme-s and Wiki
    [https://courses.cs.ut.ee/2021/MCIoT/fall/Main/PresentationsAmpReport](https://courses.cs.ut.ee/2021/MCIoT/fall/Main/PresentationsAmpReport)

• Students who don’t meet the 70 pts criteria for passing the course will have a „re-sit“ exam opportunity in January.
Project Presentations

• 13.12, 16:15
• MS Teams, in 2 parallel sessions
  • SIGN UP HERE!
    • https://doodle.com/poll/rrvwze7t3xxwb7uy
• Each team has 15 mins:
  • Shows their Pitch/Demo Video (5-7 min)
    • Send us a youtube link, dropbox link, or one drive, ...
  • Talks about project experience 5 min
    • Role assignment
    • What went well, what went poorly
    • Future improvement ideas
  • Discussion & Questions (3 min)
RGB Strips

• 1 Wire/2 Wire bus to control 1000s of Leds (individually)

• Common Types
  - WS2812(b) – often called Neopixel – usually high quality, 5V (expensive power supplies)
  - WS2811 – less quality, often just “triplets” controllable, but super cheap (< 4 EUR per meter/30 Leds)
Introduction to the Internet of Broken Things

Session 15*!@

Ulrich Norbisrath
Outline

• Internet of Broken Things
  – Awareness/Examples of Breakages
  – Countermeasures and a software engineer's perspective
  – Let's not make IoT an IoBT (Internet of Broken Things)

• Discussion about measures, we can take
IoT is Here: What Could Break?

• 12 Billion today - up to 25 Billion connected devices in 2025

• How could anything go wrong?

• From your head and Google (5 min):
  – What did already break (is broken)?
  – What will break?
  – Why?

• Open discussion (5 min)

• → portfolio
What is broken (and why)?
What is broken (and why)?

Previous findings

- No updates
- Updates happen whenever
- Direct communication with cloud
- No certificate validation
- No encryption
- Hacked devices can attack anything in local network
- Devices are too powerful for their means
- No responsibility
- Only one very weak firewall → no layered management structure possible
  - Solution? Easily controllable fine grained (ssh), to build/config layered security
During the Following Lecture Part

- Google the threats (and write down notes in portfolio about it)
- Reflect on the threats. Do you think that they are still valid?
- Start searching on more threats and (if existing) countermeasures.
Causes for Breakage

- Companies assume they can do updates for a fleet of devices
  - They can't
- Automation devices on same network as desktops or other infrastructure
- Default passwords
- Privacy exploitation enforced by corporate entities
- Star topology/no layered security
Example Break Downs

• Default passwords in devices and routers
  – Zombie webcams and routers

• WIFI networks very insecure - last widely deployed standard WPA 2 from before 2009 (IEEE 802.11w was specified 2009)
  – Deauth attack
  – Krack attack

• Cyber abuse

• Man in the middle attack
Zombie Webcams

1 500 000 internet connected cameras attack one infrastructure

Deauth Attack

• Let me take down your internet for USD 2.00
• Countless denial of service attacks possible
  – Hospitals
  – Service institution
  – Factories
• If both router and client use IEEE 802.11w, not possible (still rarely the case)

https://github.com/spacehuhn/esp8266_deauther/wiki
Krack Attack

• Most WIFI networks
  – All data of clients can be read
    (basically all WIFI – even protected ones are like public WIFIs)

• Examples
  – Passwords for local devices are visible in clear text
  – Data filled in forms can be read
  – Patient data visible
  – Insurance and identity data visible

- https://www.krackattacks.com/
- https://github.com/vanhoefm/krackattacks-scripts
Cyber Abuse

- Usually domestic
- Thanks to IoT increasing quickly
- Examples:
  - Weird behavior of smart locks, air conditioning, lights
  - Abuser spies and knows too much
  - Prevented transactions
Man in the Middle

Image from: http://www.webstepbook.com/supplements-2ed/slides/chapter15-security.shtml#slide41
Hardening in practice
Setup/connect to secure MQTT server

• Layers!
• Example: connect your local mosquitto to mosquitto in cloud with ssl
IoT in the Neighborhood

- Hand over to Jakob
Summary/Reflection/and more

• What is IoT?
  - It’s a lot about networking and connectivity → Windows networking fun!
• How can stories help?
• MCUs: ESP8266
• Arduino IDE as intro to MCU programming, small follow-up with PlatformIO
• IoT Computing Paradigms (cloud, edge, and friends)
• Low Level Busses (from serial to I2C and SPI)
• MQTT and Publish Subscribe on Network Level
• Flow-based Service Integration (Node-RED)
• A sample IoT integration and deployment framework: IoTempower
• IoT in industry (Ruben)
• Low Power consumption and alternative networks
What was missing, what would you liked to also studied?

• Open discussion
We would have liked to do...

- A bit more on security (at least layered networks, security switch)
- A bit more on networks
  - Firewalls
  - Port reflection
  - Alternative networks: work with ESP-Now (maybe LORA), PJON (→ check it out: http://pjon.org), Bluetooth
  - Cloud Integration/Cloud platforms
  - Edge Computing
  - Realtime Stream Processing
- More on energy saving, solar panels, batteries
- More Android integration – esp to phone (bt or network discovery)
- Other IoT Frameworks (Cumulosity, Mongoose, Blink, Thingspeak)
- Building automation
- The rest of the kit
What else?

- Open questions
- Remarks
- Ideas
Finalization

Do not miss the awesome projects (watch and rate your track → portfolio), but also consider watching others, at least the videos (share videos!!!)

We will record both teams sessions.