



Dieses Projekt wird aus Mitteln des  
Fonds für die Innere Sicherheit der  
Europäischen Union kofinanziert

EMERGE 



# EMERGE IoT – Herausforderungen für die Polizeiarbeit

# Gliederung

1. Das Internet der Dinge –  
Polizeiliche Fragestellungen
2. Das Projekt Emerge IoT
  - Projektziele
  - Stand des bisher Erreichten



Quelle: <https://www.derbrutkasten.com/smart-home-smart-assistants/>

# Was ist das „Internet der Dinge“?

„Internet der Dinge“ (engl.: Internet of Things, IoT)

- Teil der Vision eines allgegenwärtigen Computereinsatzes („*Ubiquitous Computing*“)
- Verknüpfung eindeutig identifizierbarer, physischer Objekte („*things*“) mit einer virtuellen Repräsentation innerhalb des Internets
- M-2-M – Kommunikation (Netzwerk von Sensoren und Aktuatoren)
- Aufgabe: Relevante Daten erfassen, verdichten und Informationen bereitstellen
- Einsatzgebiete
  - Gebäudesteuerung/Hausautomatisierung
  - Car-2-Car Kommunikation
  - Intelligente Fabrik („Industrie 4.0“)
  - ...



Quelle: <https://www.elektroniknet.de/>

# Überblick Gebäudeautomatisierung



Quelle: <https://www.notebookcheck.com/Smart-Home-Produkte-im-Trend-grosse-Kundenzufriedenheit.259484.o.html>

# Polizeiliche Fragestellungen - Risiken

- Angriffe auf das IoT-Netzwerk selbst
  - Informationsdiebstahl
  - Zerstörung von Infrastruktur
  - Angriff auf Leib und Leben
  - Kompromittieren der Nutzer/Organisation
- Angriffe mit Hilfe gekaperteter IoT-Netzwerke
  - Bot-Netze
  - Bitcoin-Mining



Quelle: Tumiso, pixabay.com



Quelle: Adtel Integration, <http://AdtelIntegration.com/smart-cities-infrastructure/>

# Polizeiliche Fragestellungen - Chancen

- Aktive und präventive Strafverfolgung
  - IoT als Beweismittel, z.B. durch Auswertung von Bewegungsprofilen
- Gefahrenabwehr
  - Lahmlegen von Steuerungselementen vor Zugriffen
  - Abwehr terroristischer Bedrohungen



Quelle: Tumiso, pixabay.com



Quelle: Alexs\_Fotos, pixabay.com

Wer und wo sind die Täter in einer vernetzten Umgebung?



Quelle: Adtel Integration, <http://Adtelintegration.com/smart-cities-infrastructure/>

# EMERGE IoT – Das Projekt



Projektbeteiligte (Landeskriminalamt MV)

- Jens Krüger
- Stephan Palm
- Dr.-Ing. Enrico Seib



Universität  
Rostock



Traditio et Innovatio

Projektbeteiligte (Universität Rostock)

- Dr.-Ing. Thomas Mundt
- Johann Bauer

Quellen: Dr. Anna Lewerenz, LKA M-V; ITMZ, Universität Rostock



Dieses Projekt wird aus Mitteln des Fonds für die Innere Sicherheit der Europäischen Union kofinanziert.

Der Förderzeitraum läuft von 2018 – 2021.  
Förderbetrag 1,2 Millionen Euro

## Projektbeirat

- Prof. Dr. Clemens Cap (Universität Rostock)
- Sybille Hofmann (LKA M-V)
- Prof. Dr. Nicholas H. Müller (Hochschule WS)
- Prof. Dr. Paul Rosenthal (Universität Rostock)

**EMERGE IoT** steht für **E**ntwicklung von Kompetenzen, **M**ethoden und Werkzeugen für zukunftsorientierte **E**rmittlungen und **E**rmittlungsunterstützung im „Internet of Things“. ([www.emerge-iot.de](http://www.emerge-iot.de))

# Projektziele EmERGE IoT

Entwicklung von Kompetenzen, **M**ethoden und Werkzeugen für zukunftsorientierte **E**rmittlungen und **E**rmittlungsunterstützung im „Internet **of Things**“.

- Identifizierung und Analyse der technischen Grundlagen des IoT
- Entwicklung und Überprüfung von polizeilich relevanten IoT-Angriffsszenarien
- Vermittlung von Wissen über das Phänomen IoT an die Strafverfolgungsbehörden
- Entwicklung von Werkzeugen zum Erkennen und Analysieren von Angriffen

# Identifizierung, Analyse und Sensibilisierung

- Aufbau einer Wissensbasis zu IoT-Protokollen und Sicherheitslücken  
→ siehe Wiki [emerge.lka-mv.de](https://www.emerge.lka-mv.de)
- Durchführung von Workshops und Präsentationen
  - Bisher drei Workshops (intern und extern mit Beteiligung versch. LKÄ, BKA, Zoll, Stand August 2020)
  - Beitrag Jahrestagung Sicherheitskooperation Cybercrime (Stuttgart im September 2019)
  - LKA-interne Präsentationen für Ermittler und Staatsanwaltschaften
  - Weitere öffentliche Auftritte bereits terminiert (z.B. beim 25. Deutschen Präventionstag im September 2020 in Kassel)
- Aus- und Weiterbildung von Polizeivollzugsbeamten i. Zus. m. FHöVPR Güstrow

# Projektziele EmERGE IoT

Entwicklung von Kompetenzen, **M**ethoden und Werkzeugen für zukunftsorientierte **E**rmittlungen und **E**rmittlungsunterstützung im „Internet **of Things**“.

- Identifizierung und Analyse der technischen Grundlagen des IoT
- **Entwicklung und Überprüfung von polizeilich relevanten IoT-Angriffsszenarien**
- Vermittlung von Wissen über das Phänomen IoT an die Strafverfolgungsbehörden
- **Entwicklung von Werkzeugen zum Erkennen und Analysieren von Angriffen**

# Erarbeitung möglicher Angriffsszenarien

- Angriffe auf Verfügbarkeit der Dienste und auf IoT-Steuerungseinheiten ((D)DoS-Attacke)
  - Angriff via Webschnittstelle auf lokale IoT-Steuerungseinheit mittels HTTP/HTTPS
  - Angriff auf Netzwerkebene (TCP/IP)
  - Angriff aus dem lokalen IoT-Netzwerk heraus
- Angriffe auf Vertraulichkeit der Kommunikationsdaten
  - Mitschneiden der Kommunikationsdaten
  - Einschleusen eines manipulierten Gerätes
- Physisches Auslesen von Informationen (*Chip Off*)



Source: kalhh-86169, pixabay.com

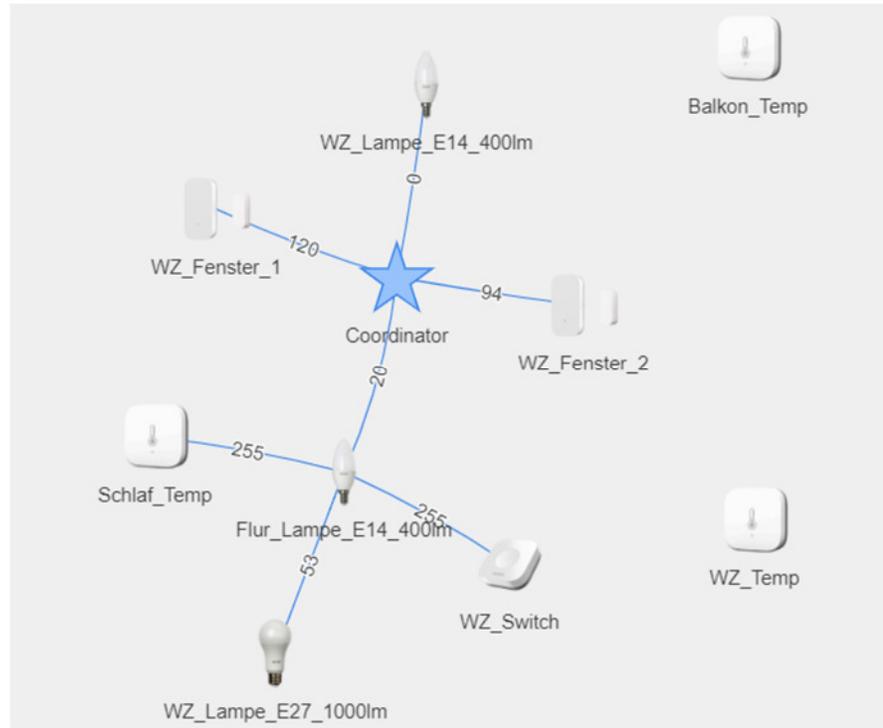
# Einschub: ZigBee - Kurzübersicht

- Verbreitetes Kommunikationsprotokoll für IoT im Frequenzbereich von 2,4 GHz (Kanäle 11 bis 26) sowie 868 MHz und 915 MHz für bis zu 100 m bzw. nahezu unbegrenzter Reichweite bei Vermaschung
- Offener Standard, verwaltet von der „ZigBee Alliance“
  - Vielzahl namhafter Hersteller (über 230 Unternehmen, darunter Philips, Osram, HomeMatic, Ikea...), gleiche Basis mit unterschiedlicher konkreter Programmierung
- ZigBee-Netzwerk besteht aus einem *Coordinator*, einer Vielzahl von *Devices* und *Routern*
- Steuerung der Funktionalität der Geräte im ZigBee-Netzwerk via Schnittstelle
  - i.d.R. (Web- | Mobile-) App



Quelle: <https://www.pcworld.com/article/2849172/zigbee-30-promises-one-standard-for-many-uses.html>

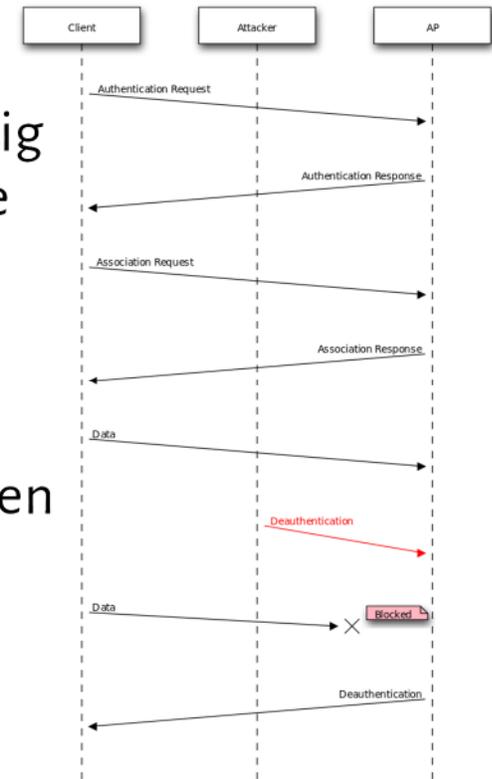
# Einschub: ZigBee - Netzwerk



Quelle: <https://forum.iobroker.net/topic/13384/aufruf-zigbee-cc253x-adapter/727>

# Beispiel 1: Deauthentifizierungsangriff via WLAN

- Das WiFi-Protokoll IEEE 802.11 bietet standardmäßig ein sog. “Deauthentication Frame”, mit dem Geräte explizit vom Netzwerk getrennt werden können
- Arbeitet nur unidirektional
- Ein Angreifer kann ein Deauthentifizierungspaket zu jedem Zeitpunkt an ein Gerät im Netzwerk senden
- Keine Verschlüsselung notwendig



Quelle: [https://en.wikipedia.org/wiki/Wi-Fi\\_deauthentication\\_attack](https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack)

# Deauthentication Attack (WiFi)

Hausautomatisierungszentrale Homee/WiFi-Geräte:

- Zentrale: Homee Brain-Cube mit ZigBee-Cube (ca. 200 €)
- Smart TV Sony KDL (ca. 800 €)
- Smart Radio Marantz CR 511 (ca. 500 €)

Angriffswerkzeug:

- *Aircrack-ng* suite (mitgeliefert bei Kali-Linux (kostenfrei))
- Laptop mit Kali-Linux (kostenlos außer Hardware)

Sniffing-Ausstattung:

- Raspberry-Pi 3B+ mit Raspbee-Modul, tragbarer Monitor etc. (ca. 200 €)
- Wireshark für Netzwerkanalyse (kostenfrei)



Quellen: amazon.de

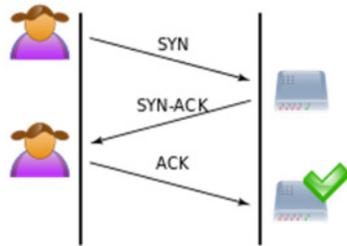


Quelle: wireshark.org

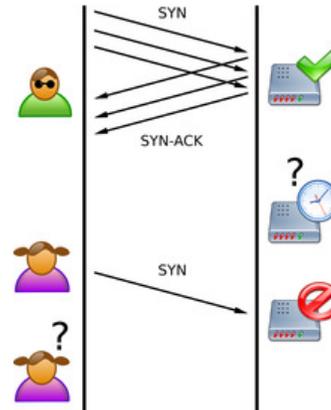


# Beispiel 2: DoS-Attacke auf ZigBee-Coordinator

**Idee:** Gerät wird mit Synchronize-Anfragen (HTTP/HTTPS) geflutet, der jeweilige Dienst des Gerätes mit dem *Coordinator* überlastet und die Gerätefunktionalität grundlegend beeinträchtigt.



Quelle: Wikipedia ([https://de.wikipedia.org/wiki/SYN-Flood#/media/Datei:Tcp\\_normal.svg](https://de.wikipedia.org/wiki/SYN-Flood#/media/Datei:Tcp_normal.svg))



Quelle: [https://de.wikipedia.org/wiki/SYN-Flood#/media/Datei:Tcp\\_synflood.png](https://de.wikipedia.org/wiki/SYN-Flood#/media/Datei:Tcp_synflood.png)

# Umsetzung einer DoS-Attacke auf den Homee

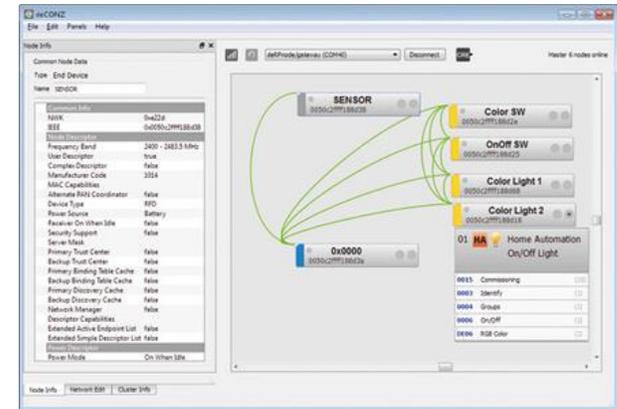
## Versuchsaufbau

### ZigBee-Steuerung:

- Raspberry Pi 3B+ mit Raspbee-Modul, portablem Monitor etc. (ca. 200 €)
- Philips Hue-Geräte (Schalter, LED-Lampen, ca. 100 €)
- DeConz-Steuerungssoftware für ZigBee (kostenlos)

### Angriffswerkzeug:

- Laptop mit Kali-Linux (kostenlos außer Hardware)



Quelle: <http://www.dresden-elektronik.de>



Quelle: <http://www.kali.org>

# Ergebnis einer DoS-Attacke auf den Homee

**DeCONZ-Steuerungssoftware auf dem Raspberry Pi konnte mehrfach verzögert bzw. zum Absturz gebracht werden**

## **ABER**

- Verhalten nicht reproduzierbar
- Verifikation mit fertig konfigurierten („*Out-of-Shelf*“) Geräten noch ausstehend

→ Erste Anhaltspunkte für weitere Angriffsvektoren

# Beispiel 3: Ungesicherte Anmeldung Homee

ZigBee-Haussteuerungsnetz mit „Homee“ als Zentrale

- Homee: Brain Cube mit ZigBee-Aufsatzmodul (ca. 200 €)
- Philips Hue-Geräte (Schalter, LED-Lampen) (ca. 100 €)
- Laptop (vorhanden) zum Aufruf der Steuerungssoftware via Webbrowser



Quelle: amazon.de

Sniffing-Ausstattung

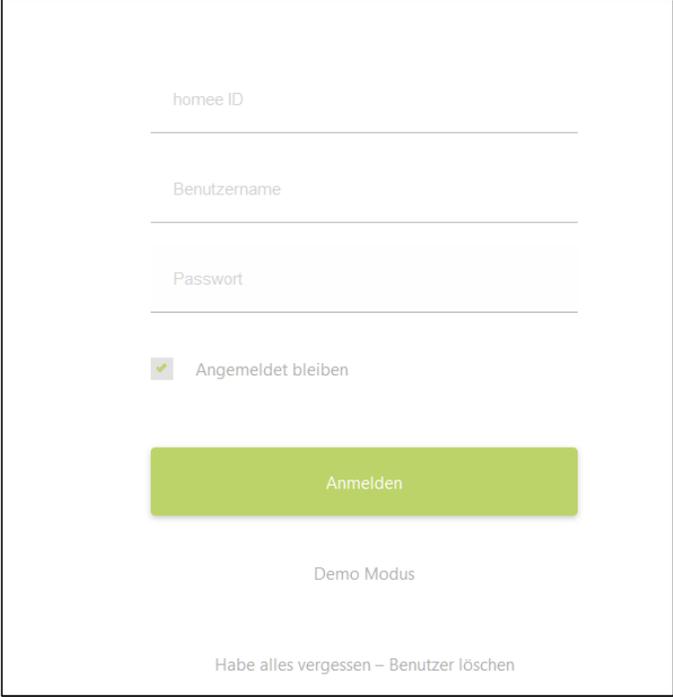
- Wireshark zur Netzwerkanalyse (kostenlos) am Hotspot-PC



Quelle: wireshark.org

# Anmeldung via Web-Frontend

Die Anmeldung am Homee erfolgt via (Web-Fronend oder (Mobile-) App über (lokales) WLAN/Internet und Eingabe von Homee-ID, Benutzername und Passwort



The screenshot displays a login form with the following elements:

- Input field for "homee ID"
- Input field for "Benutzername"
- Input field for "Passwort"
- Checkbox labeled "Angemeldet bleiben" (checked)
- Green button labeled "Anmelden"
- Text "Demo Modus" below the button
- Text "Habe alles vergessen – Benutzer löschen" at the bottom

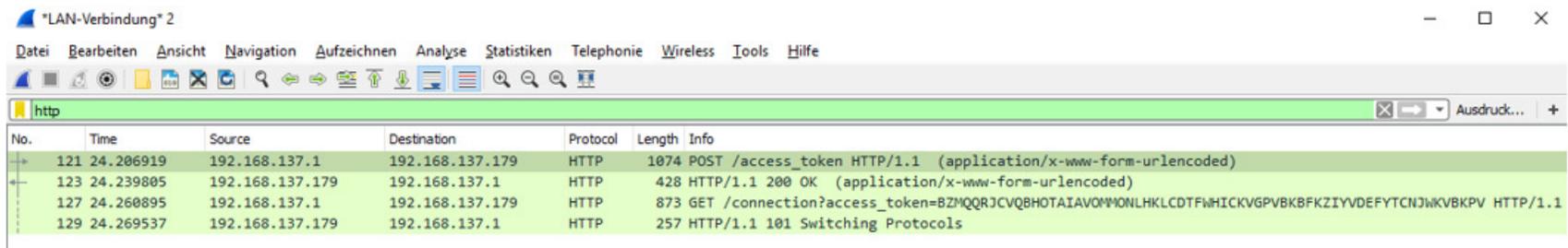
Quelle: Enrico Seib, LKA M-V

# Sichtbarer Netzwerktraffic mit Wireshark

Kommunikation zwischen Homee und Nutzergerät via Homee-(Web-)App nutzt Verschlüsselung (TLS 1.2)

**ABER**

Anmeldung via HTTP-Post



No.	Time	Source	Destination	Protocol	Length	Info
121	24.206919	192.168.137.1	192.168.137.179	HTTP	1074	POST /access_token HTTP/1.1 (application/x-www-form-urlencoded)
123	24.239805	192.168.137.179	192.168.137.1	HTTP	428	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
127	24.260895	192.168.137.1	192.168.137.179	HTTP	873	GET /connection?access_token=BZHQQRJCVQBHOTAIAVOMMONLHKLCDTFW HICKVGPVBKBFKZIYVDFYTCNDJWKBKPV HTTP/1.1
129	24.269537	192.168.137.179	192.168.137.1	HTTP	257	HTTP/1.1 101 Switching Protocols

Quelle: Enrico Seib, LKA M-V

# Übertragung von Nutzernamen und Passwort

```
> Frame 121: 1074 bytes on wire (8592 bits), 1074 bytes captured (8592 bits) on interface 0
> Ethernet II, Src: b6:6b:fc:52:a0:8a (b6:6b:fc:52:a0:8a), Dst: FSElekt_r_11:96:e1 (00:05:51:11:96:e1)
> Internet Protocol Version 4, Src: 192.168.137.1, Dst: 192.168.137.179
> Transmission Control Protocol, Src Port: 1038, Dst Port: 7681, Seq: 1, Ack: 1, Len: 1020
▼ Hypertext Transfer Protocol
  > POST /access_token HTTP/1.1\r\n
  Host: 192.168.137.179:7681\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0\r\n
  Accept: application/json, text/plain, */*\r\n
  Accept-Language: de,en-US;q=0.7,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  ▼ Authorization: Basic ZWllcmdlX2lvdDo4YmFimWE3Y2U1MjNkNmYzNDh0MGF1YTMzNTMyYmNiNGE1MmEwMjdmZTdkYjE1MjI4ZDg2MzQzZjkyYjFjMDRhZTZmNDM0YzY3OTE3MT11MzIzOGZlY2RhNjJjNmQ3ZGEwMmY5NTBhN...
    Credentials: emerge_iot:8bab1a7ce523d6f34040aea33532bcb4a52a027fe7db15228d86343f92b1c04ae6f434c6791719b3238a3cda62c6d7da02f950a709cdc42cab73021a00254a54
  Content-Type: application/x-www-form-urlencoded\r\n
```

Quelle: Enrico Seib, LKA M-V

- Analyse des Datenverkehrs zur Anmeldung mittels Wireshark
- Angaben zur „Authorization“ sind Base64-codiert

Nutzername: „emerge\_iot“

Was folgt nach „emerge\_iot:“?

## sha512 -Hashwert

→ Neuer Ansatzpunkt für Hacker, z.B. Ausprobieren des ermittelten Hashwerts gegenüber bekannter Wertelisten

# Beispiel 4: Mitlesen von ZigBee-Traffic

ZigBee-Netzwerkverkehr ist grundsätzlich verschlüsselt.

## **ABER**

Initiale Verschlüsselung zwischen *Device* und *Coordinator* ist einheitlich, um Einbindung neuer Geräte zu ermöglichen.

**Dieser Schlüssel ist veröffentlicht worden!**

Dient als Einfallstor für Hacker, wenn beim initialen Verbindungsaufbau mittels des bekannten, initialen Schlüssels der Datenverkehr entschlüsselt und der neu ausgehandelte Schlüssel mitgelesen werden kann.



Quelle: Computer Bild: Smartphones: Lausangriff über Bewegungssensoren möglich, 19.08.2017, <https://www.computerbild.de/artikel/cb-News-Handy-Smartphones-Sicherheitsluecke-Cyroskop-10710116.html>

# Versuchsaufbau

ZigBee-Haussteuerungsnetz mit „Homee“ als Zentrale

- Homee: Brain Cube mit ZigBee-Aufsatzmodul (ca. 200 €)
- Philips Hue-Geräte (Schalter, LED-Lampen) (ca. 100 €)



ZigBee-„Kontrollgruppe“

- Philips Hue-Basissatz (je ein Schalter und LED-Lampe)



Quellen: amazon.de

Sniffing-Ausstattung

- Raspberry-Pi 3B+ mit Raspbee-Modul, portablem Monitor etc. (ca. 200 €)
- Penetrationstestframework „Zigdigity“ (kostenlos)
- Wireshark zur Netzwerkanalyse (kostenlos)



Quelle: reichelt.de

# Analyse Netzwerktraffik

Identifikation des genutzten ZigBee-Kanäle im 2,4 GHz Frequenzband mittels Scan, hier: Kanal 15 & 26

The screenshot displays a network traffic analysis tool interface. On the left, a terminal window shows the process of scanning ZigBee channels from 11 to 26. The main window shows a list of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.005000	0xa44b	Broadcast	ZigBee	56	Data, Dst: Broadcast, Src: 0xa44b
2	0.002867			IEEE 8...	5	Ack
3	0.008985	0xa44b	0xe8f5	IEEE 8...	12	Data Request
4	0.011744			IEEE 8...	5	Ack
5	0.033815	0xa44b	Broadcast	ZigBee	56	Data, Dst: Broadcast, Src: 0xa44b
6	107.443258	0x0000	Broadcast	ZigBee	50	Link Status

The first packet (No. 1) is highlighted with a red box. Below the table, a detailed view of this packet is shown, indicating it is a ZigBee Network Layer Data packet with a destination of Broadcast and source of 0xa44b.

```
Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0  
= IEEE 802.15.4 Data, Dst: 0xe8f5, Src: 0xa44b  
- ZigBee Network Layer Data, Dst: Broadcast, Src: 0xa44b
```

At the bottom, a terminal window shows the command `sudo apt autoremove` being executed.

Quelle: Enrico Seib, LKA M-V

# Verschlüsselter Datenverkehr

## Verschlüsselter Datenverkehr im ZigBee Homee-Netzwerk

The screenshot shows a Wireshark capture of ZigBee traffic. The main pane displays a list of captured packets with columns for Time, Source, Destination, Protocol, Length, and Info. A packet at 43.45.394362 is selected, and the packet details pane shows a ZigBee Security Header with an Encrypted Payload highlighted in red. The hex dump at the bottom shows the raw data bytes.

Time	Source	Destination	Protocol	Length	Info
26.13.163433			IEEE 802.15.4	5	Ack
27.13.284369	0xa4ab	Broadcast	ZigBee	53	Data, Dst: Broadcast, Src: 0xa4ab
28.13.643896	0xa4ab	Broadcast	ZigBee	53	Data, Dst: Broadcast, Src: 0xa4ab
29.13.647469			IEEE 802.15.4	5	Ack
30.13.089536	0xa4ab	Broadcast	ZigBee	53	Data, Dst: Broadcast, Src: 0xa4ab
31.15.117669	0xe8f5	Broadcast	ZigBee	47	Command, Dst: Broadcast, Src: 0xe8f5
32.15.134083	0xa4ab		IEEE 802.15.4	12	Data Request
33.15.136831			IEEE 802.15.4	5	Ack
34.20.174098	0xa4ab	0xe8f5	IEEE 802.15.4	12	Data Request
35.20.176543			IEEE 802.15.4	5	Ack
36.25.175820	0xa4ab	0xe8f5	IEEE 802.15.4	12	Data Request
37.25.174486			IEEE 802.15.4	5	Ack
38.30.284921	0xa4ab	0xe8f5	IEEE 802.15.4	12	Data Request
39.30.286677			IEEE 802.15.4	5	Ack
40.30.273543	0xe8f5	Broadcast	IEEE 802.15.4	47	Data, Dst: Broadcast, Src: 0xe8f5, Bad FCS
41.33.788518	0xa4ab	0xe8f5	IEEE 802.15.4	12	Data Request
42.33.080691			IEEE 802.15.4	5	Ack
43.45.394362	0xe8f5	Broadcast	ZigBee	47	Command, Dst: Broadcast, Src: 0xe8f5

**ZigBee Security Header**

Frame Counter: 21869740  
Extended Source: Phlllpsl\_01:84:c5:5c:d7 (00:17:88:01:84:c5:5c:d7)  
Key Sequence Number: 0  
Message Integrity Code: d7b75c4a  
[Encrypted Payload]  
[Group: Undecoded]

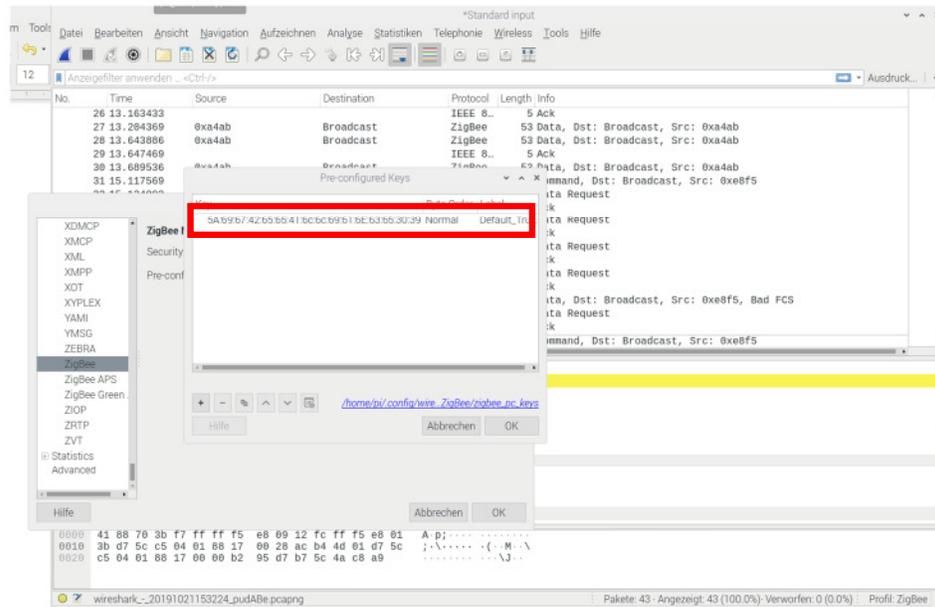
Data (2 bytes)

```
0000 41 88 70 3b f7 ff ff f5 e8 09 12 fc ff f5 e8 01  A p:.....
0010 3b d7 5c c5 04 01 88 17 00 28 ac b4 4d 01 d7 5c  ; \.....
0020 c5 04 01 88 17 00 00 b2 95 d7 d7 5c 4a c8 ab  ; \.....
```

Quelle: Enrico Seib, LKA M-V

# Kompromittierter Schlüssel

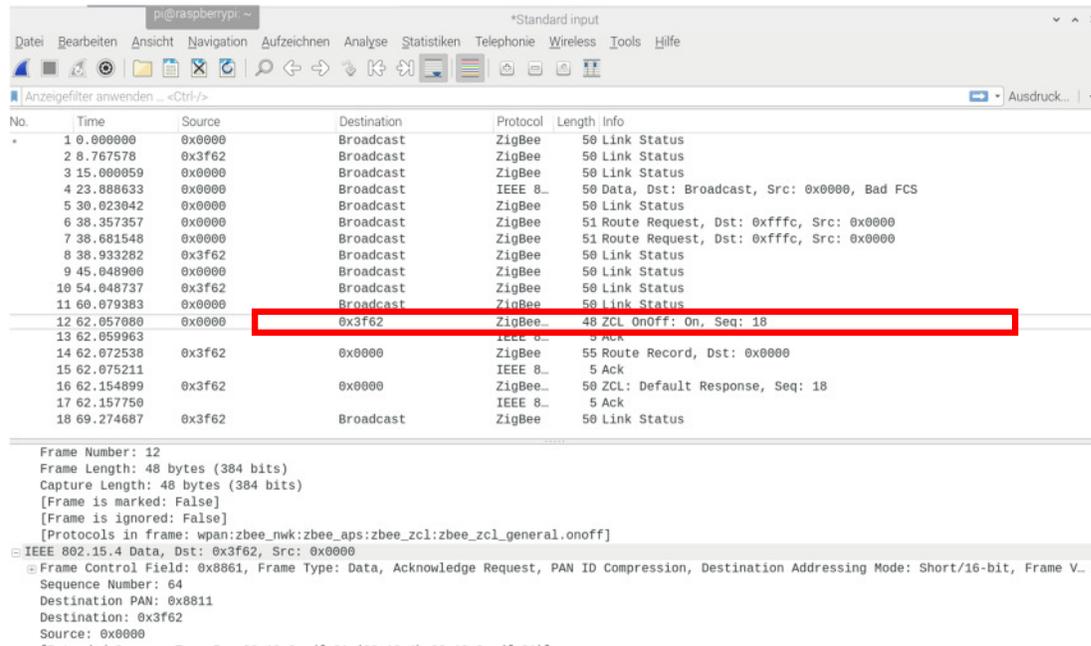
Entschlüsselung des Netzwerkverkehrs mittels kompromittiertem Schlüssel im Analysetool Wireshark



Quelle: Enrico Seib, LKA M-V

# Kein erneuter Schlüsselaustausch

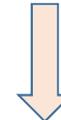
→ Die Verschlüsselung erfolgt weiterhin mittels kompromittiertem Schlüssel



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0x0000	Broadcast	ZigBee	50	Link Status
2	0.767578	0x3f62	Broadcast	ZigBee	50	Link Status
3	15.000059	0x0000	Broadcast	ZigBee	50	Link Status
4	23.888633	0x0000	Broadcast	IEEE 802.15.4	50	Data, Dst: Broadcast, Src: 0x0000, Bad FCS
5	30.023042	0x0000	Broadcast	ZigBee	50	Link Status
6	38.357357	0x0000	Broadcast	ZigBee	51	Route Request, Dst: 0xffff, Src: 0x0000
7	38.681548	0x0000	Broadcast	ZigBee	51	Route Request, Dst: 0xffff, Src: 0x0000
8	38.933282	0x3f62	Broadcast	ZigBee	50	Link Status
9	45.048900	0x0000	Broadcast	ZigBee	50	Link Status
10	54.048737	0x3f62	Broadcast	ZigBee	50	Link Status
11	60.079383	0x0000	Broadcast	ZigBee	50	Link Status
12	62.057080	0x0000	0x3f62	ZigBee	48	ZCL OnOff: On, Seq: 18
13	62.059963	0x0000	0x0000	IEEE 802.15.4	5	Ack
14	62.072538	0x3f62	0x0000	ZigBee	55	Route Record, Dst: 0x0000
15	62.075211	0x3f62	0x0000	IEEE 802.15.4	5	Ack
16	62.154899	0x3f62	0x0000	ZigBee	50	ZCL: Default Response, Seq: 18
17	62.157750	0x0000	0x0000	IEEE 802.15.4	5	Ack
18	69.274687	0x3f62	Broadcast	ZigBee	50	Link Status

Frame Number: 12  
Frame Length: 48 bytes (384 bits)  
Capture Length: 48 bytes (384 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: wpan:zbee\_nwk;zbee\_aps;zbee\_zcl;zbee\_zcl\_general.onoff]  
IEEE 802.15.4 Data, Dst: 0x3f62, Src: 0x0000  
Frame Control Field: 0x8861, Frame Type: Data, Acknowledge Request, PAN ID Compression, Destination Addressing Mode: Short/16-bit, Frame V...  
Sequence Number: 64  
Destination PAN: 0x8811  
Destination: 0x3f62  
Source: 0x0000

Quelle: Enrico Seib, LKA M-V



Quelle Abbildungen Lampen: amazon.de

# Homee – offene Kommunikation?

- Homee-ZigBee *Coordinator* und ZigBee-*Devices* kommunizieren mittels kompromittiertem Schlüssel, dieser wird nicht neu ausgehandelt

→ Kommunikation *de facto* offen

## Wie kann das sein?

# Homee – Verifikation der Sicherheitslücke

- Verifikation erfolgte anhand verschiedener Firmware-Versionen des Steuerungsgerätes und erneutem Anlernen der Geräte unterschiedlicher Hersteller, jedoch bei unveränderter Firmware des Homee-ZigBee-Coordinator

Diese Situation besteht noch im Juni 2020!

# Kurzüberblick - EnOcean

- Weiterer Standard für drahtlose Hausautomatisierung
- Spin-off der Siemens AG
- Grundprinzip des “”
- No batteries required due to energy harvesting
- Managed by the EnOcean alliance (non profit org.), ca. 350 partner companies (Microsoft, IBM, T-Systems, Siemens, Peha (Honeywell-Gruppe), Somfy, Kieback & Peter, Texas Instruments, ABB, Friends of Hue ... )
- Frequency band: 868 MHz in Europe, US/Canada: 868 MHz, Japan: 928 MHz, Bluetooth (2.4 GHz), Long Range (Japan)
- Low energy consumption
- Small data packages



Quelle: [enocean.org](http://enocean.org)

# EnOcean Sicherheitsaspekte und mögliche Exploits

- Eigenes Protokoll → optimiert für geringen Energieverbrauch
  - Energy Harvesting als Grundprinzip, Ziel ist Batteriefreiheit
  - Keine Mechanismen für Kollisionsprävention
  - Kleine Datenpakete
  - ...
- Der Hersteller wirbt mit einem *mehrstufigen Sicherheitskonzept* inkl. Aspekten wie Rolling Code und Verschlüsselung

# EnOcean – Zusätzliche Sicherheit?

- EnOcean-Geräte sind in unterschiedlichen Preisklassen erhältlich, die untersuchten Schalter bspw. nutzen jedoch den gleichen Chipsatz
- Nutzung der Sicherheitsmechanismen in EnOcean ist **nicht obligatorisch**
- Sicherheitsmechanismen müssen durch den Nutzer **zusätzlich** freigeschaltet werden
  - Ist nicht sofort ersichtlich
  - Anleitungen dazu sind im Internet mit Rechercheaufwand auffindbar



Quelle: Benjamin Kem, LKA M-V

Annahme: Großteil der EnOcean-Systeme ist noch im Auslieferungszustand ohne Sicherheitsmechanismen

# EnOcean Sicherheitsaspekte und mögliche Exploits

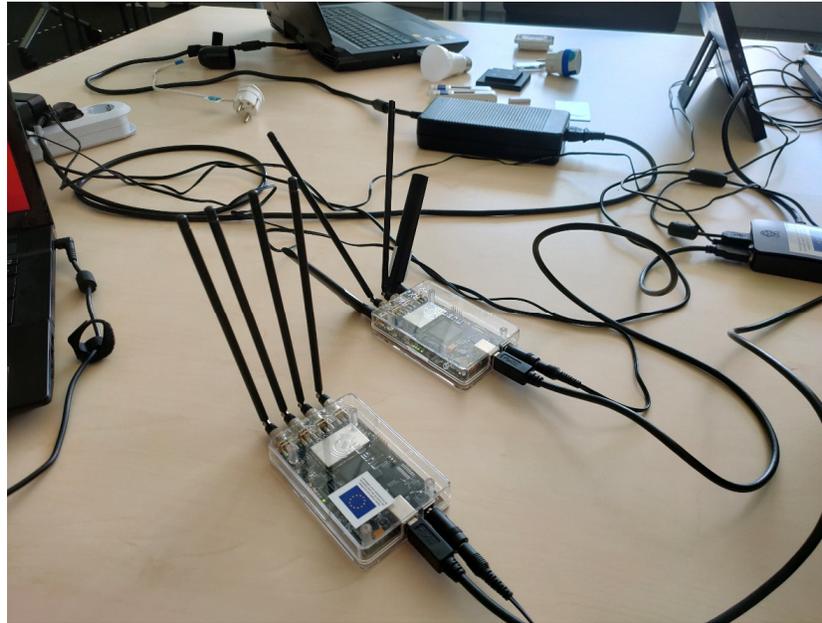
- Eigenes Protokoll → optimiert für geringen Energieverbrauch
  - ...
- *Zusätzliche/nicht obligatorische* Sicherheitsmechanismen wie Rolling Code und Verschlüsselung

**Wie lässt sich die Kommunikation in EnOcean ohne Wissen über Protokoll und Implementierung stören?**

**→ Überlagerung des physischen Signals!**

# Beispiel 5: EnOcean – Überlagerung des physischen Signals

- Überlagerung des EnOcean-Signals mittels „Software Defined Radio“ (SDR)



Quelle: Benjamin Kem, LKA M-V

# Experiment – Signalüberlagerung

## EnOcean Testaufbau:

- EnOcea-Schalter, LED-Leuchtmittel, etc. (ca. 150 €)

## SDR zur Signalerzeugung/Störung

- Nuand BladeRF 2.0 micro (ca. 800 €)
- Raspberry-Pi 3B+, portabler Monitor etc. (ca. 200 €)
- Software „Spectrum painter“ (frei auf gitHub)

## SDR zur Anzeige des Frequenzspektrums

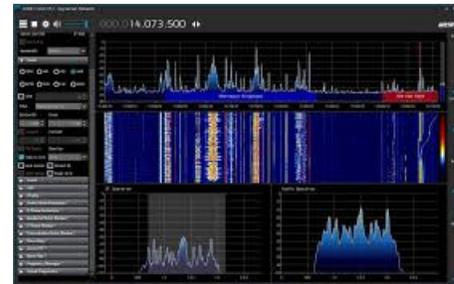
- Nuand BladeRF 2.0 micro (ca. 800 €)
- Laptop (bereits vorhanden)
- SDR# für Windows 10 (frei)



Quelle: Benjamin Kem, LKA M-V



Quelle: <https://antratek.de>



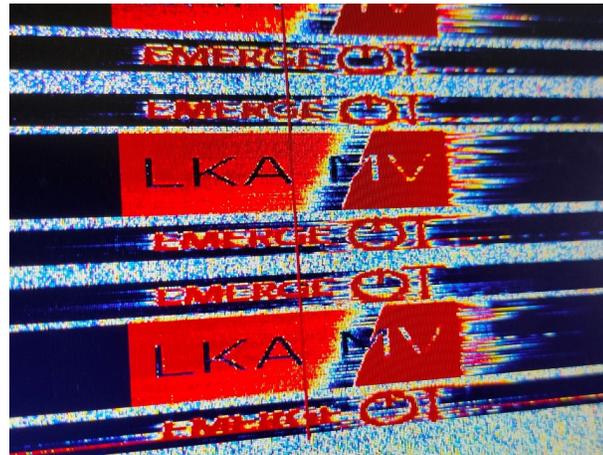
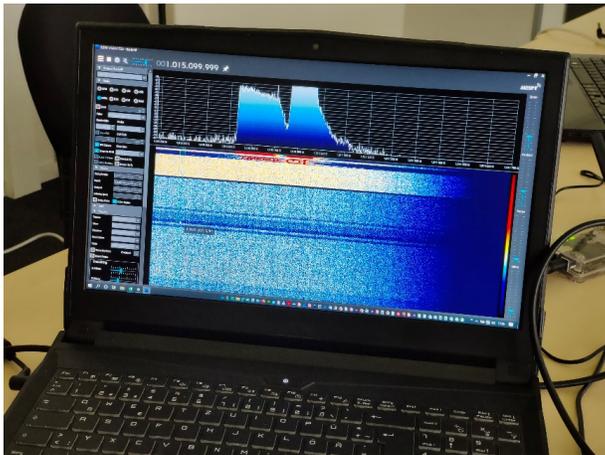
Quelle: <https://rtl-sdr.com>



Quelle: reichelt.de

# Signalüberlagerung

- Überlagerung des EnOcean-Signals im 868 MHz-Bereich



Quellen: Benjamin Kem, LKA M-V

→ Kein EnOcean-Steuerungssignal während der Signalüberlagerung

# Chip Off - Analyse

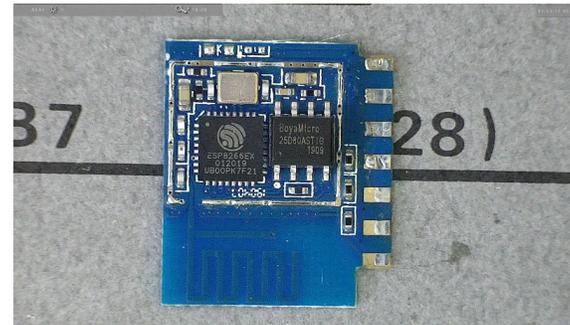
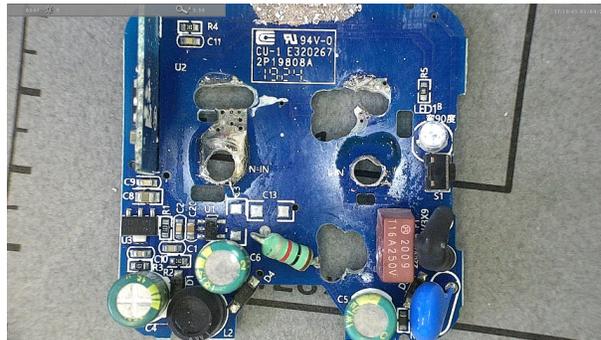
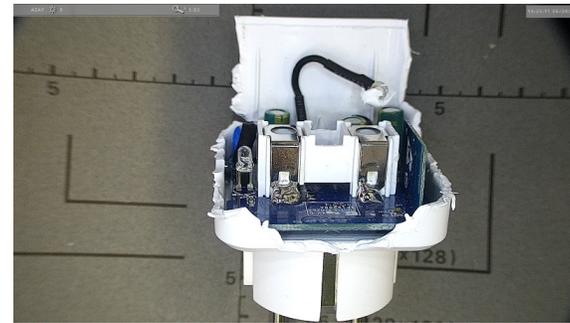
- Chip Off von unterschiedlicher WLAN-Geräten um WLAN-Passwort zu extrahieren
- Untersuchte Geräte
  - Schaltsteckdose Teckin Smart Plug SP21
  - Ring Video Doorbell
  - Ring Video Doorbell 2



Quellen: Enrico Seib, LKA M-V

# Physische Analyse – Chip Off Teckin SP 21 Schaltsteckdose

Demontage einer Teckin SP 21 – Extraktion des WLAN-Chips

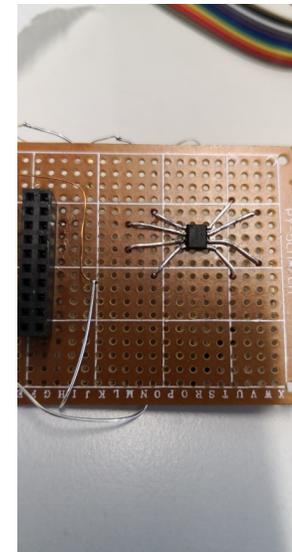


Quellen: Daniel Reimann, LKA M-V

# Teckin SP 21 – Analyse Speicherchip WLAN-Modul

Idee: WLAN-Modul enthält Speicherchip mit WLAN-Zugangsinformationen

- Extraktion des WLAN-Moduls (Controller **ESP8266EX** mit Speicherchip **BY25D80**)
- Auslesen von Controller & Chip → Kein Ergebnis (Speicher konnte nicht isoliert angesprochen werden)
- Extraktion des Speicherchips und Auslesen der Daten mittels SPI-Interface & Raspberry Pi 4 mit Pythonmodul „spidev“

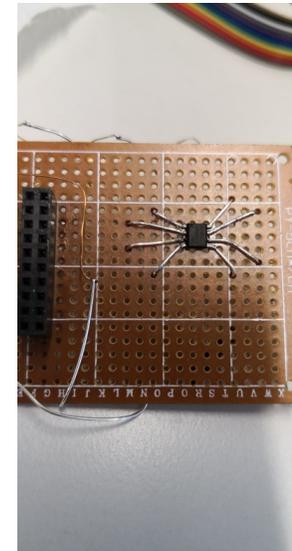


Quellen: Daniel Reimann, LKA M-V

# Teckin SP 21 – Ergebnis der Speicherdumpanalyse

## Ergebnis:

- Speicherbereiche mit hoher/geringer Entropie, vermutlich Firmware- und Nutzerdaten
- Möglicherweise verschleiertes oder verschlüsselte Ablage der Nutzerdaten
- Stichprobenartige Untersuchung verschiedener Kodierungs- und Darstellungsvarianten der SSID+PSK, **jedoch ohne Erfolg**
- getestete Variationen SSID + PSK:
  - Base64 Kodierung (hex/ascii)
  - DKDF2(SHA256/4096Iterationen)



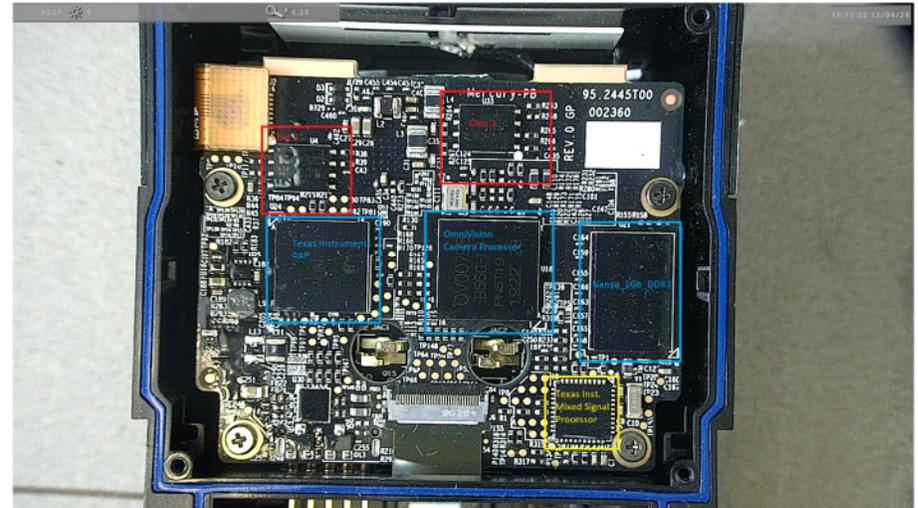
Quellen: Daniel Reimann, LKA M-V

# Chip Off Ring Video Doorbell 2

Ring Video Doorbell 2 Hauptplatine mit Fotoplatine



Ring Video Doorbell 2 Hauptplatine Vorderseite



Quellen: Daniel Reimann, LKA M-V

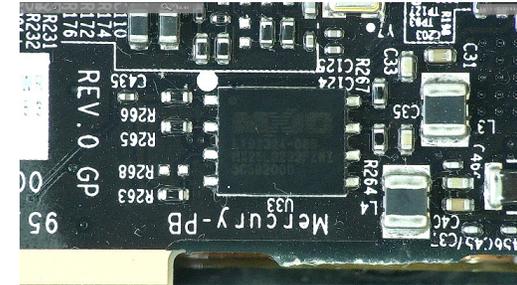


# Ring Video Doorbell 1&2 – Analyse der Speicherdumps

## Ergebnis

- Chip 1: Alternierende Bereiche mit hoher bzw. geringer Entropie, teilweise in Klarschrift, könnten einzelne Logs darstellen
- Chip 2 & 3: Alternierende Bereiche mit hoher bzw. geringer Entropie, zum Teil Klarschrift mit Hinweis auf Logdateien bzw. Firmware

Suche nach Nutzerdaten im „Klartext“, nach einfach verschleierten Daten (Base64, MD5 Hash etc.), nach Datenstruktur (Blöcke, Nummerierung), nach möglichem XOR-Scrambling **ohne weiterführenden Erkenntnisse**



# Emerge IoT- Status

- Bisher erreicht
  - Grundlegende Wissensbasis geschaffen
  - Laufende Sensibilisierung für Risiken im Bereich IoT
  - Präsentation des Projektes und der Projektergebnisse auf Landes- und Bundesebene
  - Planungen und Durchführungen von Angriffsszenarien für unterschiedliche Protokolle und Produkte (WLAN, ZigBee, Homematic/Homematic IP, EnOcean, Z-Wave)
  - Erste vielversprechende Ergebnisse für einzelne IoT-Produkte und Protokolle
- Noch durchzuführen u.a.
  - Weitere Analysen und Tests mit zusätzlichen Protokollen und Publikation der Ergebnisse
  - Engagement in Fort- und Weiterbildung mit FHöVPR Güstrow für Polizeivollzugsbeamte
  - Entwicklung einheitlicher Workflows und Handlungsanweisungen

---

# ENDE

**Vielen Dank für Ihre Aufmerksamkeit!**

**Kontakt: <https://www.emerge-iot.de>**