PHYSEC: The key technology for the IoT

Internet Security Days
17.09.2015, Bruehl

Benedikt Driessen, Heiko Koepke, Christian Zenger

Background

Dr.-Ing. Benedikt Driessen
Security Expert

M.Sc. Christian Zenger
Leader and inventor

Prof. Dr.-Ing. Christof Paar
Mentor and experienced founder

Dipl.-Ök. Heiko Koepke
Economist

Background

Dr.-Ing. Benedikt Driessen
Security Expert

M.Sc. Christian Zenger
Leader and inventor

Prof. Dr.-Ing. Christof Paar
Mentor and experienced founder

Dipl.-Ök. Heiko Koepke
Economist

BMWi "EXIST Forschungstransfer"

- October 2015 – March 2017
- Total funding: **650.000 €**
- Goal: Product

Bundesministerium
für Wirtschaft
und Energie

eXIST
Existenzgründungen
aus der Wissenschaft

Background

Dr.-Ing. Benedikt Driessen
Security Expert

M.Sc. Christian Zenger
Leader and inventor

Prof. Dr.-Ing. Christof Paar
Mentor and experienced founder

Dipl.-Ök. Heiko Koepke
Economist

BMWi “EXIST Forschungstransfer”

- October 2015 – March 2017
- Total funding: **650.000 €**
- Goal: Product

Bundesministerium
für Wirtschaft
und Energie

eXIST
Existenzgründungen
aus der Wissenschaft

BMBF project “PROPHYLAXE”

- March 2013 – August 2015
- Total funding: **3,5 Mio.**
- First demonstrator

BOSCH

hgi
Horst Görtz Institute
for IT-Security

escrypt
Embedded Security

Fraunhofer
Heinrich Hertz Institute

RUB
DKS

Technische Universität
Kaiserslautern

Technische
Universität
Dresden

Summary

Mission of PHYSEC: *Simple and strong protection of data for „smart home", „industry 4.0" and the „internet of things"*

- ○ Sensors and actuators in the „internet of things" measure and influence our daily lives
- ○ Protection of data via cryptography requires trust in cryptographic keys
- ○ Our technology solves this key problem for wirelessly communicating embedded devices

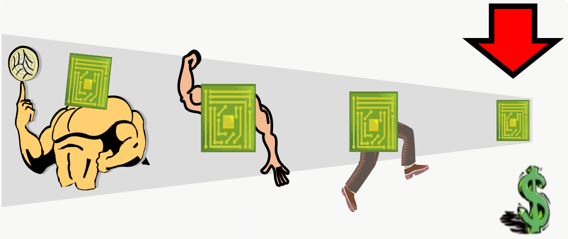
Challenges for the security of communication links in the IoT

Challenges for IoT security

3.4×10^{38}

Huge number of things

Challenges for IoT security

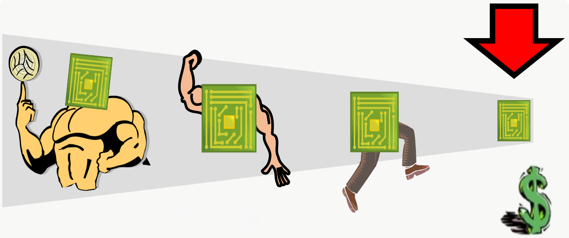


Resource-constrained

3.4×10^{38}

Huge number of things

Challenges for IoT security



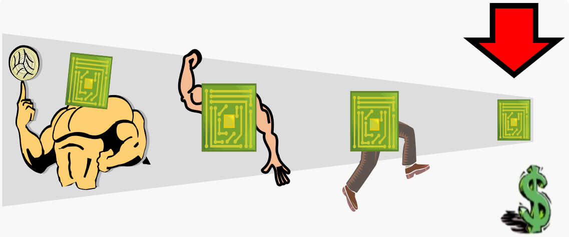
Resource-constrained

3.4×10^{38}

Huge number of things

Energy-constrained

Challenges for IoT security



Resource-constrained

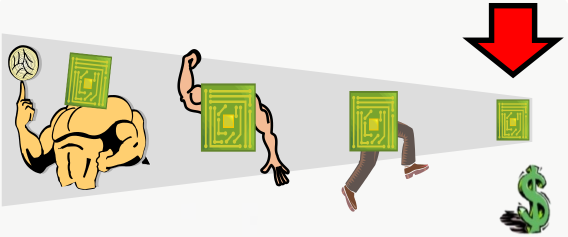
3.4×10^{38}

Huge number of things

No comfortable user interface

Energy-constrained

Challenges for IoT security



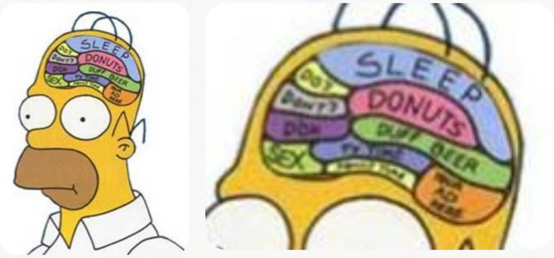
Resource-constrained

3.4×10^{38}

Huge number of things

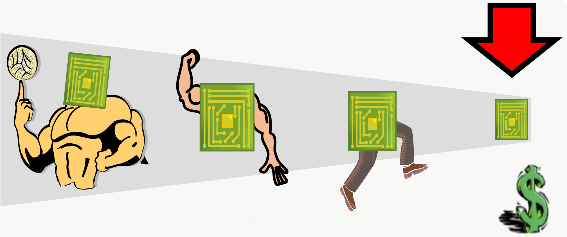
No comfortable user interface

Energy-constrained



And the worst… users!

Challenges for IoT security



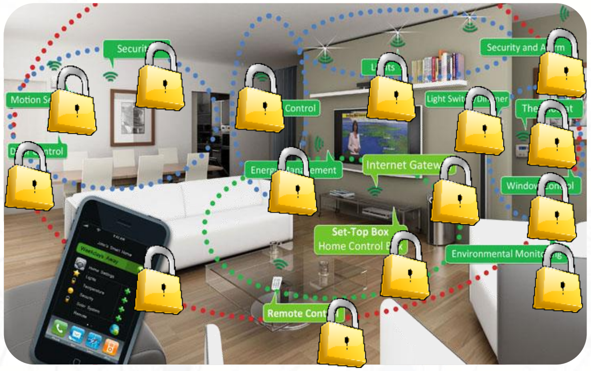
Resource-constrained

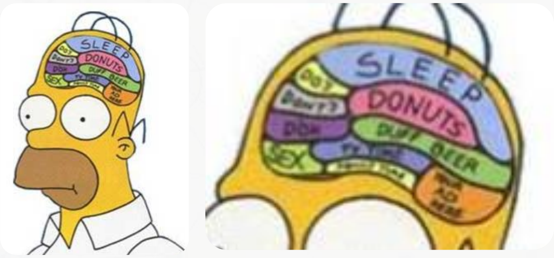
3.4×10^{38}

Huge number of things

No comfortable user interface

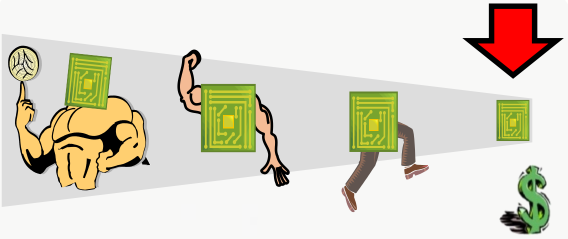
Energy-constrained





And the worst… users!

Challenges for IoT security



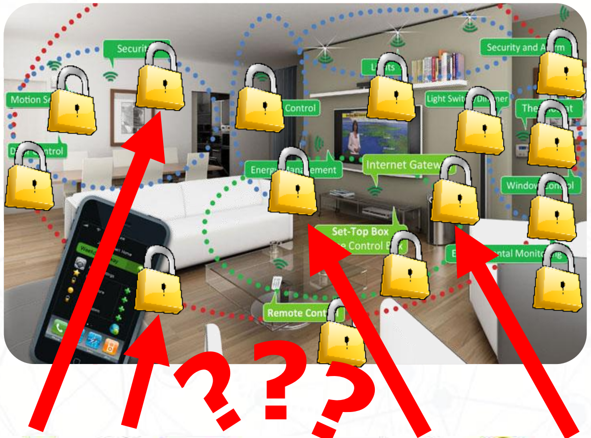
Resource-constrained

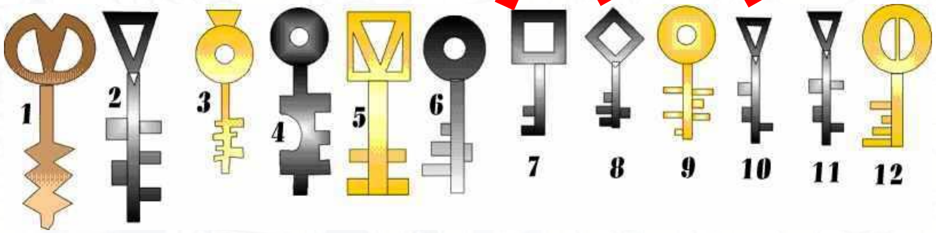
3.4×10^{38}

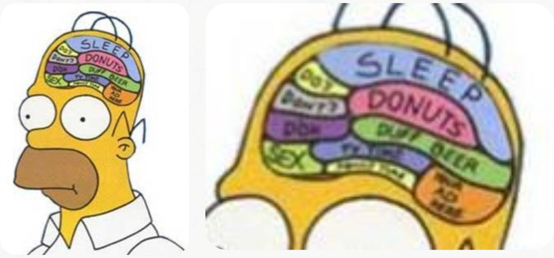
Huge number of things

No comfortable user interface

Energy-constrained

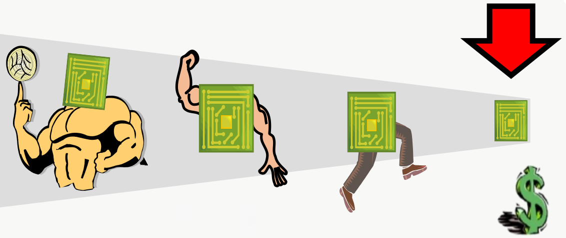




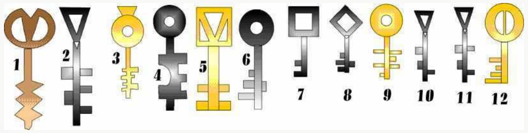


And the worst… users!

Challenges for IoT security



Resource-constrained

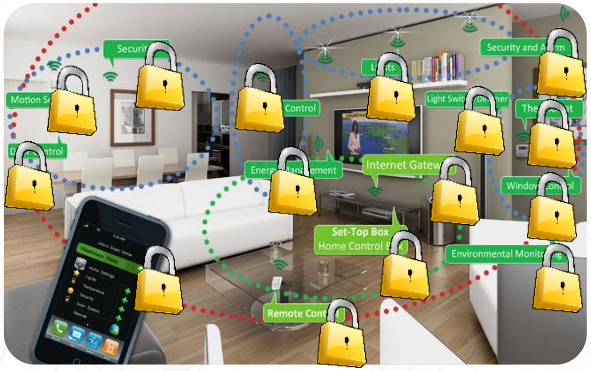


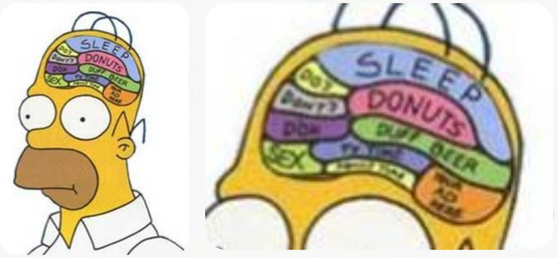
3.4×10^{38}

Huge number of things and keys

No comfortable user interface

Energy-constrained



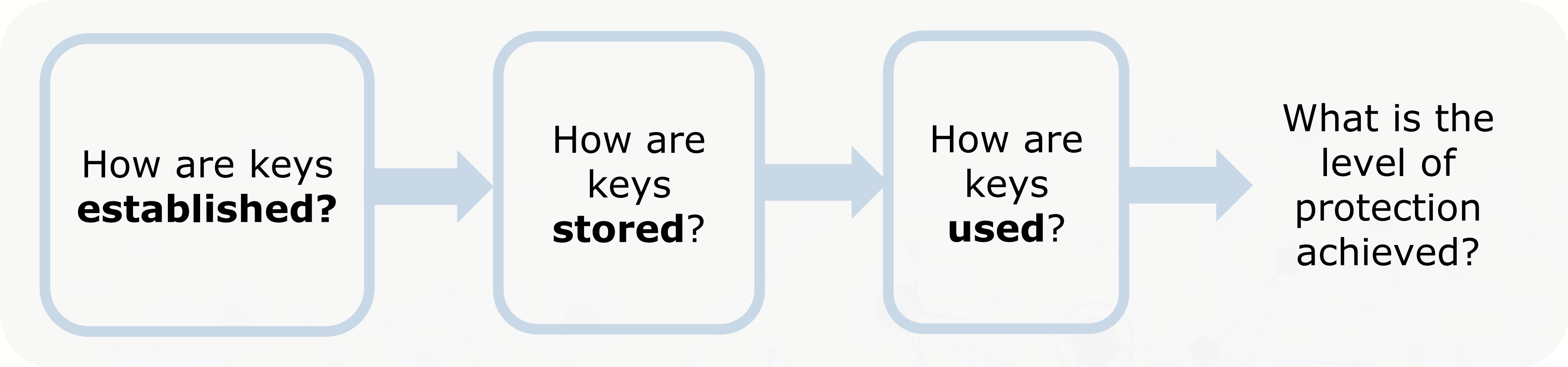


And the worst… users!

- ○ Easy-to-use and cost-efficient security is required
- ○ Conventional approaches have serious shortcomings

Cryptographic keys as trust anchor

Keys as trust anchor



How are keys **established?**

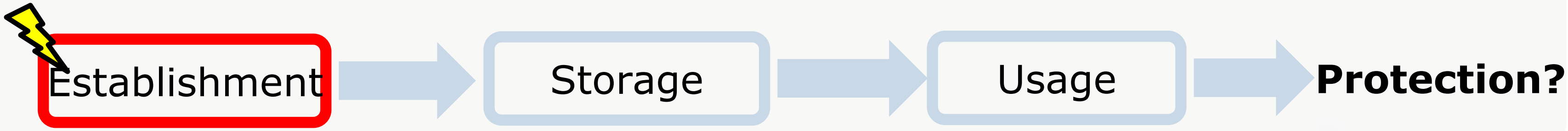
How are keys **stored**?

How are keys **used**?

What is the level of protection achieved?

- Trust in a cryptographic system starts with trust in the cryptographic key(s)
- Protection is the result of correct establishment, storage and usage

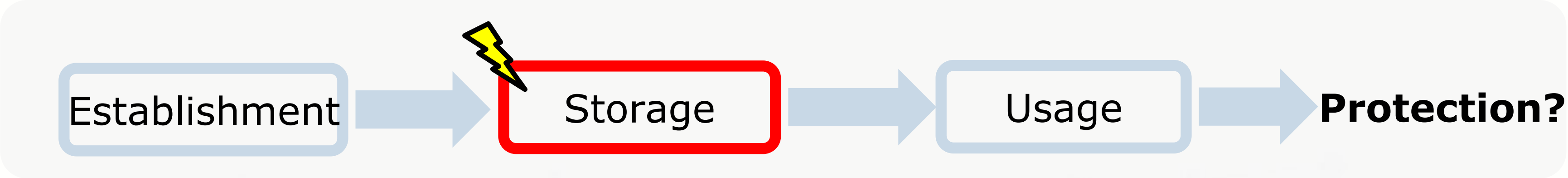
Challenges for the secure establishment of keys



- Programming of keys during manufacturing
  - Most simple form of key management
  - Manufacturing processes have to be secured
  - Attacks scale extremely good
  - No flexibility in case of attack

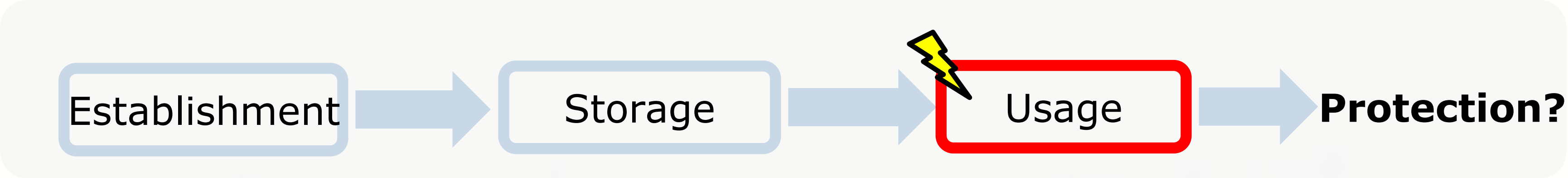
- Dynamic key management (e.g., based on a PKI)
  - More flexibility
  - High complexity in implementation and infrastructure
  - Higher resource usage on devices
  - High cost for infrastructure of HSMs and servers

Challenges for the secure storage of keys



- Obfuscation of stored keys and software-based approaches typically fail
- Security hardware can significantly harden a system against attacks
  - Increased cost
  - Increased complexity and integration efforts

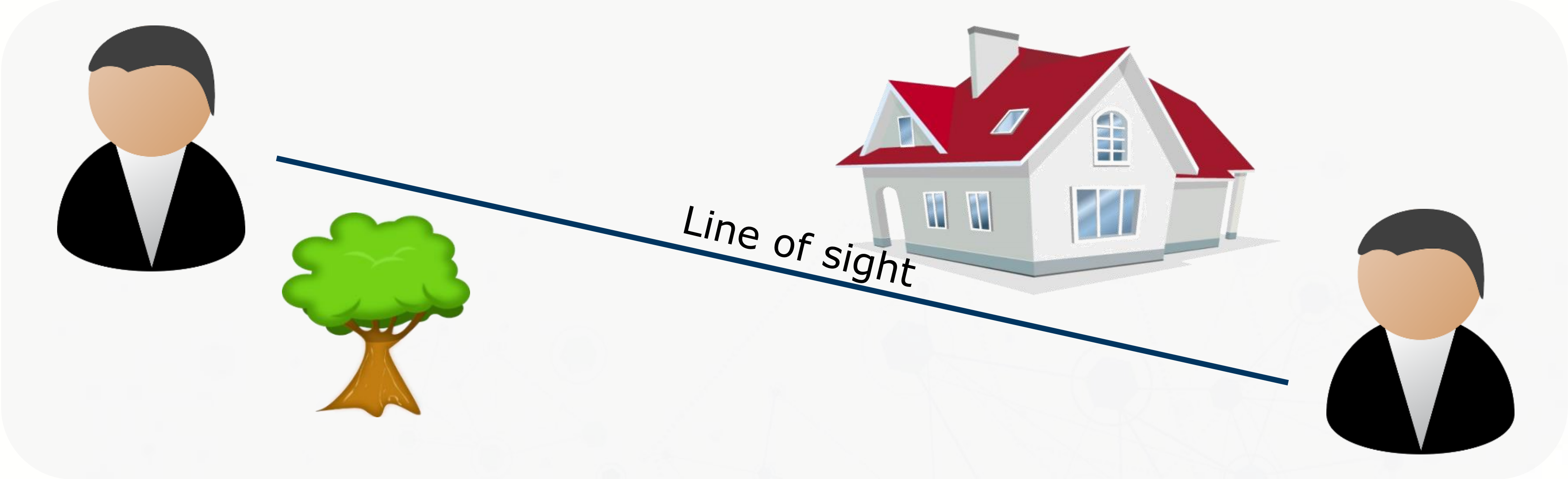
Challenges for the secure usage of keys



- Attacks against cryptographic implementations are standard
  - Attacks are complex but effective
  - Countermeasures exist but require deep expertise
- Techniques for attacks against crypto algorithms get better every day
  - Choice of algorithms not always easy
  - Proprietory algorithms are in danger

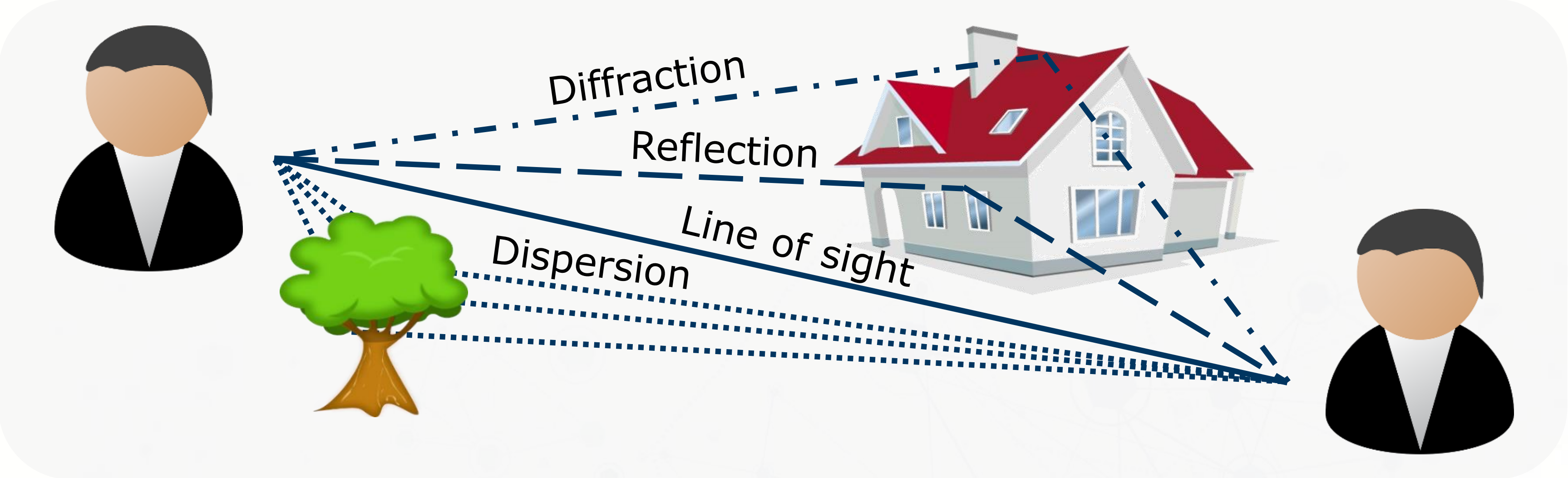
The basic idea

Idea: Evaluate the wireless channel (1/3)



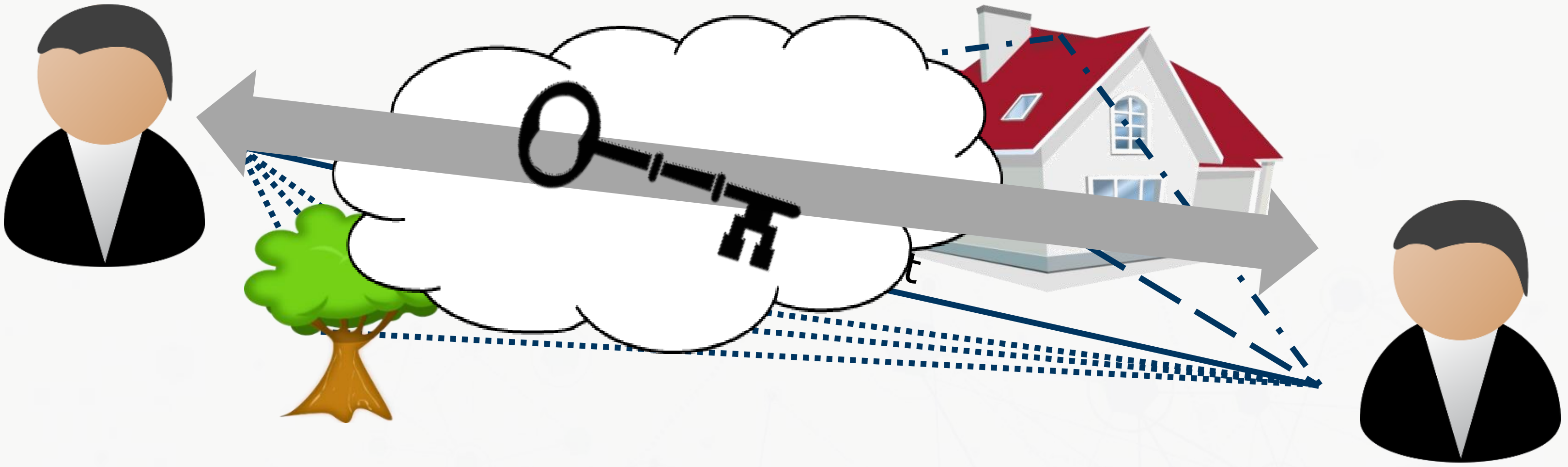
- Alice and Bob communicate via a wireless channel
- A channel has properties that can be measured
  - If Alice and Bob measure simultanously, the measurements will be correlated

Idea: Evaluate the wireless channel (2/3)



- Wireless signals do not only propagate along the line of sight
- Diffraction, reflection and dispersion are dependent on the surroundings and thus highly variable
  - High entropy of measurements

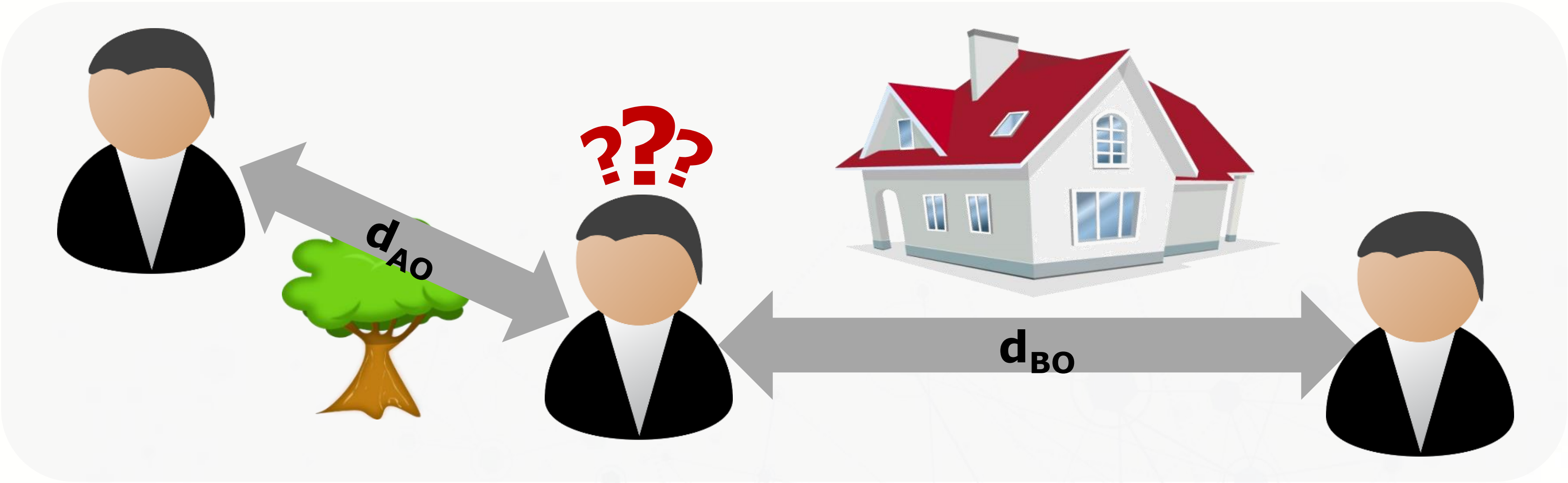
Idea: Evaluate the wireless channel (2/3)



○ Wireless signals do not only propagate along the line of sight

○ Diffraction, reflection and dispersion are dependent on the surroundings and thus highly variable
   – High entropy of measurements

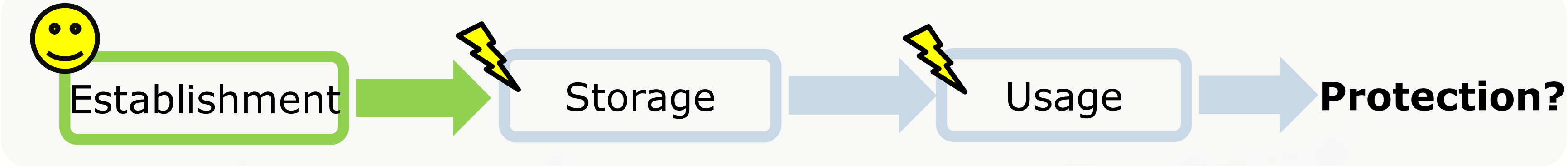
Idea: Evaluate the wireless channel (3/3)



- Measurements decorrelate quickly
  - Depends on surroundings and frequency
  - WiFi at 2.4GHz: d_{AO} > 7cm, d_{BO} > 7 cm

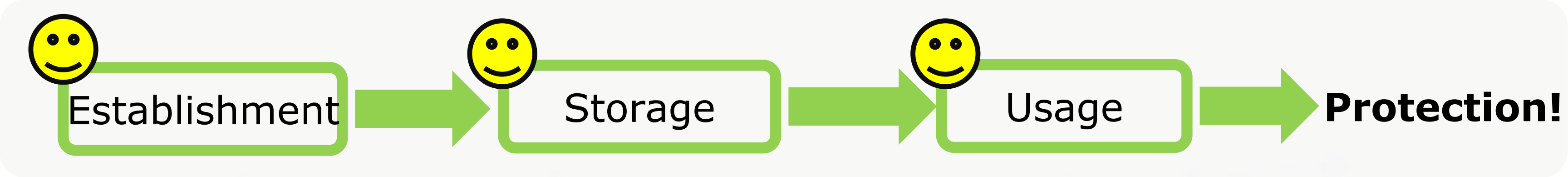
Applications and benefits

Principle 1: Authentication through proximity



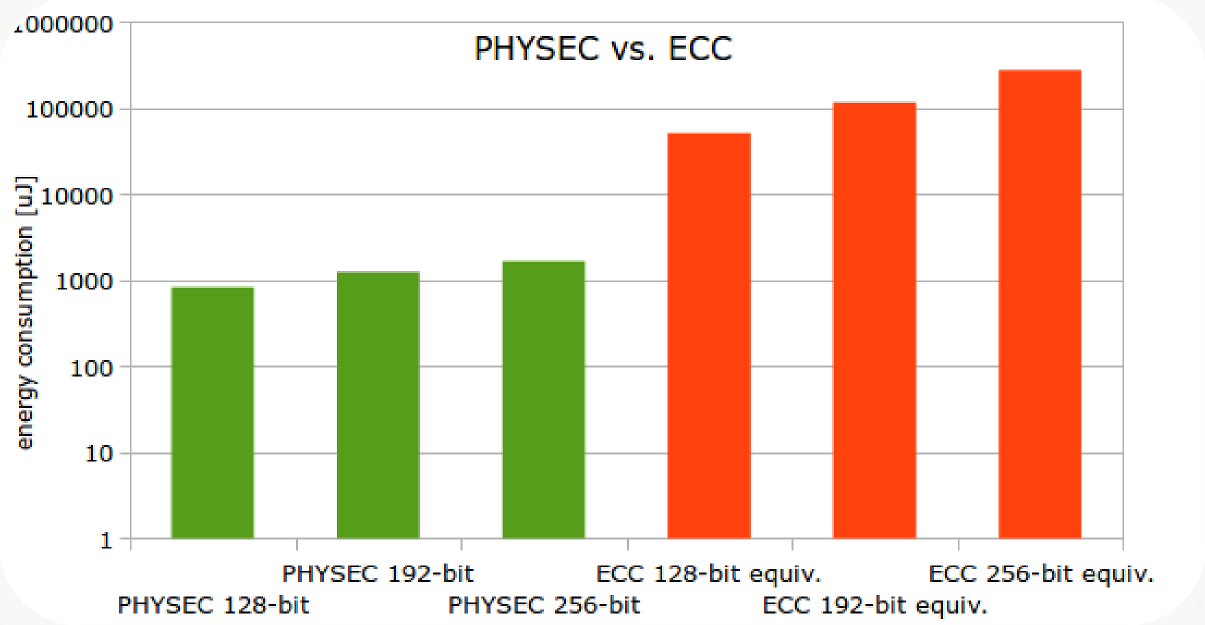
- Establishment of keys between gateway and sensors with the help of a trusted authenticator device (e.g., smartphone)
- Transfer of trust by placing authenticator next to new device
  - Proximity implies correlated measurements

Principle 2: Key (re-)generation



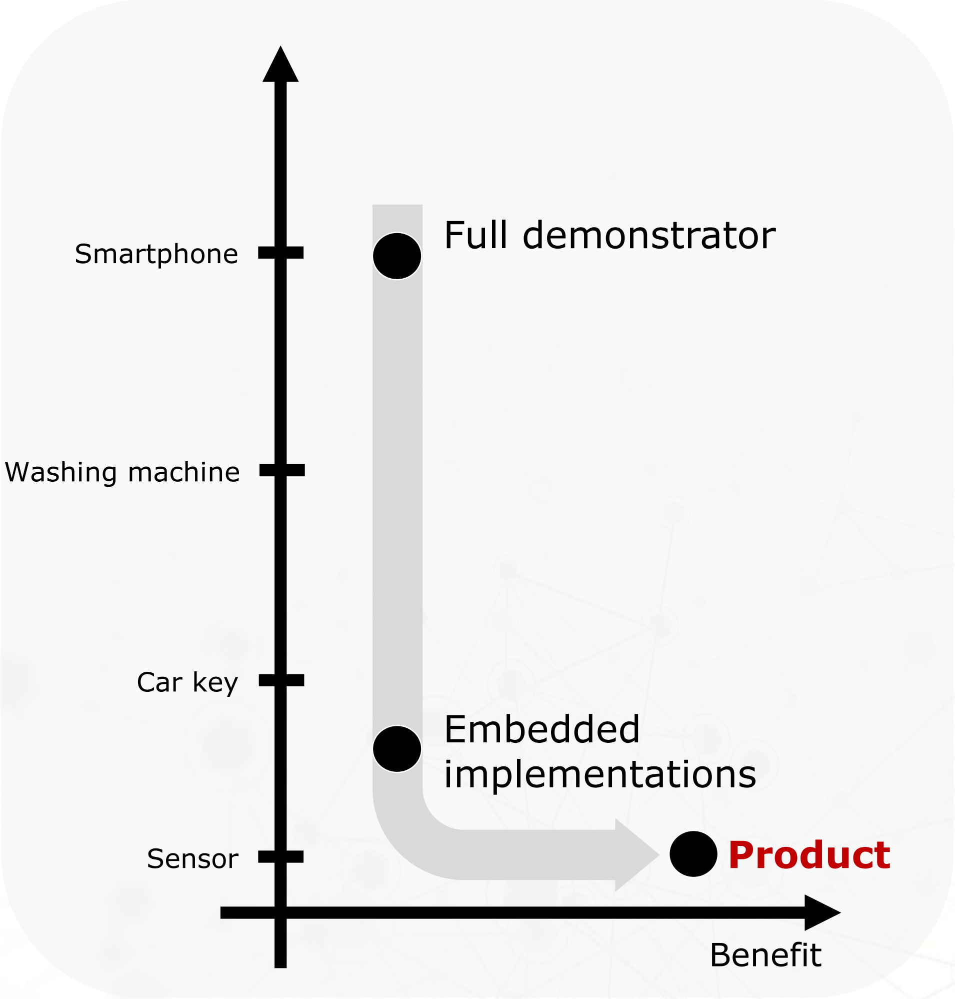
- Cryptographic keys derived from channel
- Continuously changing keys
  - Every communication produces new measurements
- Attacks on storage and usage of keys less attractive and effective
  - Individual keys make attacks unscalable
  - Keys only used for a limited period
  - Statistical attacks require huge amounts of data with same key

High security for low energy



- PHYSEC requires between one and two orders of magnitude less energy than ECC
  - Alle klassische Verfahren brauchen zudem zusätzlich einen guten RNG

Status and perspective



- ○ Fully functional demonstrator
  - – 700Mhz ARM
  - – WLAN IEEE 802.11n, 2.4 GHz
  - – Modification of OS kernel
- ○ Further implementations
  - – ARM Cortex M3 (32 bit)
  - – MSP 430 (16 bit)
  - – Intel 8051 (8 bit)

Conclusion

- ○ Advantages of the technology
  - Saves energy and thus ideal for embedded devices
  - High security without need for further measures
  - Intuitive usage for end customer
- ○ **PHYSEC is looking for collaboration partners**
  - Use cases
  - Prototypical integration

Bundesministerium
für Wirtschaft
und Energie

eXIST
Existenzgründungen
aus der Wissenschaft

BOSCH

escrypt
Embedded Security

Fraunhofer
Heinrich Hertz Institute

RUB
DKS

TECHNISCHE
UNIVERSITÄT
DRESDEN

TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN