PADERBORN IT-FLASH #3

SECURITY RISK SMART HOME

HOLGER FUNKE

SPYING 1.0

Source: The Lives of Others

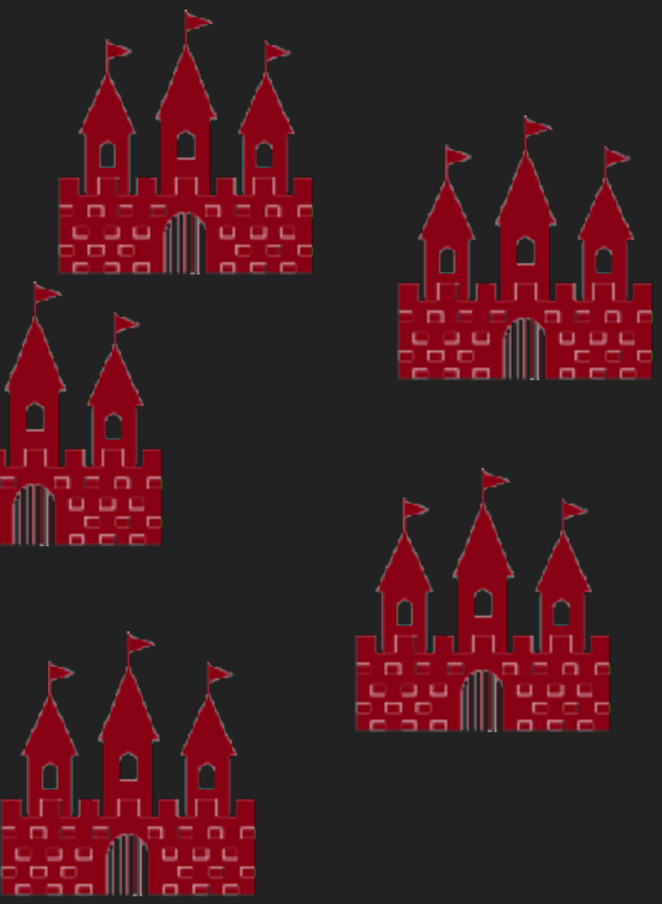
SMART HOME REQUIREMENTS

- Comfort, Compatibility, Availability
- Protection against unauthorized use
- Protection of privacy

Source: Huffington Post

SITUATION: SEVERAL ISOLATED PROTOCOLS

- Cable:
  - KNX, LAN, Power Line
- Wireless:
  - KNX-RF, FS-20
  - WiFi, Dect, Bluetooth (Low Energy)
  - ZigBee, Z-Wave
  - Homematic (BidCoS), RWE
  - *EnOcean*



ENOCEAN IN A NUTSHELL

- Energy Harvesting (no batteries)
- Short, uni- or bidirectional radio messages
- Frequency: 868 MHz
  - Limitation in Germany: sending 36 sec / hour
- International standard: ISO/IEC 14543-3-10
- Several vendors using EnOcean components:
  - actors, sensors, integration in e.g. openHAB

ENOCEAN TELEGRAMS

- Payload of a telegram: 14 bytes (plus Chaining)
- Header, Data, CRC
- Unique ID (MAC-address)
- EnOcean Equipment Profiles
- Rolling Code available

Sync Byte		1 Byte
Header	Data Length	2 Bytes
	Optional Length	1 Byte
	Packet Type	1 Byte
CRC8 Header		1 Byte
Data		1...n Bytes
Optional Data		0...n Bytes
CRC8 Data		1 Byte

Source: blog.protocolbench.org

PASSIVE ATTACK ON ENOCEAN TELEGRAMS

- Idea: Log telegrams to collect data of Smart Home
- Raspberry Pi with Power Bank or WakaWaka
- EnOcean Stick (USB300) or SoC TRX 8051
- Software to log telegrams, e.g. EnOceanSpy (github)
- Format collected data as graph
  - Who communicates with which device?
  - Who sends which information?
- EnOcean Specification, Software: freely available

DEMO
PASSIVE ATTACK

ACTIVE ATTACK: CAPTURE & REPLAY

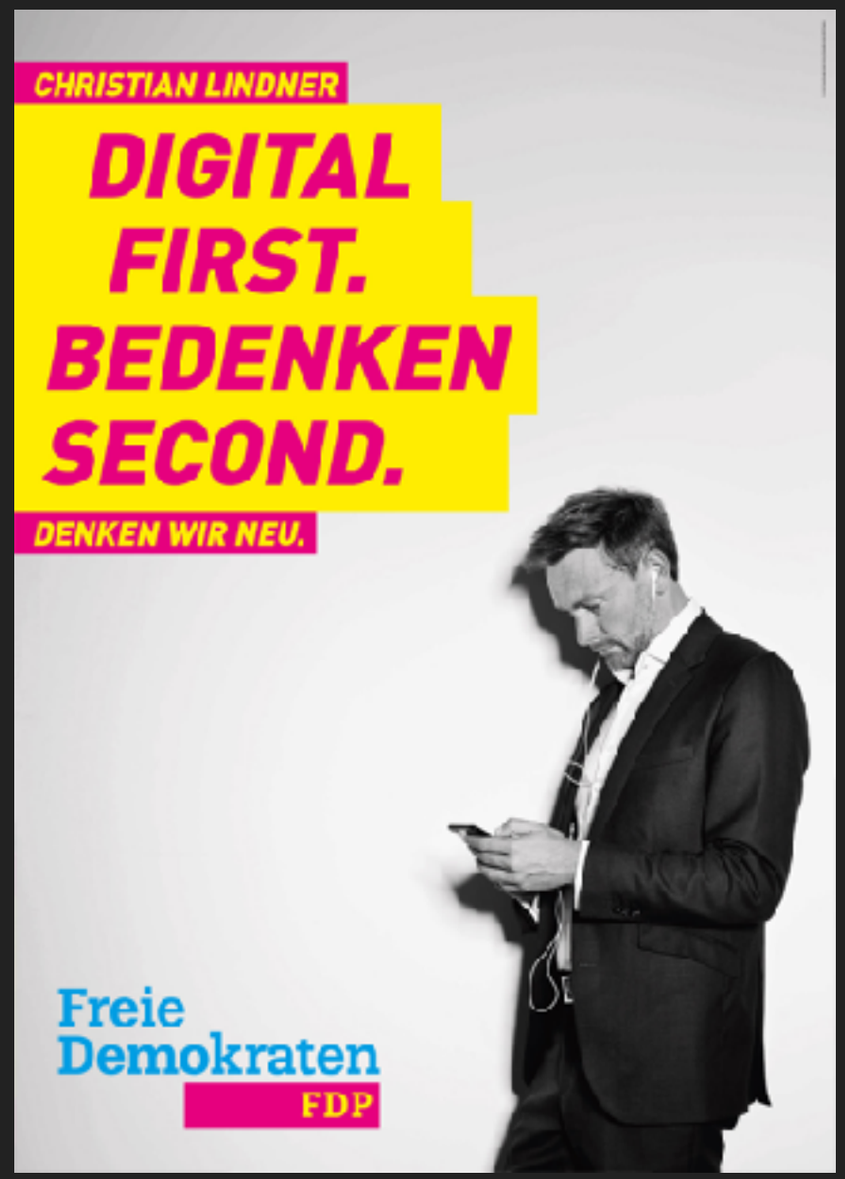
- Problem: Activator and sensor are linked
- Activator expects ID of device (sender)
- Solution 1: USB310 can change the MAC address
- Solution 2: Capture & Replay Attack
  - Software Defined Radio (SDR) tools: HackRF One
  - Capture complete telegram including ID and replay telegram

DEMO
C&R ATTACK

SPYING 2.0

- Profile of resident can be set up automatically
  - cheap hardware, no detection
- Easy to overtake and manipulate complete Smart Home

That’s not a good idea:



HOW TO PROTECT YOUR SMART HOME

- Use encryption of messages (EnOcean: Rolling Code)
  - Storing keys, RNG, Firmware Updates, Personalization
    - Smart Cards?
- Send dummy messages to confuse
- The less data the better!

THANKS FOR YOUR PATIENCE

QUESTIONS?

- Contact:

  Holger Funke

  blog.protocolbench.org

  twitter.com/holgerfunke