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

EMERGE IoT

Landeskriminalamt Mecklenburg-Vorpommern

Universität Rostock Traditio et Innovatio

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.259484.0.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 gekaperter IoT-Netzwerke
  - Bot-Netze
  - Bitcoin-Mining

Quelle: Tumiso, pixabay.com

Quelle: Adtel Integration, http://Adtelintegration.com/smart-cities-inftrastructure/

Polizeiliche Fragestellungen - Chancen

- Aktive und präventive Strafverfolgung
  - IoT als Beweismittel, z.B. durch Auswertu 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-inftrastructure/

EMERGE IoT – Das Projekt

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

Landeskriminalamt Mecklenburg-Vorpommern

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

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 **Er**mittlun**g**en und **E**rmittlungsunterstützung im „**I**nternet **o**f **T**hings“. (www.emerge-iot.de)

Projektziele Emerge IoT

Entwicklung von Kompetenzen, **M**ethoden und Werkzeugen
für zukunftsorientierte **Er**mittlun**g**en und **E**rmittlungsunterstützung
im „**I**nternet **o**f **T**hings“.

- 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

- 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 **Er**mittlun**g**en und **E**rmittlungsunterstützung
im „**I**nternet **o**f **T**hings“.

- 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

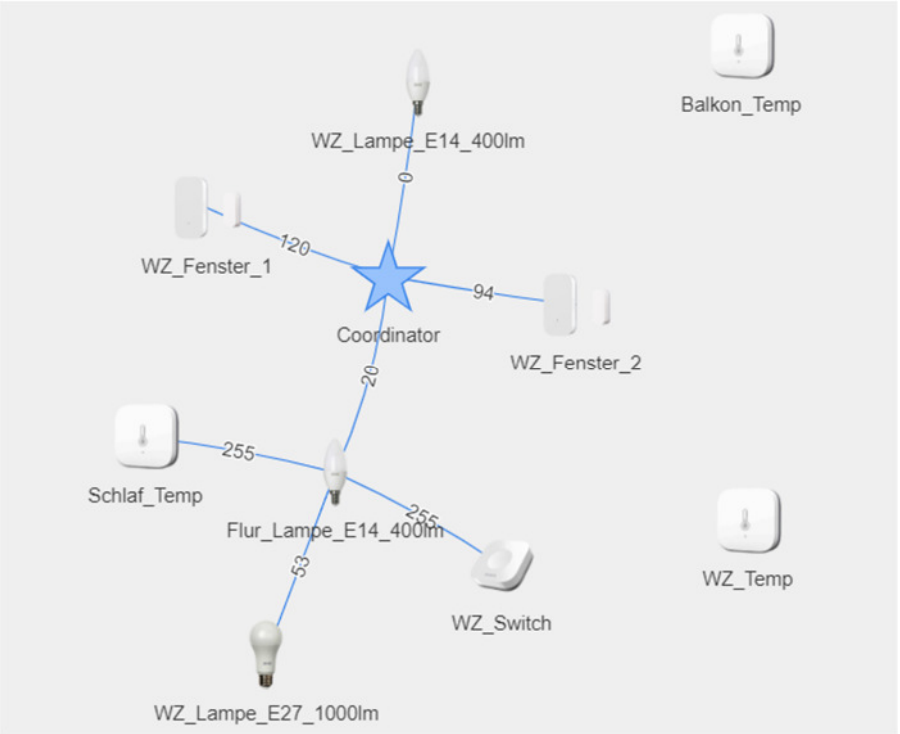
Einschub: ZigBee - Kurzübersicht

- 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

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

- 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

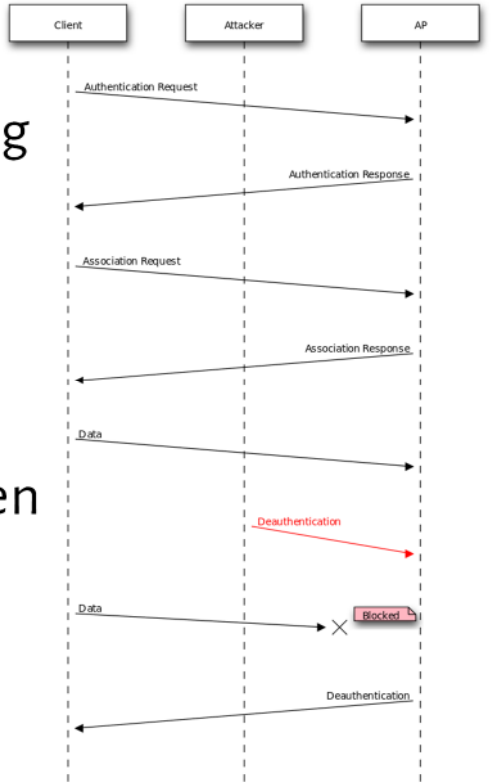
Einschub: ZigBee - Netzwerk



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

Deauthenfication 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-Ausstattatung:

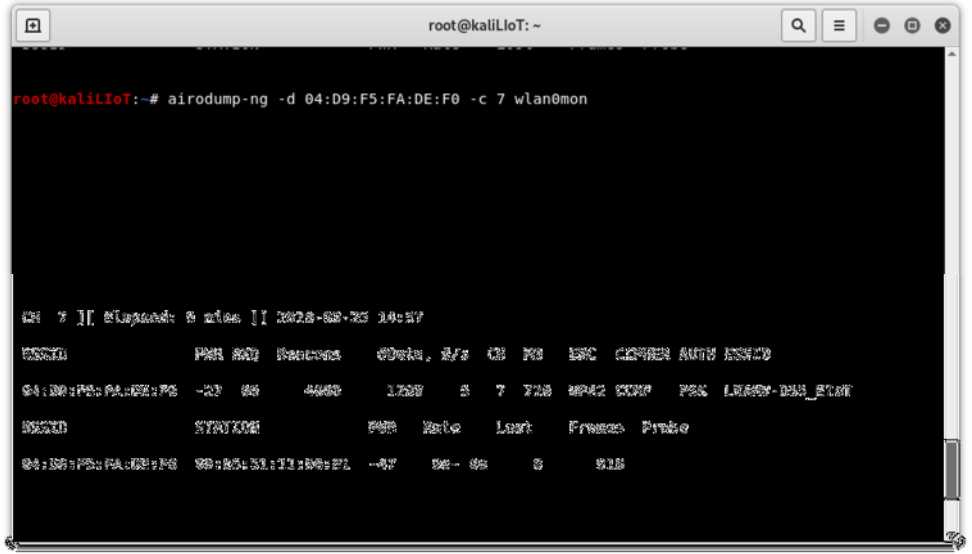
- Raspberry-Pi 3B+ mit Raspbee-Modul, tragbarer Monitor etc. (ca. 200 €)
- Wireshark für Netzwerkanalyse (kostenfrei)

Quellen: amazon.de

Quelle: wireshark.org

Erfolgreicher Deauthentifizierungsangriff

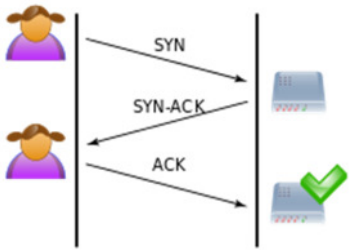
- Funktioniert wie erwartet, daTeil des Standards IEEE 802.11
- Geräte/Netzwerkverbindungen „erholen“ sich nach dem Angriff wieder
- Gezielte Auswahl von Netzwerken/Geräten möglich



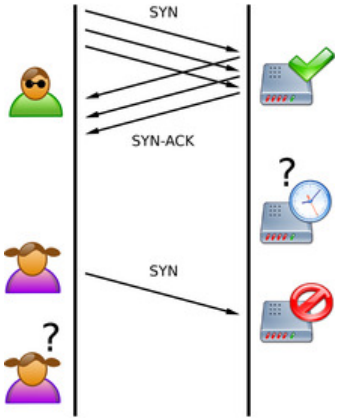
Quelle: Enrico Seib, LKA M-V

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)



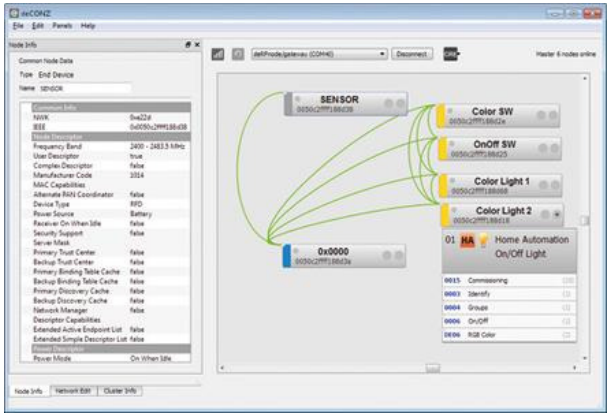
Quelle: https://de.wikipedia.org/wiki/SYN-Flood#/media/Datei:Tcp_synflood.png

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)



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

Angriffswerkzeug:

- Laptop mit Kali-Linux (kostenlos außer Hardware)

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

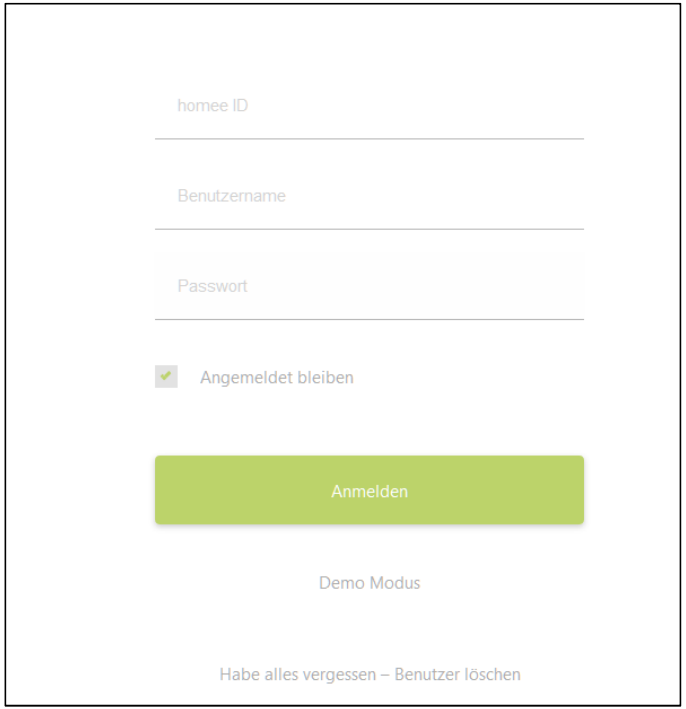
Sniffing-Ausstattung

- 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



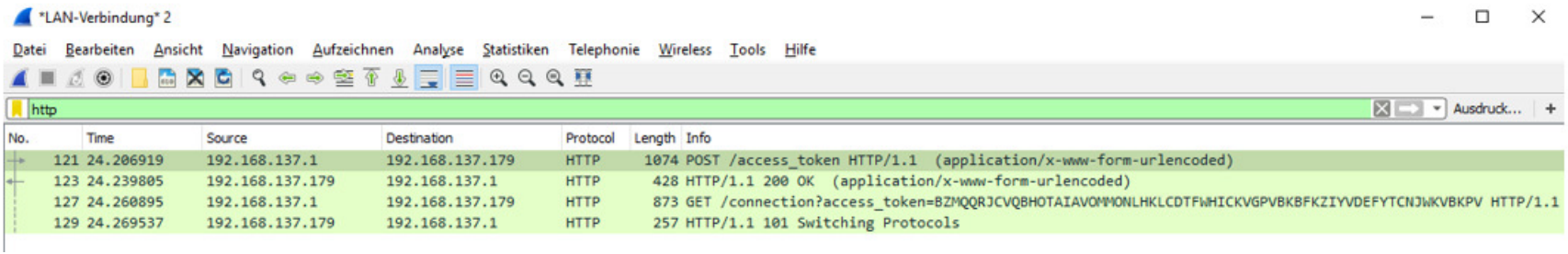
Quelle: Enrico Seib, LKA M-V

Sichtbarer Netzwerktraffic mit Wireshark

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

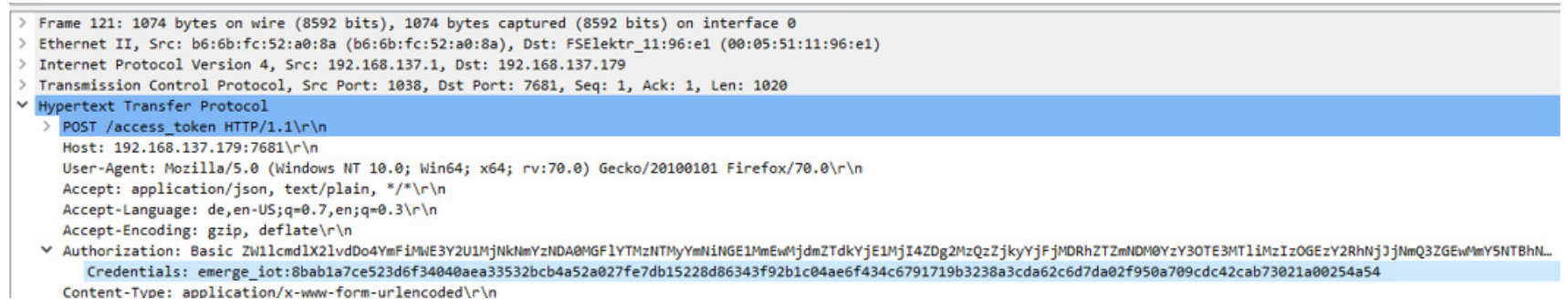
ABER

Anmeldung via HTTP-Post



Quelle: Enrico Seib, LKA M-V

Übertragung von Nutzername und Passwort



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!

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

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.

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)

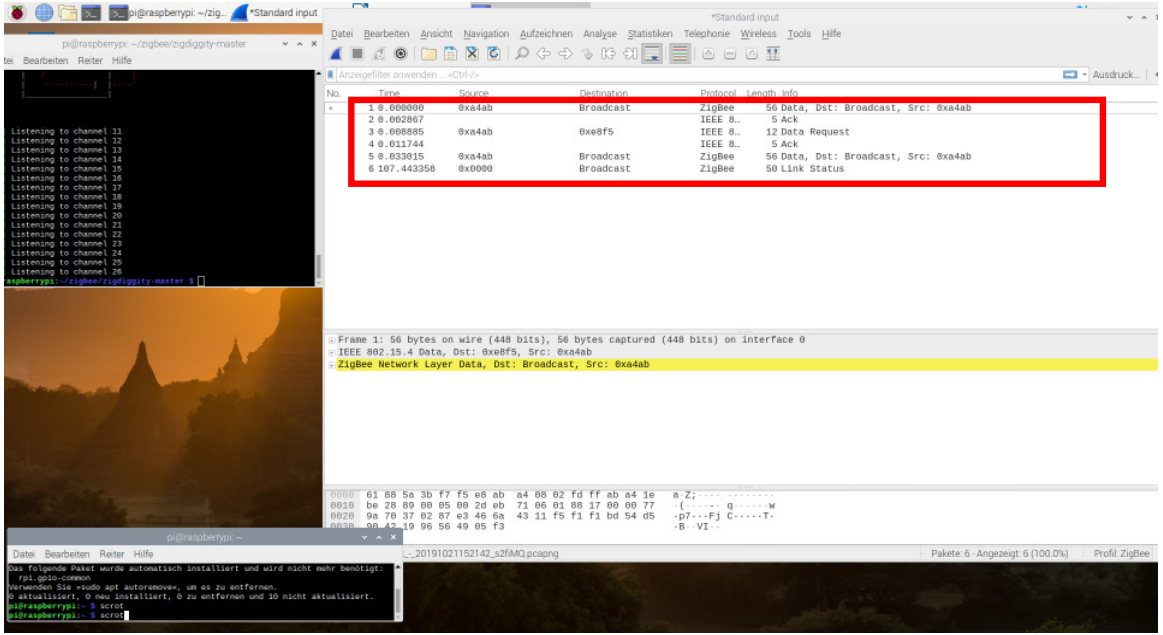
Quellen: amazon.de

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

Quelle: reichelt.de

Analyse Netzwerktraffic

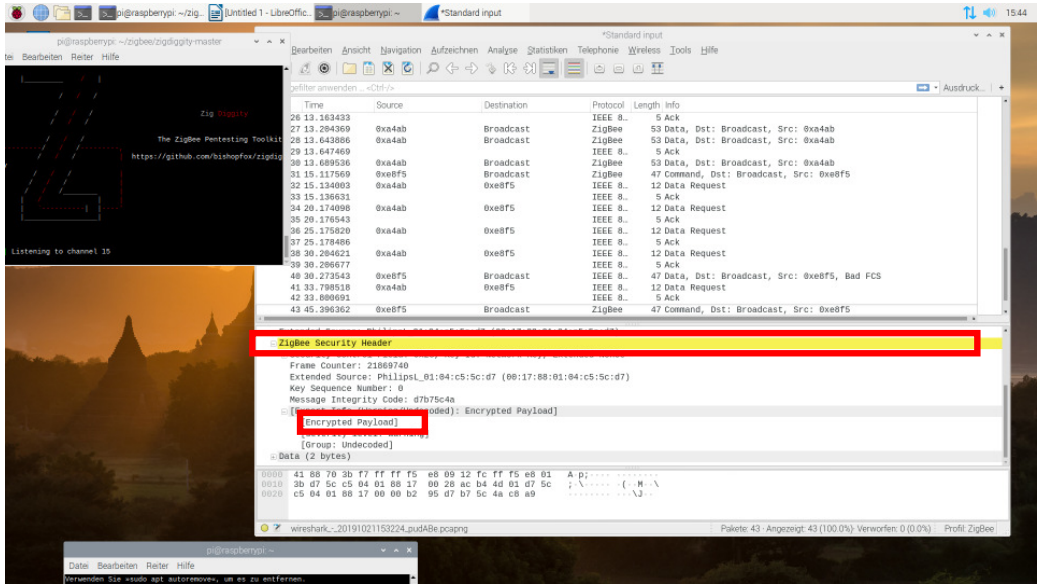
Identifikation des genutzten ZigBee-Kanäle im 2,4 GHz Frequenzband mittels Scan, hier: Kanal 15 & 26



Quelle: Enrico Seib, LKA M-V

Verschlüsselter Datenverkehr

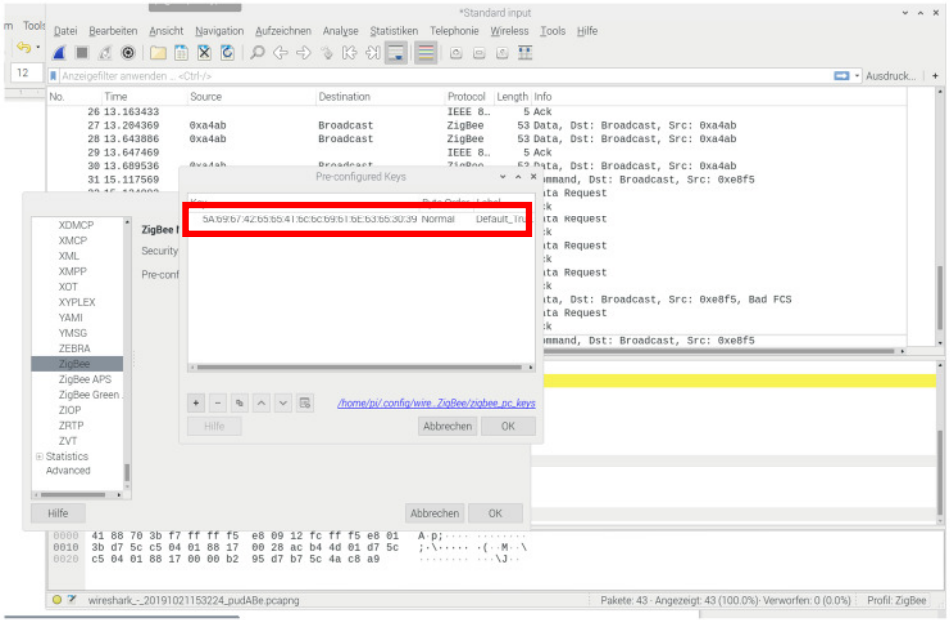
Verschlüsselter Datenverkehr im ZigBee Homee-Netzwerk



Quelle: Enrico Seib, LKA M-V

Kompromittierter Schlüssel

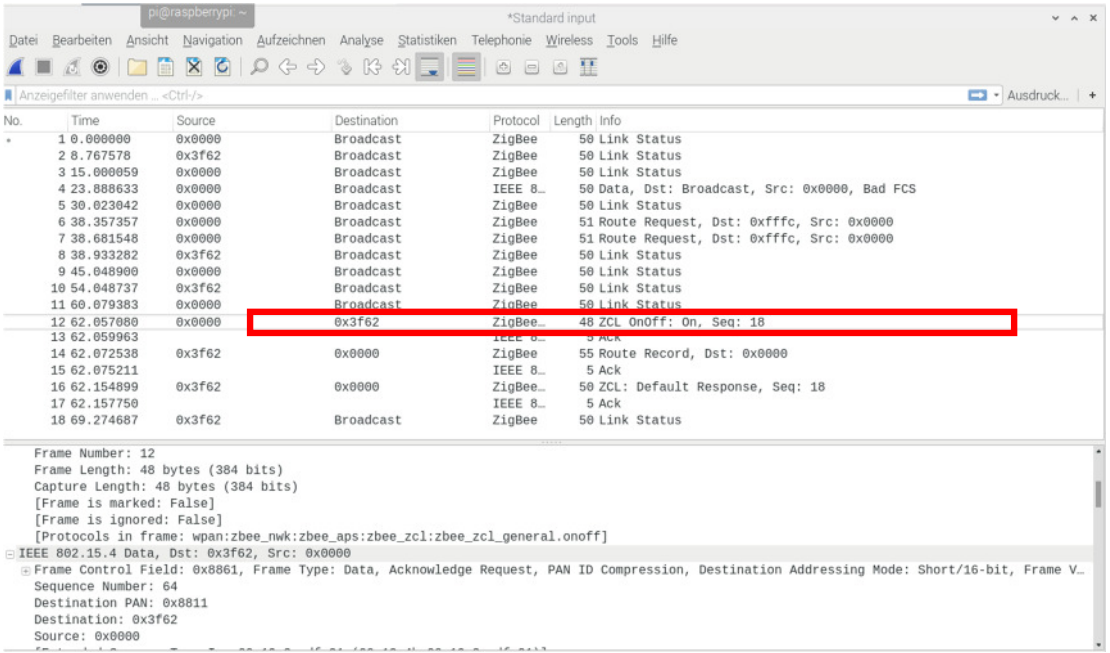
Entschlüsselung des Netzwerkverkehrs mittels kompromittiertem Schlüssel im Analysetool Wireshark



Quelle: Enrico Seib, LKA M-V

Kein erneuter Schlüsselaustausch

→ Die Verschlüsselung erfolgt weiterhin mittels kompromittiertem Schlüssel



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

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 Kern, LKA M-V

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

EnOcean Sicherheitsaspekte und mögliche Exploits

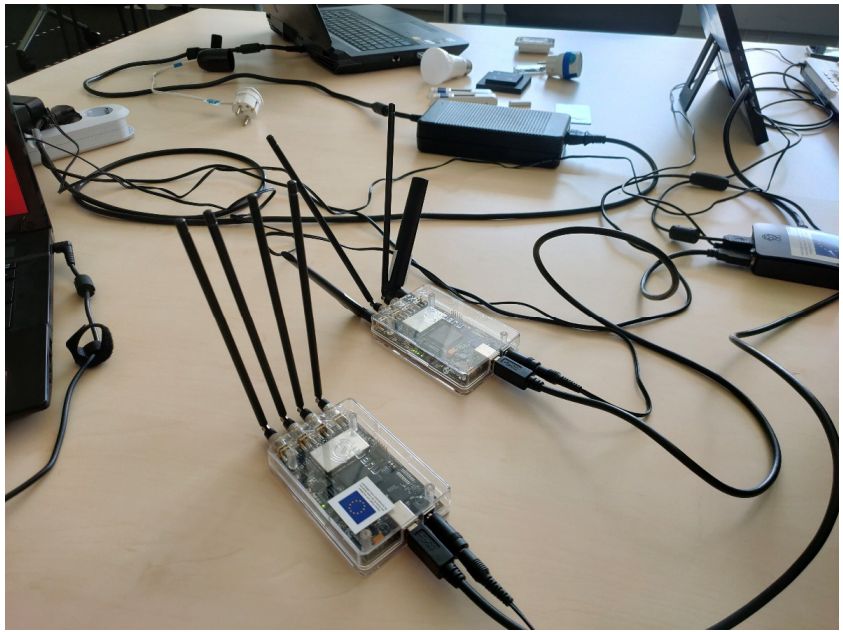
- Eigenes Protokoll → optimiert für geringen Energieverbrauch
  - …
- *Zusätzliche/nicht obligatorische* Sicherheitsmechanismen wie Rolling Code und Verschlüsselung

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)



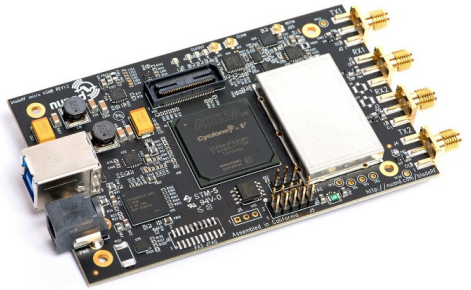
Quelle: Benjamin Kern, LKA M-V

Experiment –Signalüberlagerung

EnOcean Testaufbau:

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

Quelle: Benjamin Kern, LKA M-V



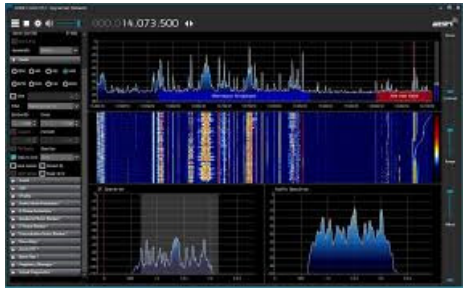
Quelle: https://antratek.de

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)

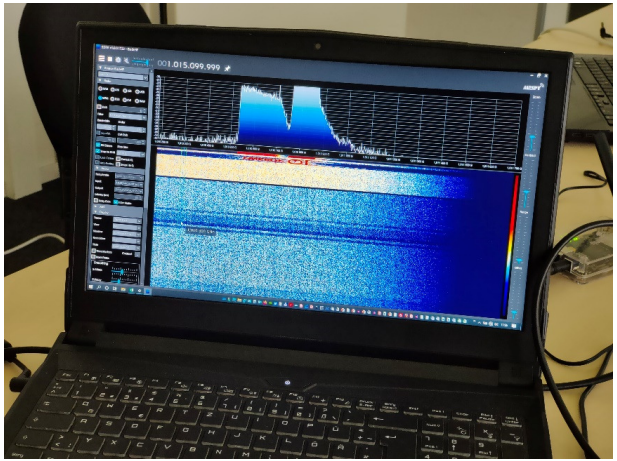


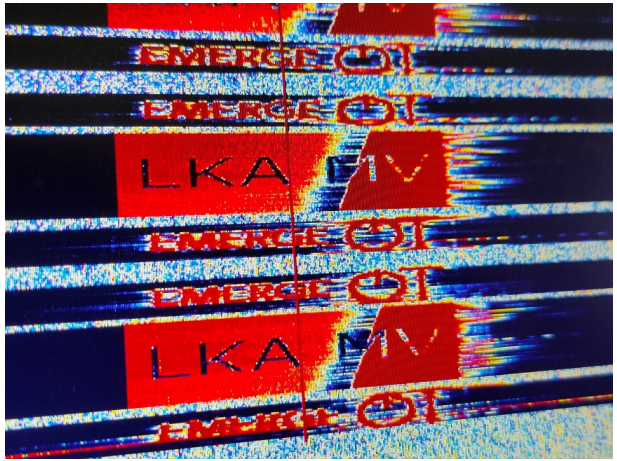
Quelle: https://rtl-sdr.com

Quelle: reichelt.de

Signalüberlagerung

- Überlagerung des EnOcean-Signals im 868 MHz-Bereich





Quellen: Benjamin Kern, LKA M-V

→ Kein EnOcean-Steuerungssignal während der Signalüberlagerung

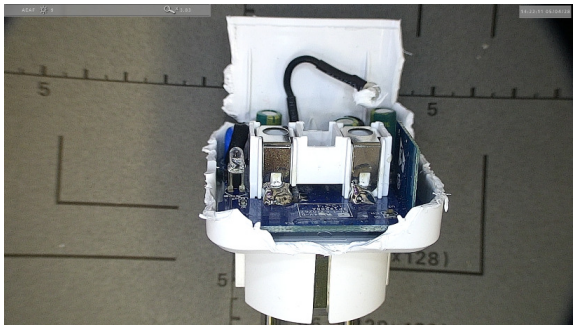
Chip Off - Analyse

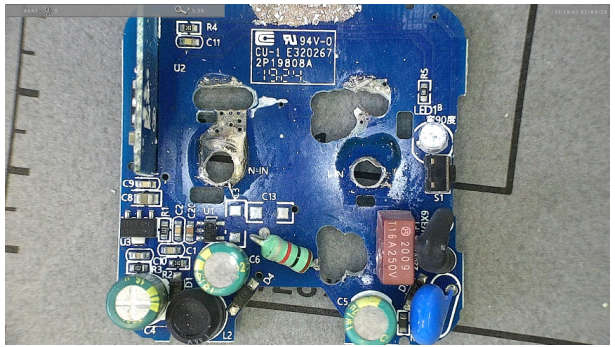
- Chip Off von unterschiedlicher WLAN-Geräten um WLAN-Passwort zu extrahieren
- Untersuchte Geräte
  - Schalttsteckdose Teckin Smart Plug SP21
  - Ring Video Doorbell
  - Ring Video Doorbell 2

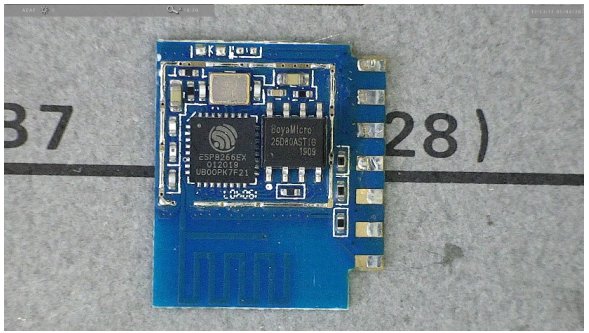
Quellen: Enrico Seib, LKA M-V

Physische Analyse – Chip Off Teckin SP 21 Schaltsteckdose

Demontage einer Teckin SP 21 – Extraktion des WLAN-Chips





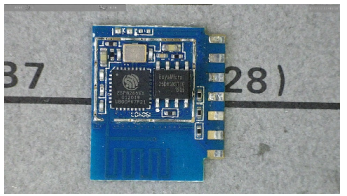


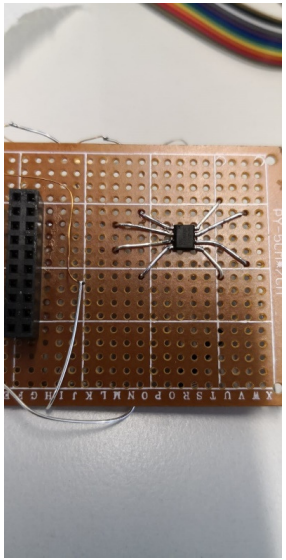
Quellen: Daniel Reimann, LKA M-V

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“



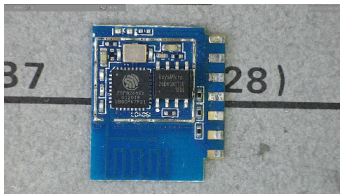


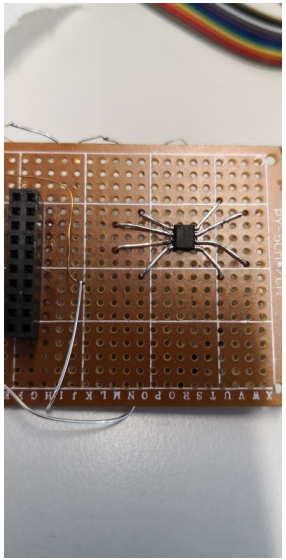
Quellen: Daniel Reimann, LKA M-V

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)

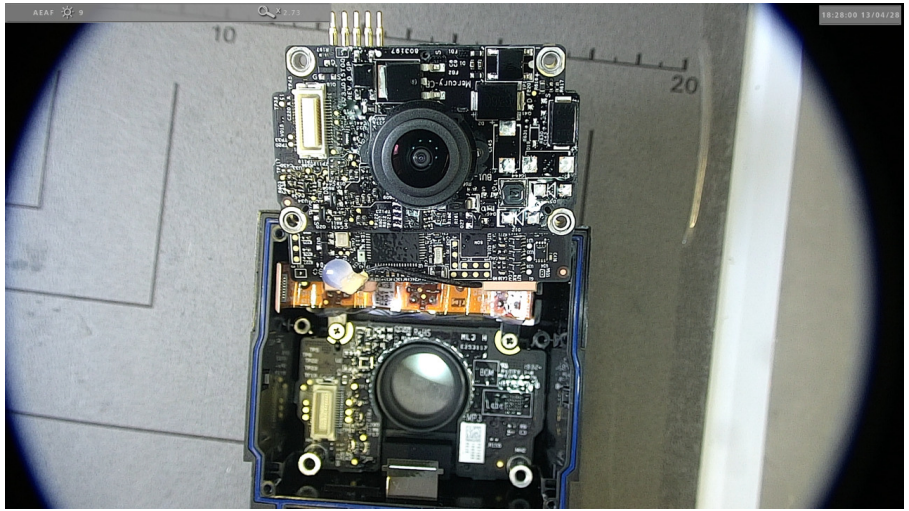




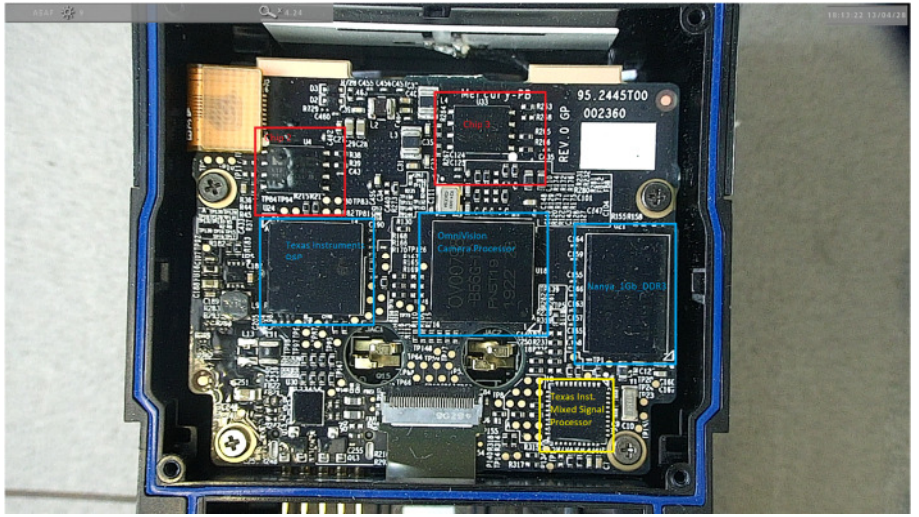
Quellen: Daniel Reimann, LKA M-V

Chip Off Ring Video Doorbell 2

Ring Video Doorbell 2 Hauptplatine mit Fotoplatine



Ring Video Doorbell 2 Hauptplatine Vorderseite

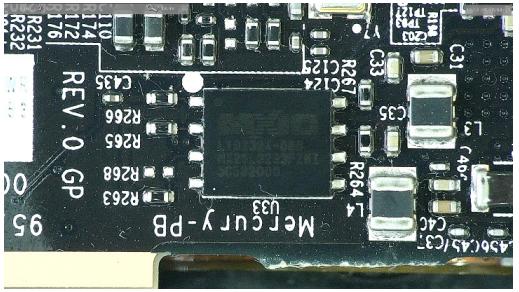


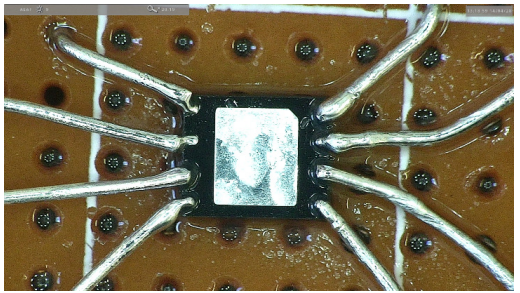
Quellen: Daniel Reimann, LKA M-V

Ring Video Doorbell 1&2 – Analyse Speicherchips

Idee: Videotürklingel enthält WLAN-Zugangsdaten

- Aufbau Ring Video Doorbell 1 & 2 im Wesentlichen identisch
- Drei Speichermodule Flash Memory **Macronix X25L3233F** identifiziert
- Extraktion des Speicherchips und Auslesen der Daten mittels SPI-Interface & Raspberry Pi 4 mit Pythonmodul „spidev“





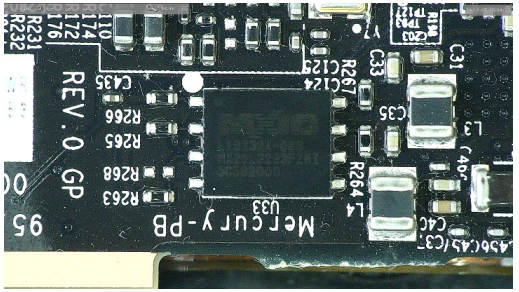
Quellen: Daniel Reimann, LKA M-V

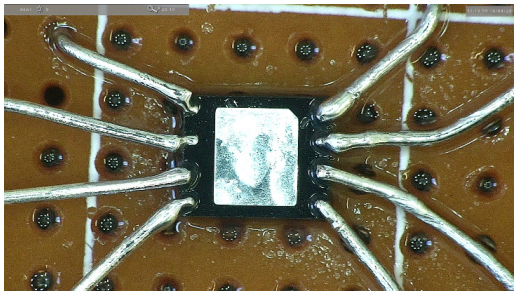
Ring Video Doorbell 1& 2 – Analyse der Speicherdumps

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**





Quellen: Daniel Reimann, LKA M-V

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