TU Clausthal

Institute for Software and Systems Engineering

# Emerging Technologies for the Circular Economy

## Lecture 5b: IoT Security and Privacy

Prof. Dr. Benjamin Leiding (Clausthal)
M.Sc. Arne Bochem (Göttingen)
M.Sc. Anant Sujatanagarjuna (Clausthal)

# License



- Updated versions of these slides will be available in our Github repository.

# EXAMPLES AND LESSONS LEARNED

# Who Refuses to Wash Hands?

2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications

## Who refuses to wash hands?

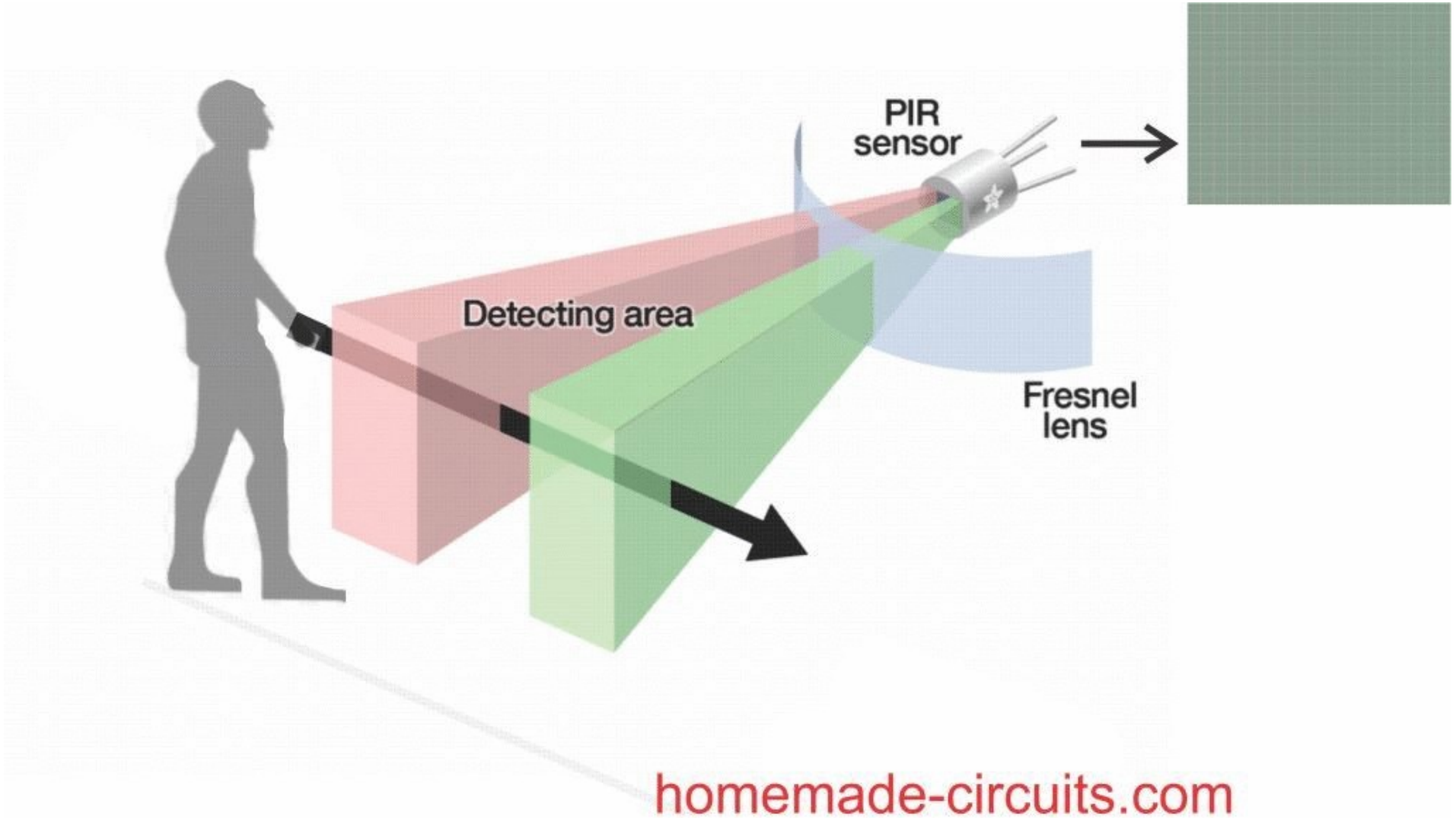
### Privacy issues in modern house installation networks

Thomas Mundt
Department of Computer Science
University of Rostock
Rostock, Germany
Email: thomas.mundt@uni-rostock.de

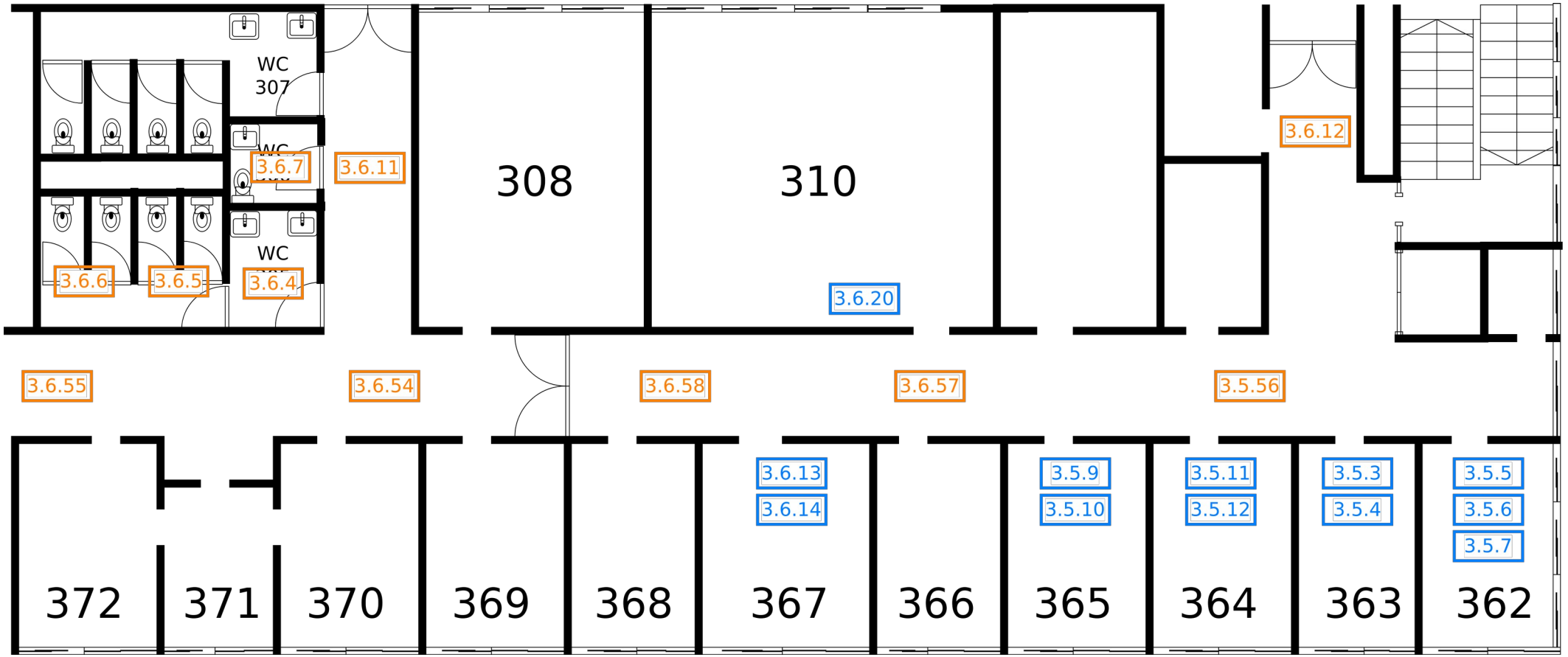
Frank Krüger
Department of Computer Science
University of Rostock
Rostock, Germany
Email: frank.krueger2@uni-rostock.de

Till Wollenberg
Department of Computer Science
University of Rostock
Rostock, Germany
Email: till.wollenberg@uni-rostock.de

# Who Refuses to Wash Hands?



# Who Refuses to Wash Hands?



# Who Refuses to Wash Hands?

Lessons learned:

- Correlation of data might reveal interesting and unexpected information.
- Implement existing IT security and data protection concepts (KNX can be operated securely) → e.g. encryption and authentication.
- In general:
  - Collect/store/analyze data vs. GDPR
  - Stored data must be secured and protected accordingly

# Jeep Cherokee Hack 2015

# Jeep Cherokee Hack 2015

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

# Jeep Cherokee Hack 2015

- WPA2 password → “TyYMxfPhZxkp”

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

# Jeep Cherokee Hack 2015

- WPA2 password → “TyYMxfPhZxkp”
- This corresponds to Epoch time 0x50e22720

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

# Jeep Cherokee Hack 2015

- WPA2 password → “TyYMxfPhZxkp”
- This corresponds to Epoch time 0x50e22720
- This is Jan 01 2013 00:00:32 GMT

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

# Jeep Cherokee Hack 2015

- WPA2 password → “TyYMxfPhZxkp”
- This corresponds to Epoch time 0x50e22720
- This is Jan 01 2013 00:00:32 GMT
- Took 32 seconds for WifiSvc to get started up
- Really only a few dozen passwords to try

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

# Jeep Cherokee Hack 2015

Lessons learned:

- No *security by obscurity*

# MORE EXAMPLES

# Fish Tank Thermometer

- Casino with fish tank in the lobby
- IoT fish tank thermometer
- Attackers compromise thermometer
- Use it to further compromise local network
- Exfiltrate customer database

https://www.businessinsider.in/Hackers-stole-a-casinos-high-roller-database-through-a-thermometer-in-the-lobby-fish-tank/articleshow/63769685.cms

# Fish Tank Thermometer

Lessons learned:

- IoT devices can be the weakest link
- Consider security between possibly vulnerable devices and local networks

https://www.businessinsider.in/Hackers-stole-a-casinos-high-roller-database-through-a-thermometer-in-the-lobby-fish-tank/articleshow/63769685.cms

# Library vulnerabilities: NAME:WRECK

- Vulnerabilities in multiple TCP/IP stacks
- Impact: From DoS to RCE
- Affects:
  - Medical devices
  - Avionics
  - Baseband processors in mobile phones
  - Servers
- Vulnerability in domain name parsing

https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/

# Ripple20

- 19 vulnerabilities including remote code execution in widely used low-level TCP/IP-stack library distributed under various names
- “Affected vendors range from one-person boutique shops to Fortune 500 multinational corporations, including HP, Schneider Electric, Intel,  Rockwell Automation, Caterpillar, Baxter, as well as many other major international vendors suspected of being of vulnerable in medical, transportation, industrial control, enterprise, energy (oil/gas), telecom, retail and commerce, and other industries.” – JSOF
- Demonstration: Turning off IoT UPS

https://www.jsof-tech.com/disclosures/ripple20/

# Library Vulnerabilities

Lessons learned:

- Even widely used libraries can contain grave security issues

# SECURING THE IOT

# Security

- General best practices for developing secure software
  - Avoid common issues:
    - Buffer overflows
    - SQL injections
    - etc..
  - Input validation
  - Secure defaults
  - Overall system design
- May also need to consider hardware security
  - Tamper-proof devices
- However: Often IoT devices are not designed with security in mind from the start.

# Cryptography (1)

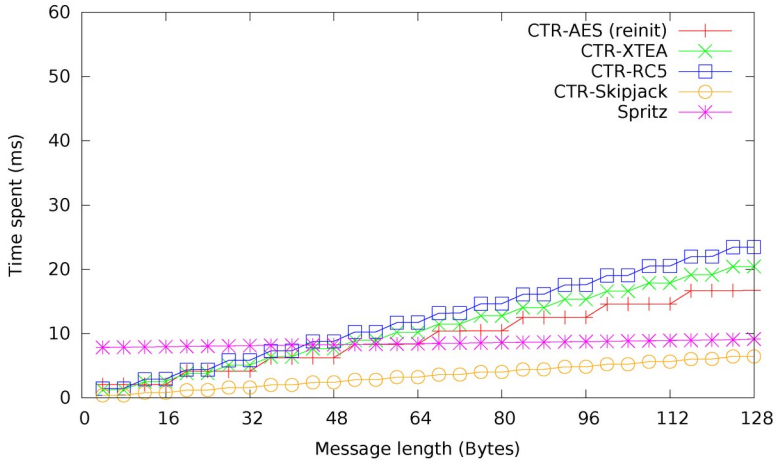
- Consider low-power devices
- Common protocols (SSL/TLS) often too heavy
- Main things to consider:
  - Confidentiality
  - Integrity
  - Authentication
- Different approaches

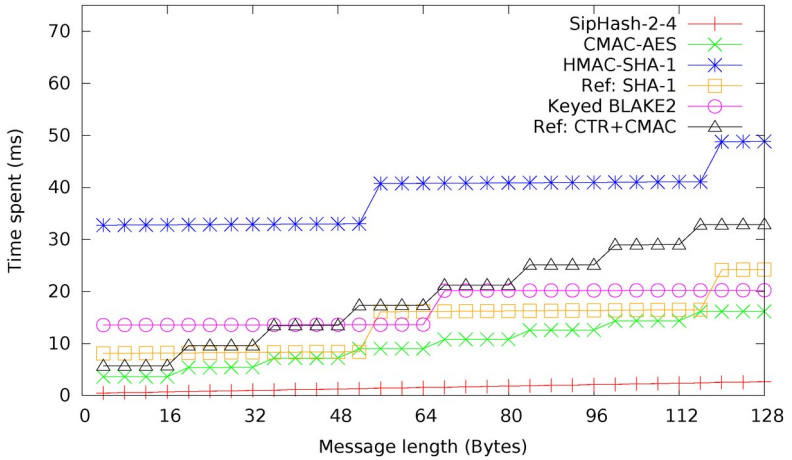
# Cryptography (2)

- RSA too heavy for very low-powered devices
- ECC can be acceptable, but still slow

- Main focus on symmetric cryptography:
  - AES128 can perform well even on 8bit micro-controllers
  - Block cipher based MACs
  - SipHash (but is short)
  - SHA family comparatively slow

- Issue: Shared keys




https://www.mdpi.com/1424-8220/15/8/19560/htm

# Privacy

- Complex topic
- Requires:
  - Secure implementations
  - Additional care take to:
    - Minimize personal data being stored/processed
    - Where possible, process locally
    - Where necessary, store encrypted
    - Trust considerations

# Questions?