Ad-hoc Security for the Internet of Things (Project No. 2,3,4)

Christian Zenger, Prof. Christof Paar
HGI, Ruhr-Universität Bochum
PHYSEC GmbH
AI-Studienprojekt, 20. Januar 2017
HGI @ Ruhr Universität Bochum

• one of Europe’s largest security research centers

• founded in 2002

• 17 research groups / professors

• 100+ scientific staff

• 600 students in IT-security

• 4 M.Sc./B.Sc. programs
PHYSEC at a Glance

• PHYSEC is an **HGI spin-off !!!**

• World leading hackers, engineers and researchers in **security and cryptography**

• USP: Making resource-constrained devices **post-quantum resistant**

• Management:

**PHYSEC GmbH**
Universitätsstr. 150
D-44801 Bochum

+49 234 32 23158
www.physec.de
info@physec.de
FATTYPANTS IS KIDDING HIMSELF IF HE THINKS HE’S EATING LESS THAN 2000 CALORIES A DAY!

AT LEAST YOU GET USED! I NEVER DO! ALL HE EATS IS TAKE-OUT!

HE SPENT A FORTUNE ON US SMARTBULBS AND HE ONLY USES THE “WHITE LIGHT” SETTING! *SIGH*

DID YOU SEE WHAT TIME HE GOT IN LAST NIGHT? SCANDALOUS!

I REFUSE TO PICK UP THIS FRENCH FRY. LAZYBONES CAN DO IT HIMSELF!

DUMMY NEEDS TO TEST ME NOW AND THEN, OR AT LEAST CHECK MY APP!

DON’T BOTHER HIM! THE PREVIOUS SMOKE DETECTOR, HE BEAT TO DEATH WITH A BROOM HANDLE!!

HEY GUYS! THE HOUSE SMARTMETER IS TELLING EVERYONE THAT SCAREDY CAT STILL USES A NIGHT LIGHT! HA HA!

What your Internet of Things is saying about you...
Wie etabliert man sichere Verbindungen?
**IoT-Security 3. Generation**

1. **Generation**
   Hard-coded, factory default, or easy-to-guess passwords

2. **Generation**
   Trust-third party, PKI, CA, Certificated,
   Extremely complex (always)

3. **Generation**
   Ad-hoc Security
   Extremely simple (new)

---

Ransomware (2015)

---

Christian Zenger | Ruhr-Universität Bochum/PHYSEC GmbH | Harvard University | Radiowave-based Virtual Proofs of Reality | 20.01.2017
Gen. 2 vs. Gen. 3

Gen. 2: PKI-Classic

Certificate Signing Request

Production

Certificate Signing Request

Key Management

IoT Platform

Gen. 3: Ad-hoc

Production

IoT Platform

Key Management

Certificate Signing Request
Your job in this Project

- Get used to the IoT-platform
- Understand key management
- Extract certificates or token
- Implement a nice use-case

- Get used to the hardware platform
- Understand REST/HTTP
- Implement certificates or token
3 Projects available

No. 1: AWS IoT

No. 2: SAP HANA

No. 3: KRITIS

Key Management