Introduction to the Internet of Things

Session 09

Ulrich Norbisrath

LORA (2nd part)

- Andreas Spiess, Youtube, explanation movie
  - https://www.youtube.com/watch?v=hMOwbNUpDQA
- Make notes regarding (→ research record):
  - What is the relation bandwidth/range/power?
  - What is the link budget?
  - What is the community approach?
  - What are benefits with LORA?
  - what are problems with LORA?

LORA (after movie, 10+5min)

- Google link budget again:
    - what is it exactly , find examples
- Google "radio link budget calculator"
    - Do two calculations for LoRa and for WiFi
    - Note down results
- Google: LORA in Austria and Linz.
    - What activities exist
- Google how expensive a LORA client adapter, LORA gateway (or gateway adapter) is
- Check LORA's software support (and licenses for the respective libraries)
- Discuss with neighbor:
    - What is Lora good for, what might it be bad at?
    - What are its advantages/short comings?
    - How does it fit into IoT?
- → research record

ESP-Now, super cheap alternative for LORA?

- Andreas Spiess: https://youtu.be/6NsBN42B80Q
- Research report (while watching):
  - What are the advantages of ESP-Now in comparison to LORA
  - What are the disadvantages of ESP-Now in comparison to LORA
  - How could this be integrated with/into IoTempower?
  - What do you think yourself is the more interesting option (for what kind of projects)?

Introduction to the Internet of Broken Things

Session 09*!@

Ulrich Norbisrath

Outline

- Internet of Broken Things
  - Awareness/Examples of Breakages
  - Contermeasures 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?

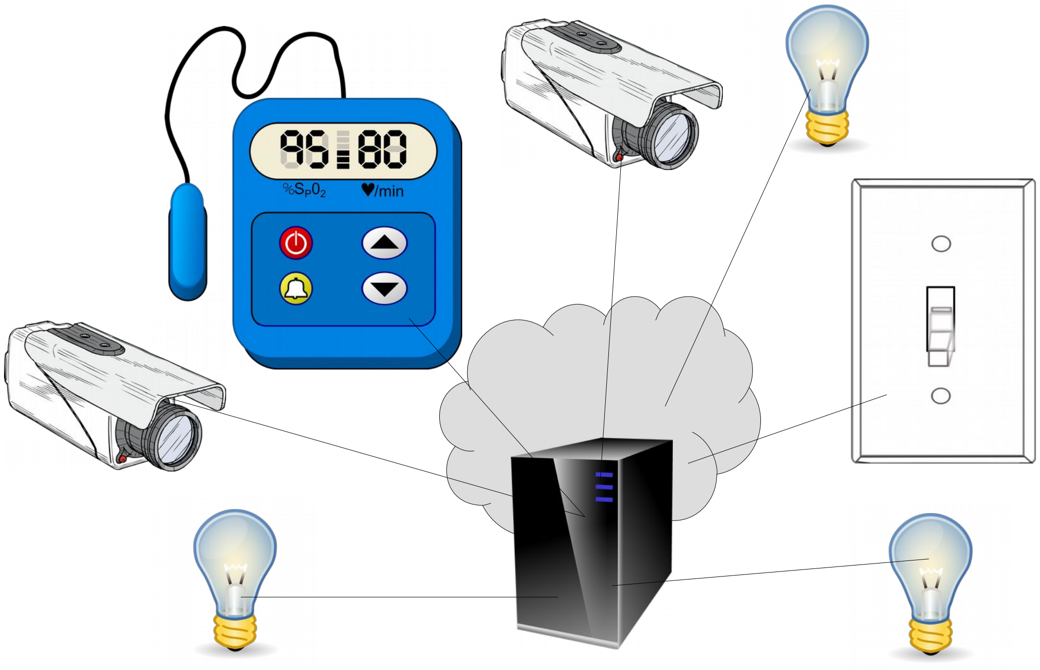
- 20-50 Billion connected devices in 2020
- How could anything go wrong?
- From your head and Google (5 min):
  - What did already break?
  - What will break?
  - Why?
- Open discussion (5 min)
- → research report

During the Following Lecture Part

- Google the threats
  (and write down notes about it)
- Reflect on the threats. Do you thing 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



What is broken?

What is broken?

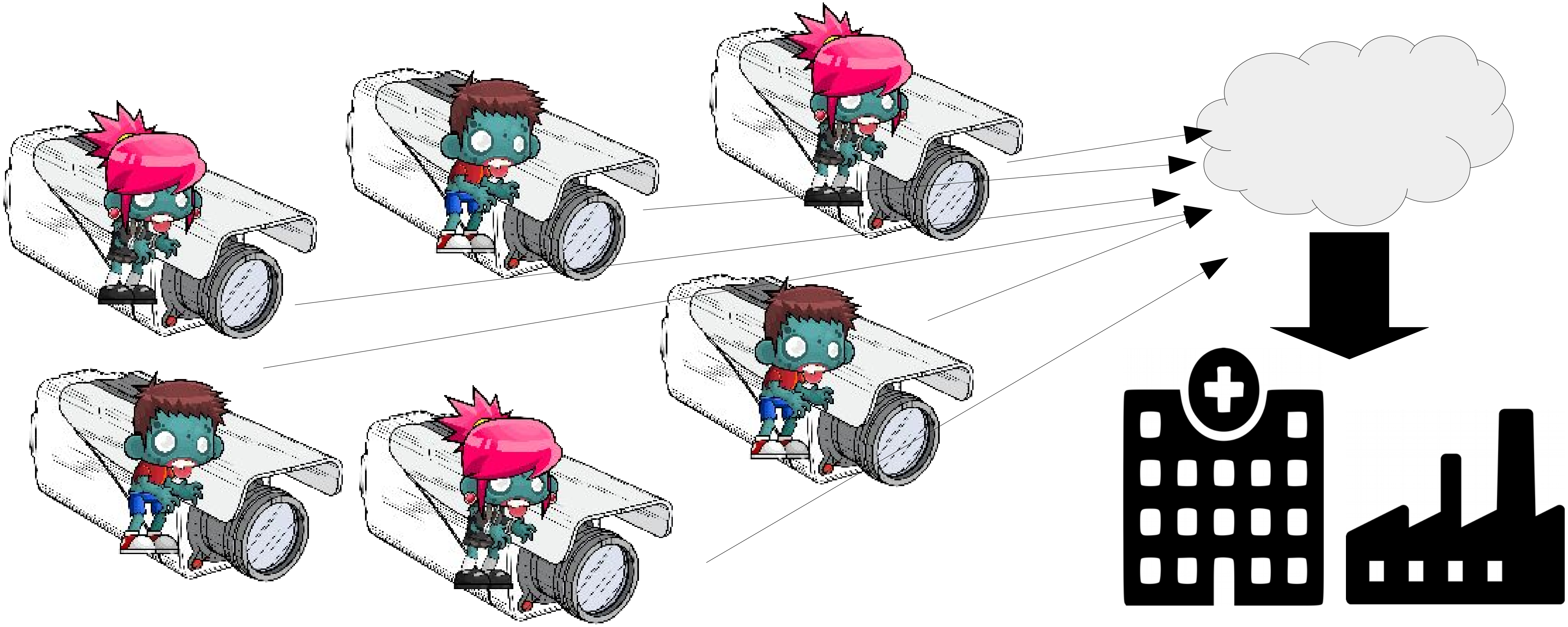
- No updates
- Updates happen whenever
- Direct communication with cloud
- No certificate validation
- No encryption
- Hacked devices can attack anything in local network
- Devices are too powerful for their means
- No responsibility
- Only one very weak firewall → no layered management structure possible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

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

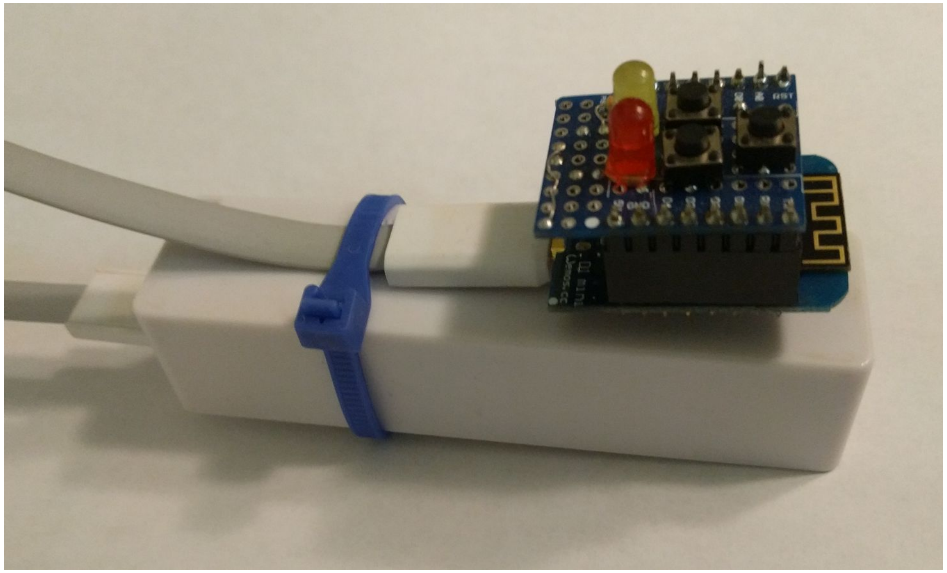
1 000 000 internet connected cameras attack one infrastructure



- https://www.law360.com/articles/861699/attack-of-the-zombie-webcams-ddos-attacks-and-the-insecure-iot
- https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

Deauth Attack

- Let me take down your internet for USD 3.00
- 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

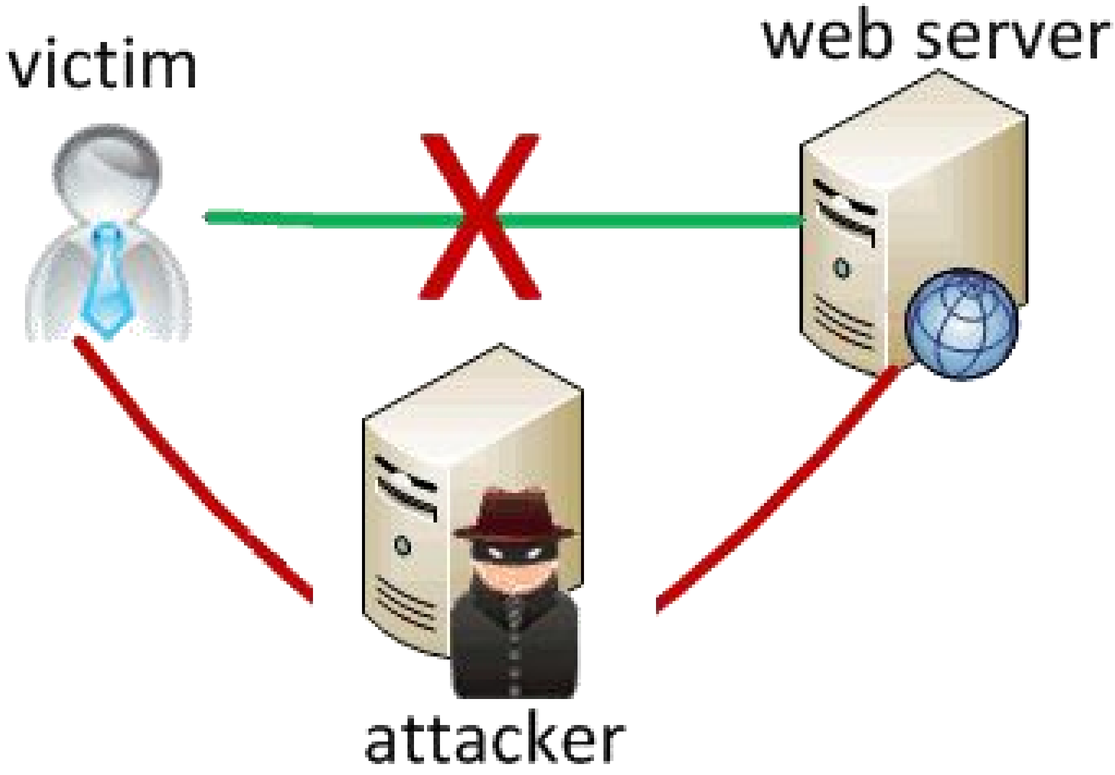


Image from:
http://www.webstepbook.com/supplements-2ed/slides/chapter15-security.shtml#slide41

Hardening in practice
Setup/connect to secure MQTT server

- Demonstration with ulno.net
- Note down relevant data to connect your Node-RED in lab to this → research report

Lab 9

- Continue and finish project 1
- Connect your Node-Red to other team's node-red via ulno.net (topic iot2019/UniqueMergeTeamName), exchange sensor data
- ESP-Now
  - Use unicast examples from https://github.com/yoursunny/WifiEspNow in platform.io or Arduino IDE (no IoTempower yet in this task)
  - Build a connection tester for ESP-Now (two nodes/esp8266 sending numbered packages to each other), check how many are dropped.
  - Leave one in lab, take other one around campus
  - Check how far you can still transfer data (and in which direction) – if you have already a big team (for final project), you can do this task only once per big team (maybe with another node to speed up test)

Alternative Lecture: Research Exercise and Debate

- Form teams of 6-9 people
- Spent 5min to pick 5-8 research papers/articles on the Internet of Broken Things
- Divide people in pro and con IoT (randomly, ~50/50)
- Read papers and compile lists on (each pro and con sub team has to read all papers) (40min):
  - What is broken (with examples)?
  - How can it be fixed/counter measures?
  - Newsworthy failures/successes
- Elect a moderator (both pro and con and can decide the winning team)
- Break
- Debate in team: “We should abandon all work with the Internet Of Things and only focus on classics (mobile devices and industrial building automation).” (That’s the hypothesis of the con team).
- Open discussion, constructive solutions → write down keywords for solutions → participation proof