Die wunderbar unsichere Welt der Internet der Dinge

Emanuel Mairoll, Julian Oberhofer

SICHERHEITSRISIKO SMART HOME

Die Hacker kommen durch den Kühlschrank

von Thomas Kuhn
05. November 2014

Immer mehr Alltagsgeräte bekommen Internet-Zugang. Eine Studie zeigt: Das vernetzte Haus hat teils massive Sicherheitslücken. Sie werden zum Einfallstor für Hacker.

Thomas Hatley lag noch im Bett, als eines Morgens im vergangenen Sommer das Telefon klingelte. „Darf ich das Licht in Ihrem Schlafzimmer einschalten?“, fragte die Frau am anderen Ende der Leitung den verblüfftem Hausbesitzer aus dem US-Westküstenstaat Oregon.

arstechnica.com/g

ars TECHNICA SUBSCRIBE SIGN IN

DARK CLOUDS AHEAD —

Eufy's "local storage" cameras can be streamed from anywhere, unencrypted

The URLs for accessing your camera streams are also way too easy to brute-force.

KEVIN PURDY - 12/1/2022, 9:57 PM

Enlarge / Eufy's camera footage is stored locally, but with the right URL, you can also watch it from anywhere, unencrypted. It's complicated.

(**Update 7:30 a.m. ET 12/2/2022:** Eufy has issued a statement in response to findings from The Verge and a security researcher:

"eufy Security adamantly disagrees with the accusations levied against the company concerning the security of our products. However, we understand that the recent events may have caused concern for some users. We frequently review and test our security features and encourage feedback from the broader security industry to ensure we address all credible security vulnerabilities. If a credible vulnerability is identified, we take the necessary actions to correct it. In addition, we comply with all appropriate regulatory bodies in the markets where our products are sold. Finally, we encourage users to contact our dedicated customer support team with questions."

www.computerwor

COMPUTERWORLD UNITED STATES

NEWS ANALYSIS

Hackers demonstrated first ransomware for IoT thermostats at DEF CON

Ransomware-infected smart thermostats, it's no longer hypothetical. An attacker could crank up the heat and lock the IoT device until sweltering occupants paid a ransom to unlock it.

Oh goody, a hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees and leave the IoT device like that until its owner pays a ransom to regain control.

This is no longer a hypothetical attack; two hackers showed off the first proof-of-concept ransomware for smart thermostats; an attacker could set any temperature to try to melt or freeze the occupants until the ransom is paid. This first ransomware locked the temperate at 99 degrees until the owner paid a ransom to obtain a PIN which would unlock it.

gridinsoft.com/blog

NoaBot Botnet: The Latest Mirai Offspring

Mirai-based NoaBot botnet deploys cryptominers on Linux servers

A new botnet called NoaBot emerged in early 2023. It reportedly targets SSH servers for cryptocurrency mining using the Mirai platform. On top of the Mirai's functionality, it brings several detection evasion tricks.

NOABOT INVOLVED IN CRYPTO MINING

Cybersecurity experts have discovered a new botnet called NoaBot. It has been active since at least the beginning of 2023, and **the purpose of this botnet is illegal crypto mining**. It is based on the Mirai botnet, a notorious malware for harnessing infected IoT devices for large-scale network attacks. Despite being a derivative, it keeps all the functionality of the Mirai – a thing that can barely be underestimated.

Internet of Things

Internet of Things?

The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network, and be individually addressable.

Internet of Things!

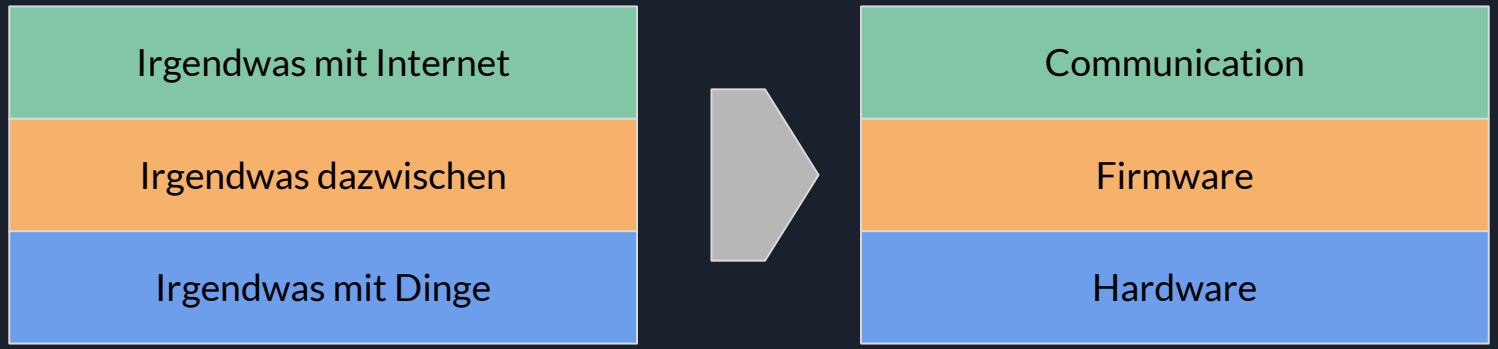
- ➔ Geräte und Gadgets,
- ➔ die traditionell nicht vernetzt waren,
- ➔ Sensoren und/oder Aktuatoren besitzen,
- ➔ und remote gesteuert werden können.


AI


NUKI
1 2
3 4
5 6
7 8
9 ◀
NUKI


Dryer
Washer

Also zusammengefasst:



Firmware-Layer

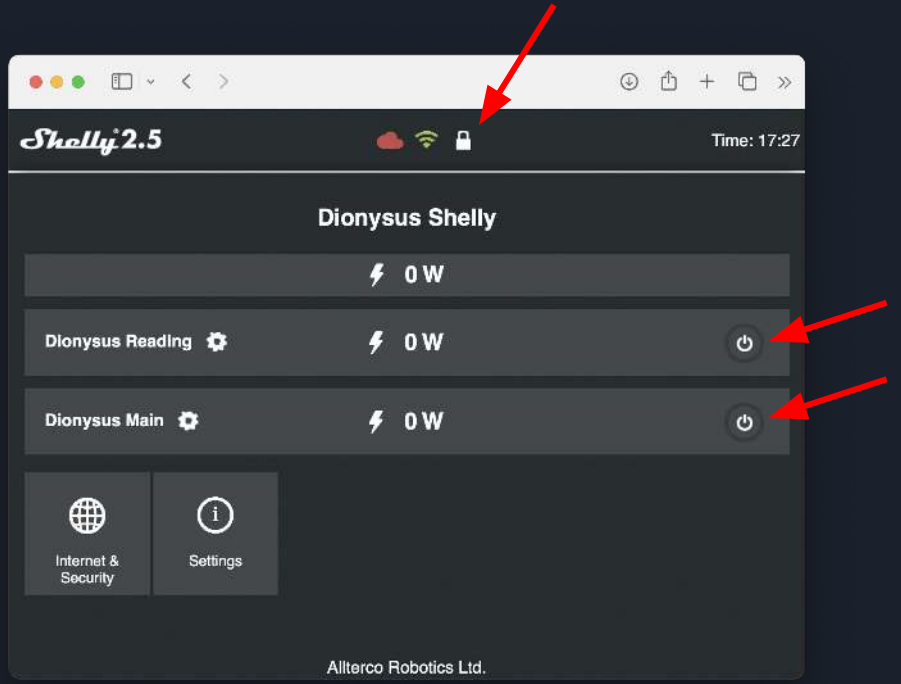
Was macht eine smarte Glühbirne “smart”?

API

“Ich bin eine Glühbirne”

Simpler Webserver

- Webinterface
- via Browser erreichbar
- Einfach, aber etwas umständlich
- “Sicher”, solange Zugang mit Passwort versehen ist



REST / RPC

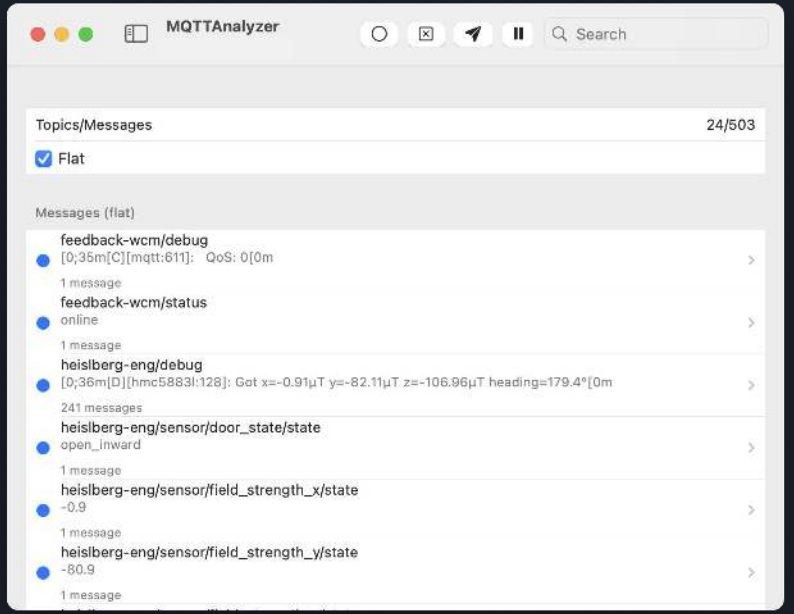
- Für Einbindung in andere Systeme
- Gut, weil unkompliziert - wenig Angriffsfläche
- **Sollte** ebenso mit Auth gesichert sein

Request frame invoking Switch.Set method:

```
{
   "id": 2,
   "src":"user_1",
   "method":"Switch.Set",
   "params": {
     "id":1,
     "on":true
   }
}
```

MQTT

- Device nicht Server, sondern Client
- Verbindet zu MQTT-Broker
- Publishen und Subscriben auf “Topics”
- “wohnzimmer/licht1 -> AN”



Vendor-spezifische Protokolle

Apple HomeKit

Amazon Smart Home API

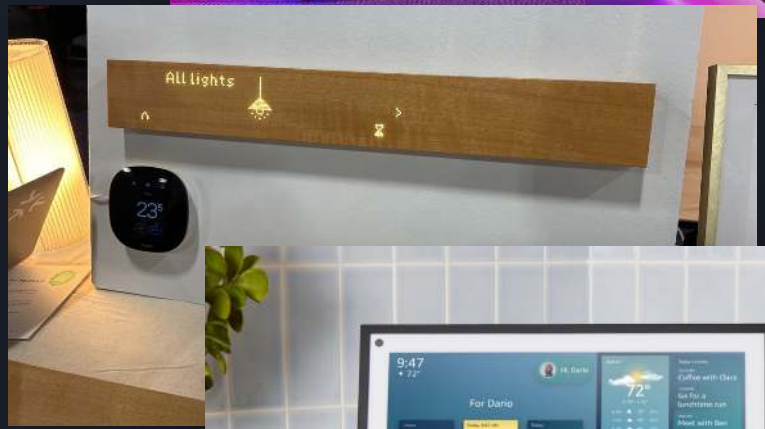
Google Home

Vendor-spezifische Protokolle

- Vordefinierte Services (Glühbirne, Rolläden) und Charakteristiken (Helligkeit, Farbe)
- Kryptographisches Pairing
- Sehr userfreundlich
- Allerdings: Vendor Lock-In

matter

- Zusammenschluss quasi aller großen Hersteller
- Initial Amazon, Apple, Google, Comcast und ZigBee Alliance
- Quelloffener, lizenzfreier Verbindungsstandard
- Aktuell großer Hype, rechts Bilder der CES2024



Herausforderungen

- Wenig Rechenleistung
  - oft schwache Krypto
  - Security by Obscurity beliebt
- Embedded Development ist *schwer*
  - Doku oft intransparent
  - SDKs umfangreich und closed source
- Keine “Standardimplementierungen”
  - Hersteller müssen selbst Software und APIs basteln
  - Meist in C/C++ (keine Memory safety)
  - Software strotzt vor Vulnerabilities

ESP8266

ESP8266-IC

Manufacturer	Espressif Systems
Type	32-bit microcontroller
CPU	Tensilica Diamond Standard 106Micro (aka. L106) @ 80 MHz (default) or 160 MHz
Memory	32 KiB instruction, 80 KiB user data
Input	17 GPIO pins
Power	3.3 V DC
Successor	ESP32

Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations

Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum and Nasir Ghani

Practical Experience Report: Exploiting Memory Corruption Vulnerabilities in Connman for IoT Devices

K. Virgil English, Islam Obaidat, and Meera Sridhar
Department of Software and Information Systems, UNC Charlotte, Charlotte, NC, USA
{kenglis8,iobaidat,msridhar}@uncc.edu

IoTFuzzer: Discovering Memory Corruptions in IoT Through App-based Fuzzing

Die Vendor-Cloud...

- Direkte Verbindung zur Cloud, keine lokale API
- Kontrolle durch Hersteller
- Erlaubt detaillierte Datenverarbeitung
- Firmware jederzeit remote austauschbar

www.tuya.com

tuya

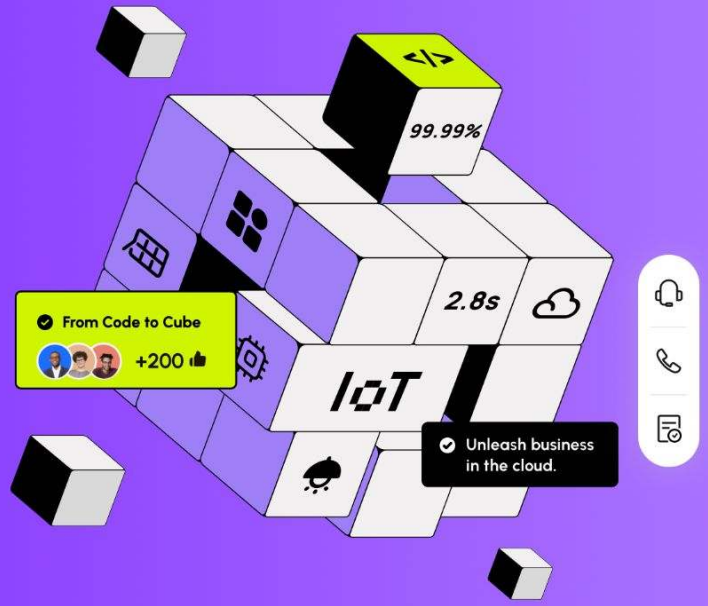
Platform Solutions Developers Services & Support Company

English Register Make IoT Easy

Create your IoT Product right now

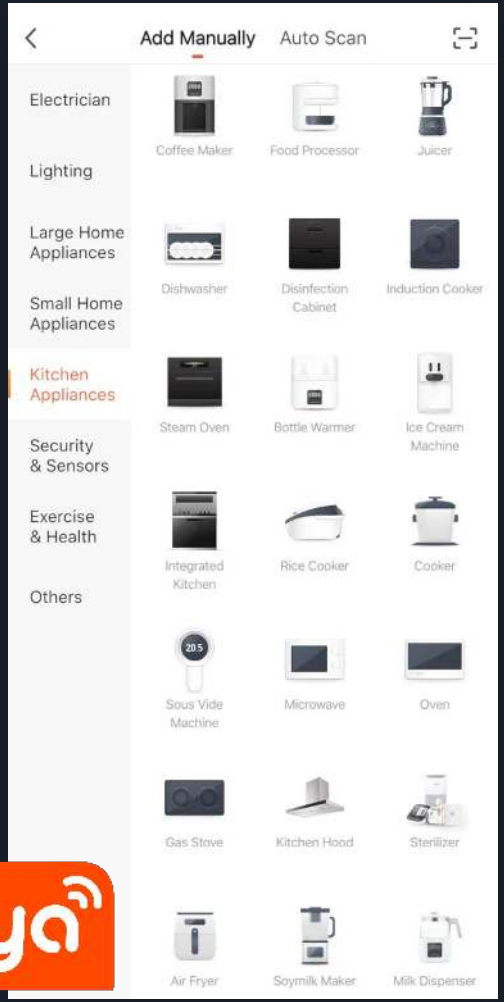
Boost IoT productivity with our decade-long proven, flexible, and open platform. Welcome to Tuya PaaS2.0.

Watch Now Contact Us



Tuya, a.k.a. “Die Cloud-Hölle”

- Plattform für Hersteller zum “Zusammenklicken” von IoT-Geräten
- Enormer Outreach, weltweit vertreten
- Geräte von verschiedensten Herstellern mit unterschiedlichen Namen verkauft
- Von Glühbirne bis Kühlschrank
- Bindet Geräte direkt in die Tuya Cloud ein



media.ccc.de/v/35c3-9723-smart_home_-_smart_hack#t=85

media.ccc.de

Search...

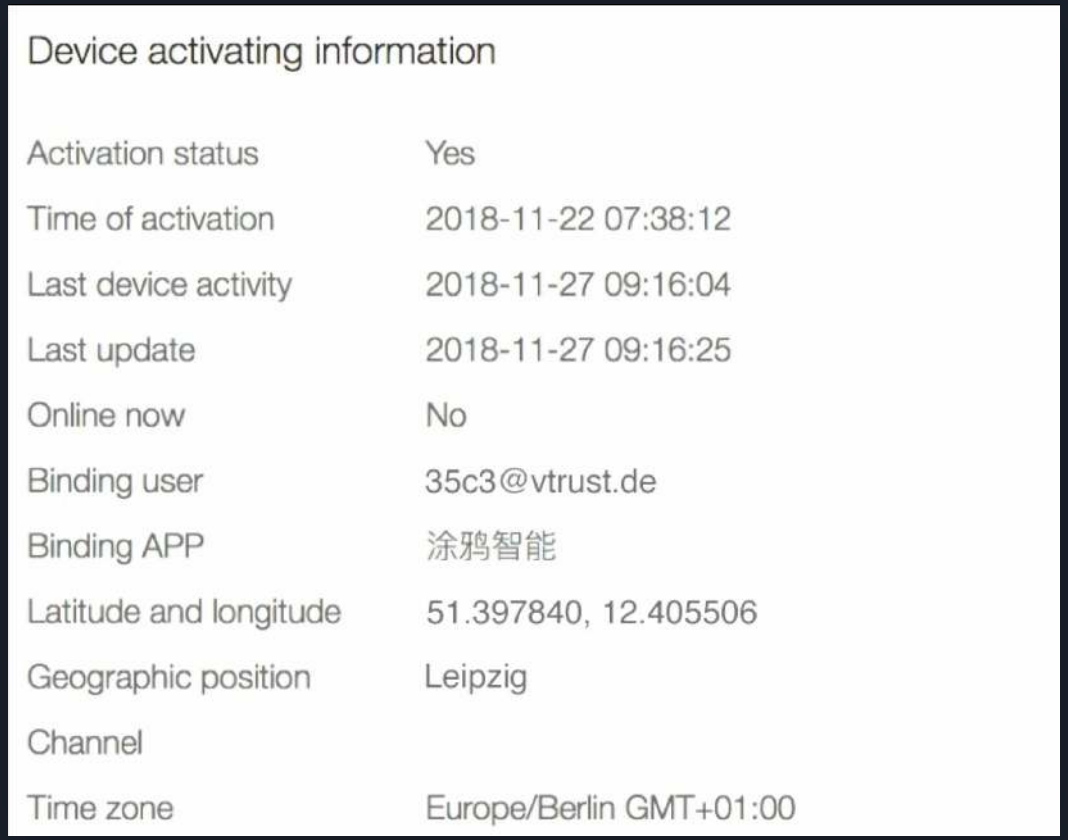
browse > congress > 2018 > event

Smart Home - Smart Hack

Wie der Weg ins digitale Zuhause zum Spaziergang wird

Michael Steigerwald

The bad, the bad and the ugly



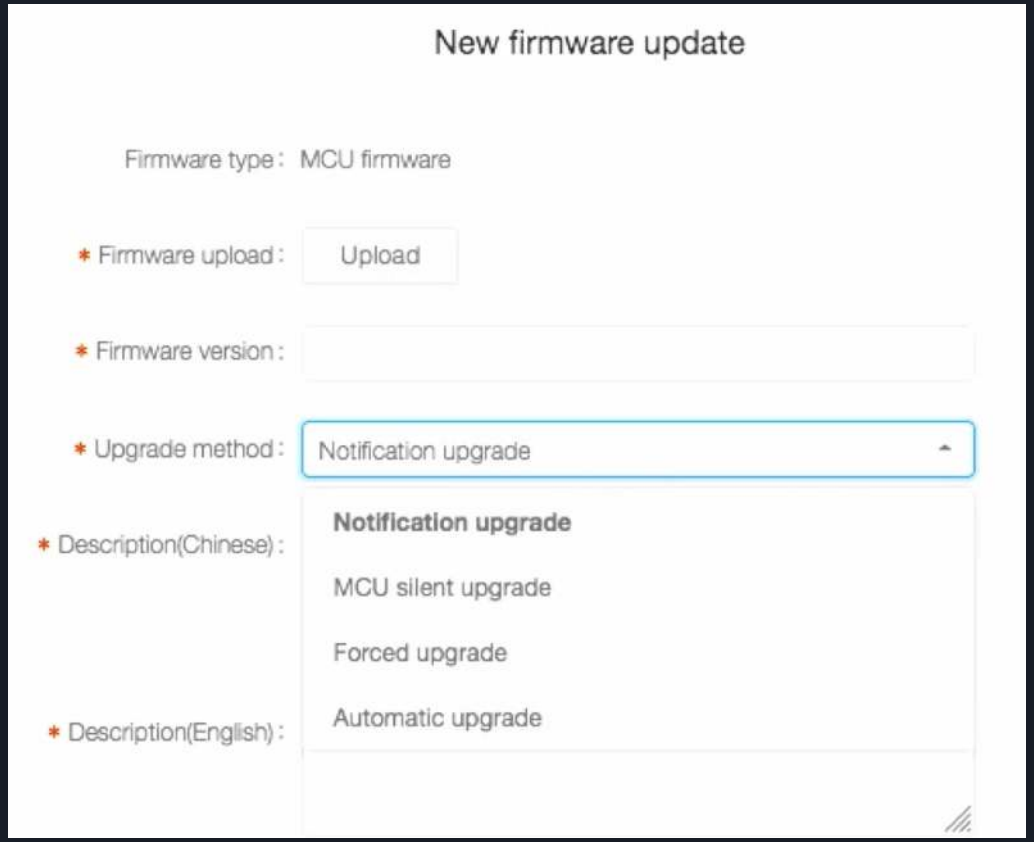
Device activating information

Activation status	Yes
Time of activation	2018-11-22 07:38:12
Last device activity	2018-11-27 09:16:04
Last update	2018-11-27 09:16:25
Online now	No
Binding user	35c3@vtrust.de
Binding APP	涂鸦智能
Latitude and longitude	51.397840, 12.405506
Geographic position	Leipzig
Channel	
Time zone	Europe/Berlin GMT+01:00

The bad, the bad and the ugly

Time	Function	Value
2018-12-21 16:43:00	Countdown 1	30s
2018-12-21 16:42:30	Countdown 1	60s
2018-12-21 16:42:00	Countdown 1	90s
2018-12-21 16:41:30	Countdown 1	120s
2018-12-21 16:40:38	Switch 1	OFF
2018-12-21 16:40:37	Switch 1	ON

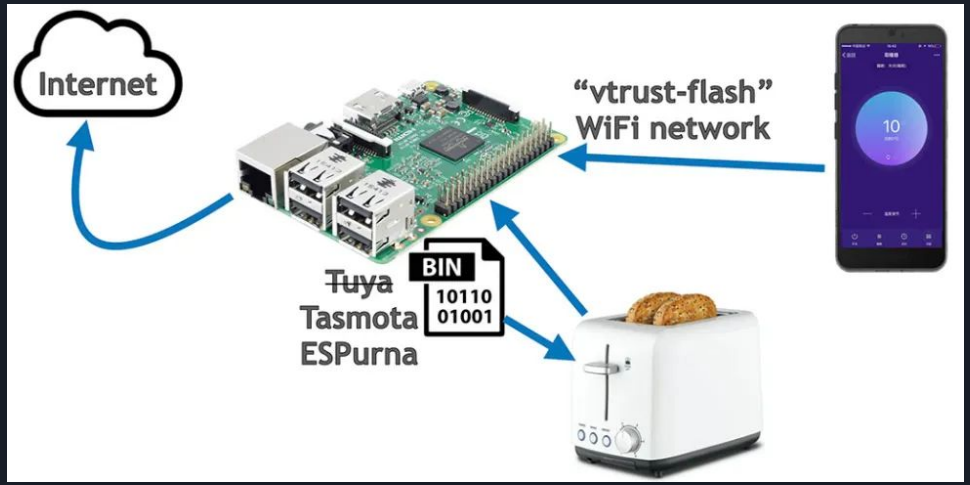
The bad, the bad and the ugly



Tuya-Convert

- Nutzt Schwachstelle in Updatemechanismus
- MITM über eigenen Access Point (RPi)
- Eigene Firmware, Tasmota, ESPHome

https://github.com/ct-Open-Source/tuya-convert



DARK CLOUDS AHEAD —

Eufy's "local storage" cameras can be streamed from anywhere, unencrypted

The URLs for accessing your camera streams are also way too easy to brute-force.

KEVIN PURDY - 12/1/2022, 9:57 PM

Local-Only in der Cloud

- Höchst irreführendes Marketing
- Kameras laden Thumbnails von Gesichtsdaten in die Cloud hoch
- Streams ohne Verschlüsselung via URL zugänglich
- URL-Schema einfach und ungesichert
- Eufy plant Änderungen in Marketing zur Cloud-Nutzung…

www.amazon.de/s?k=kamerasystem+8ch+dvr&__mk_de_DE=ÅMÅŽÕÑ&crid=HA1E15C3

amazon.de | Liefern nach Österreich | Alle | kamerasystem 8ch dvr | DE | Hallo, anmelden Konto und Listen | Warenrücksendungen und Bestellungen | 0 Einkaufswagen

Alle | Bestseller | Mehr kaufen und sparen | Amazon Basics | Musik | Angebote | Neuerscheinungen | Prime Video | Prime | Geschenkideen | Audible | Bücher | Küche, Haushalt & Wohnen | Games | Shopping-Tipps

amazon.de | Mehr kaufen und sparen

1-48 von 195 Ergebnissen oder Vorschlägen für **"kamerasystem 8ch dvr"**

Sortieren nach: Empfohlen

Berechtigt zum kostenfreien Versand

- [ ] GRATIS-Versand durch Amazon

Gratis Versand von Amazon in ausgewählte Länder

Kategorie

Videoüberwachungstechnik
- DVR-Videoüberwachungs Sets
- Überwachungskameras
- Videorekorder für Überwachungstechnik

Komplettsysteme

Kundenrezension

★★★★☆ & mehr
★★★☆☆ & mehr
★★☆☆☆ & mehr
★☆☆☆☆ & mehr

Marke

- [ ] Reolink
- [ ] ZOSI
- [ ] SANNCE

Preis

115 EUR – 970 EUR & mehr

Los

100 bis 200 EUR
200 EUR & mehr

Angebote & Ersparnis

Alle Angebote

Ergebnisse

Erfahre mehr über diese Ergebnisse. Preis und weitere Details sind von Größe und Farbe des Produkts abhängig.

ANNKE Überwachungskamera Set 8CH 3K Lite DVR mit 4 System 1080P CCTV-Überwachungskamera IP66...

★★★★☆ 45

191 59 €

Spare 10,00 € mit Rabattgutschein

✓prime Lieferung bis **Freitag, 19. Januar**

KOSTENFREIER Versand durch Amazon

Nur noch 4 auf Lager

Andere Angebote
189,99 € (1 neuer Artikel)

ZOSI 8CH 1080P Überwachungskamera Set mit Kabel, 8CH 1TB DVR und 4X Aussen Dome...

★★★★☆ 37

Befristetes Angebot

161 34 € Statt: ~~201,67€~~

Spare 20,00 € mit Rabattgutschein

Andere Angebote
149,99 € (4 gebrauchte und neue Artikel)

Xenocam 8CH 1080N Hybrid 5-in-1 AHD DVR (1080P NVR+1080N AHD+960H Analog+TVI+CVI) Standalone...

67 55 €

✓prime Lieferung bis **Freitag, 19. Januar**

KOSTENFREIER Versand durch Amazon

Nur noch 14 auf Lager

Andere Angebote
66,99 € (1 neuer Artikel)

ZOSI 1080P HD CCTV Überwachungssystem Videoüberwachung Set 8CH 4in1 H.265+ DVR mit 4...

★★★½☆ 39

131 09 €

Spare 5 % bei 2 ausgewählten Artikeln

✓prime Lieferung bis **Freitag, 19. Januar**

KOSTENFREIER Versand durch Amazon

Nur noch 5 auf Lager

Andere Angebote
129,99 € (3 neue Artikel)

Anlapus 1080P Außen Video ...

★★★★☆ 733

131 09 €

Spare 15,00 € mit Rabattgutschein

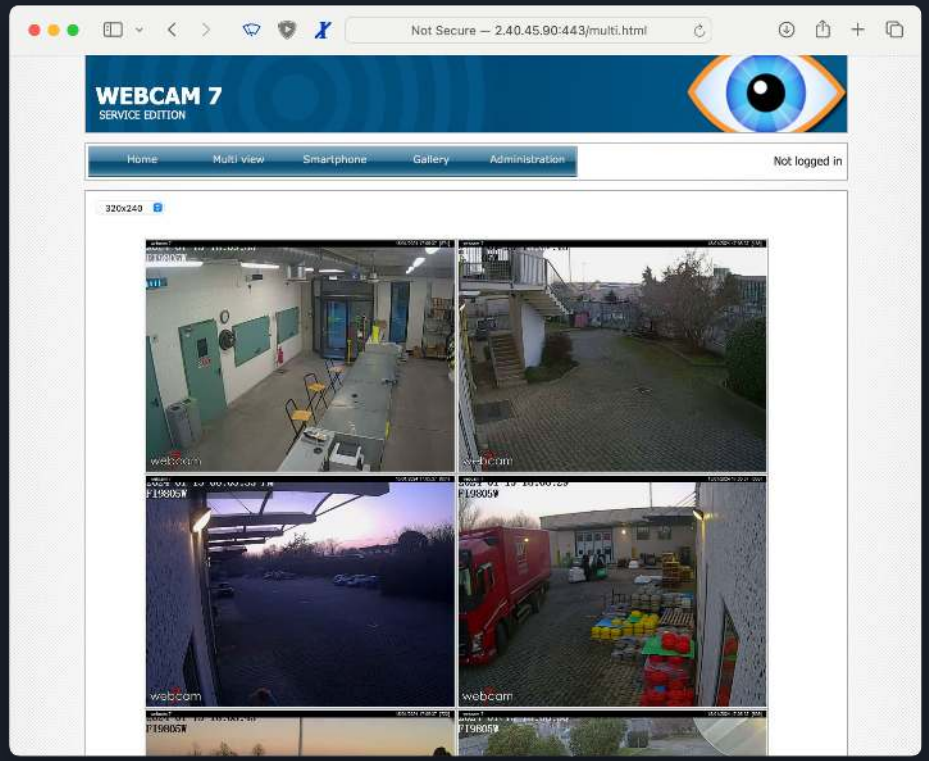
✓prime Lieferung bis **Freitag, 19. Januar**

KOSTENFREIER Versand durch Amazon

Andere Angebote
129,99 € (1 neuer Artikel)

CCTV-Recorder

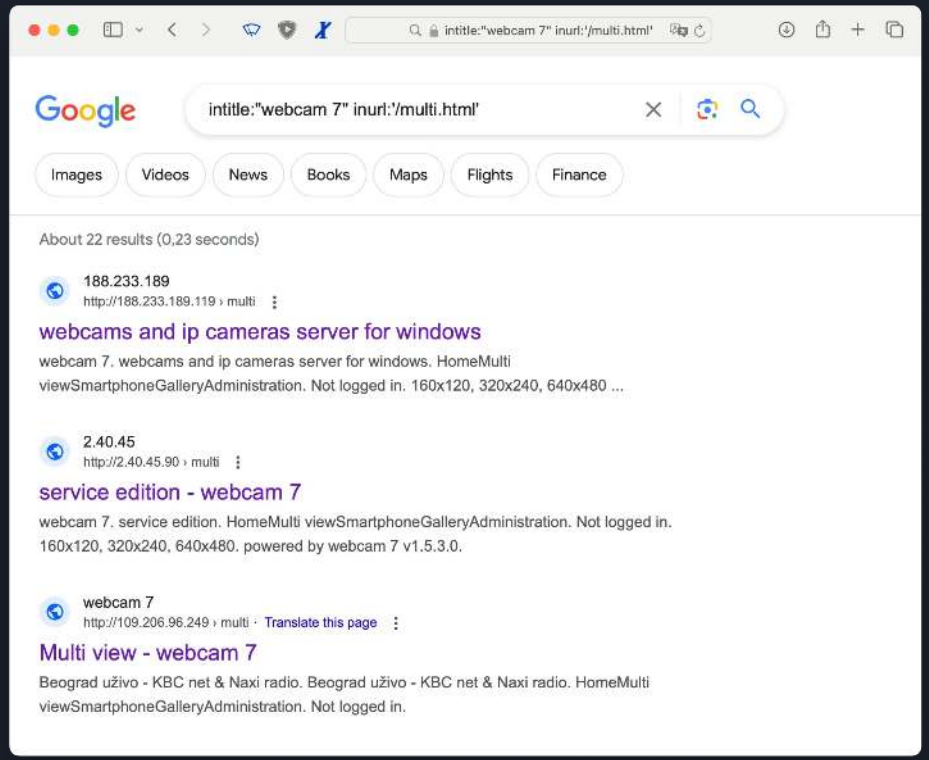
- Über Internet erreichbar
  - “semi-gewünscht”
- NAT Hole Punching
  - UPnP
  - Manuell
- Meist ohne Passwort
  - wenn überhaupt, Standardpasswörter



Google-Dorking

- Suchmaschinen-Crawler finden Admin-Panels
- Suche nach bekannten Fenstertiteln, URLs
- Zero “Exploitation Effort”

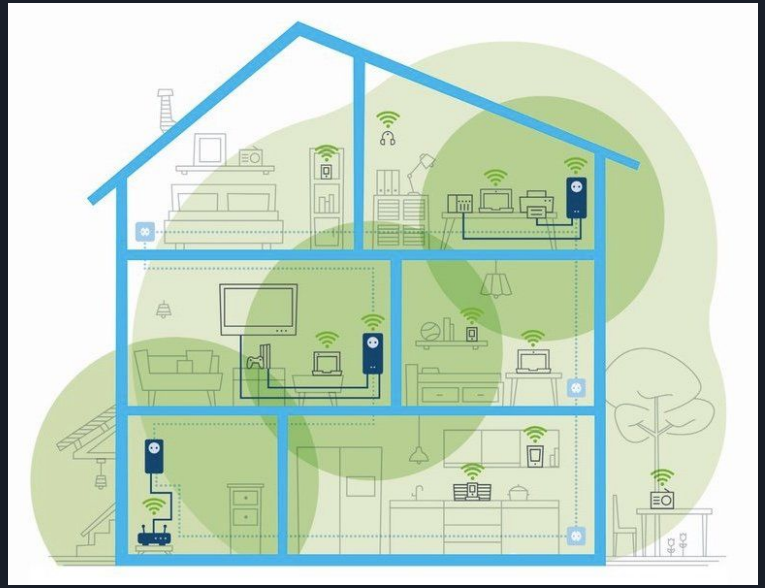
https://www.exploit-db.com/google-hacking-database?category=13



Transport-Layer

Warum Wireless?

- Einfache Installation
  - Retrofitting
  - Netzwerkintegration
  - Skalierbarkeit
- Flexibilität/Mobilität
- Geringer Wartungsaufwand
  - “Höchstens” Batteriewechsel



Sub-GHz

z.B.: 433.92 MHz

Vorteile:

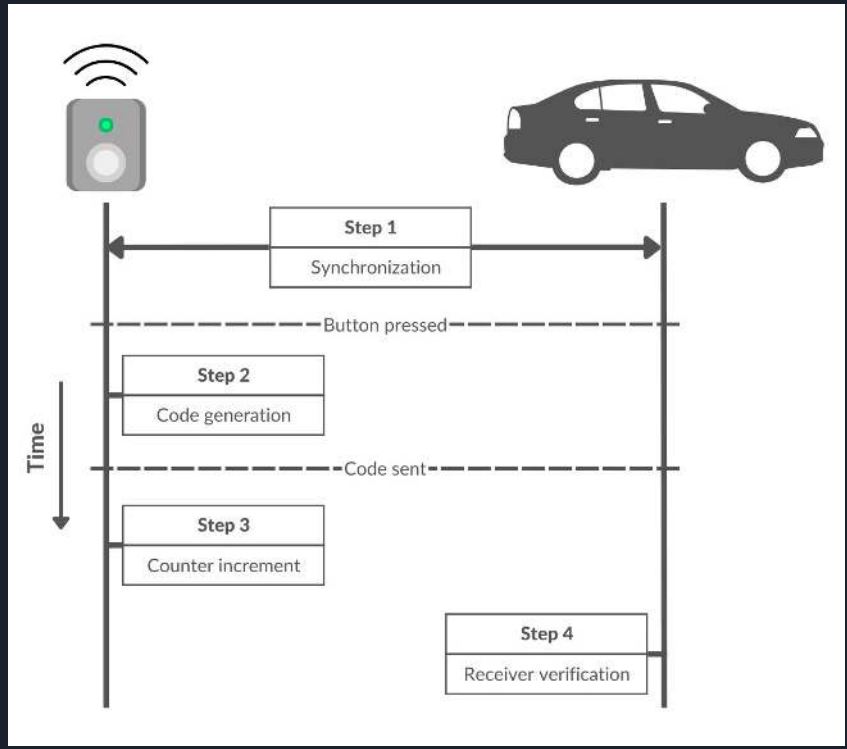
- Hohe Reichweite
- Gute Durchdringung
- Energieeffizient
- Sehr einfach

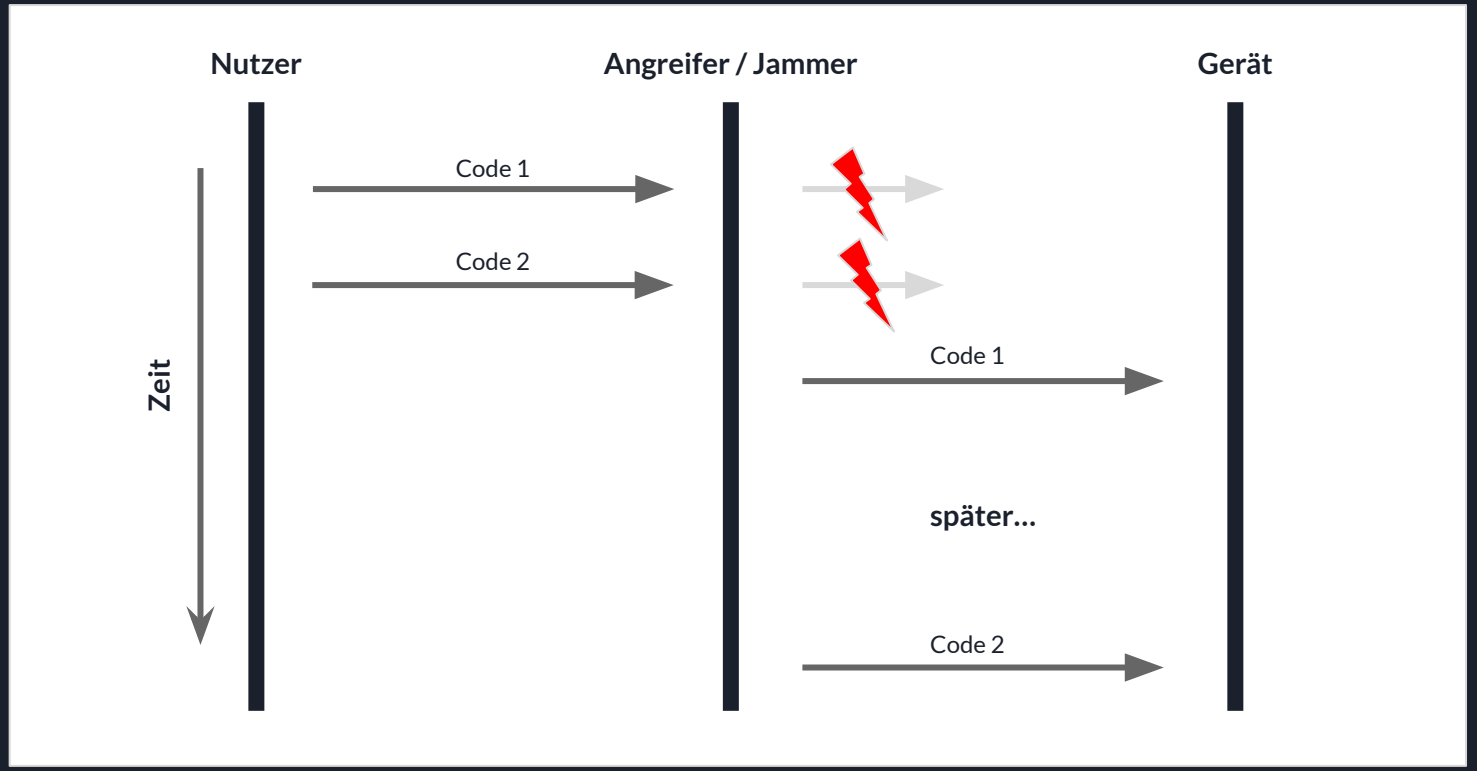
Nachteile:

- Geringere Datenraten
- Sicherheit

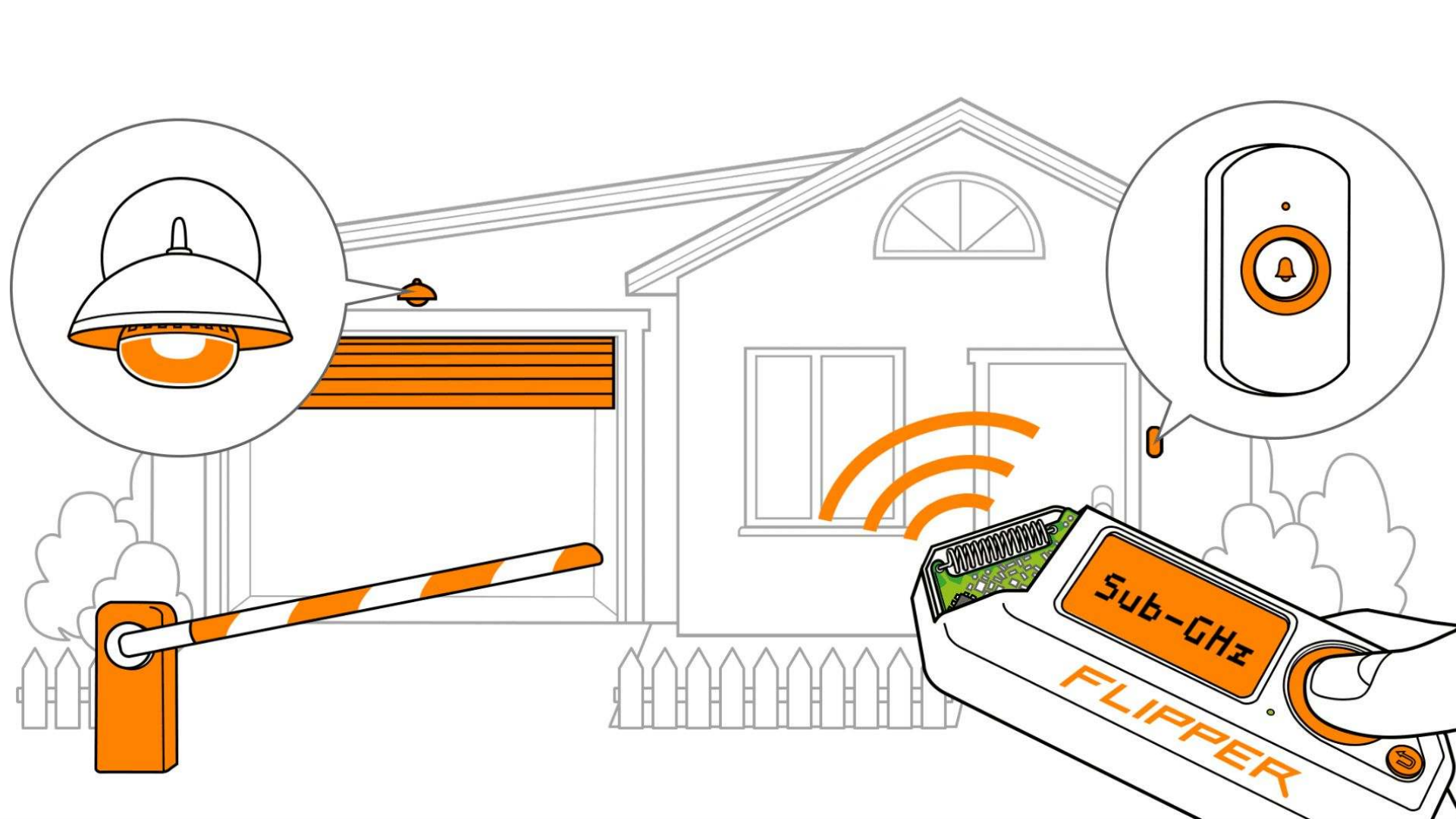
Sub-GHz sicher?

- Komplett “unverschlüsselt”
  - z.B: Steckdosen- / Klimagerät- / Lampen-Steuerungen
- Replay Attacks sehr einfach
- Sicherer mit Rolling-Codes
  - Bypassbar mit Jamming

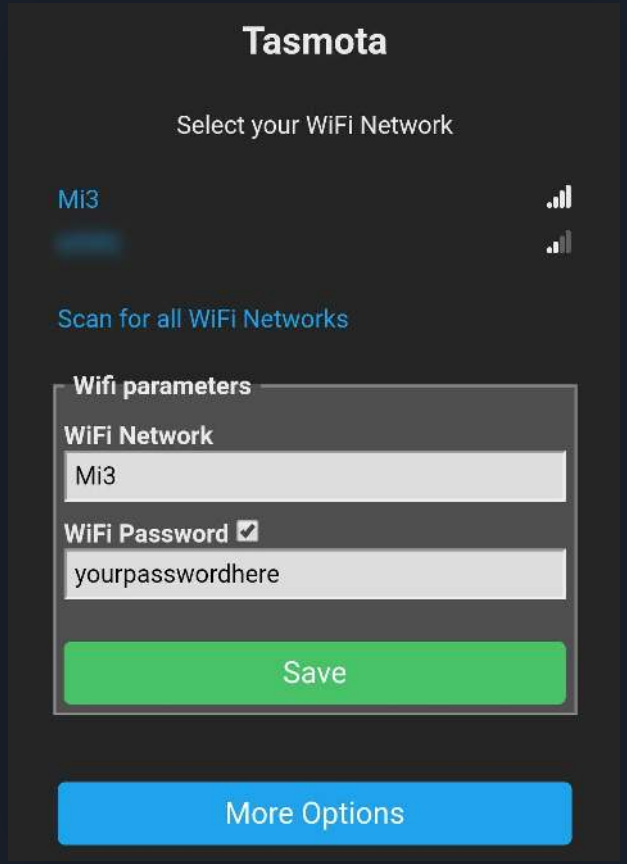




Jamming-Attacke (vereinfacht)


Sub-GHz
FLIPPER

- “Kennt man, macht man”
- Aber: Kompliziert, Krypto aufwendig
- Pairing über Captive Portal
  - Kann stellenweise mit Jamming übernommen werden
- Vendors liefern oft keine Updates
  - z.B. Arduino-SDK von ESP8266 kann kein WPA3 (kommt auch nicht mehr)



BUSINESS & TECHNOLOGY

WPA2 Has Been Broken. What Now?

By Bill McGee | October 16, 2017

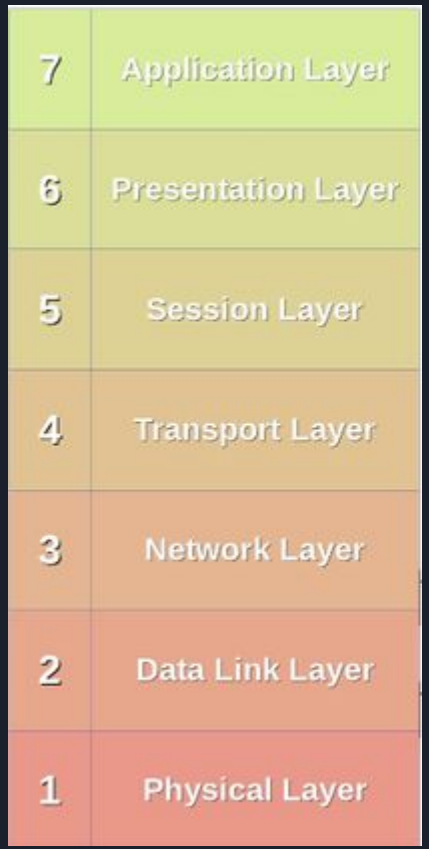
Early Monday morning it was announced that WPA2, WiFi's most popular encryption standard, had been cracked. A new attack method called KRACK (for Key Reinstallation AttaCK) is now able to break WPA2 encryption, allowing a hacker to read information passing between a device and its wireless access point using a variation of a common – and usually highly detectable – man-in-the-middle attack. If successful, this vulnerability can potentially allow a hacker to spy on your data as well as gain access to unsecured devices sharing the same WiFi network.

Of course, as computing power grows, it was just a matter of time before another encryption protocol was broken. In this case, Belgian security researchers at KU Leuven university, led by security expert Mathy Vanhoef, discovered the weakness and published details of the flaw on Monday morning.

Essentially, KRACK breaks the WPA2 protocol by "forcing nonce reuse in encryption algorithms" used by Wi-Fi. In cryptography, a nonce is an arbitrary number that may only be used once. It is often a random or pseudo-random number issued in the public key component of an authentication protocol to ensure that old communications cannot be reused. As it turns out, the random numbers used on WPA2 aren't quite random enough, allowing the protocol to be broken.

zigbee

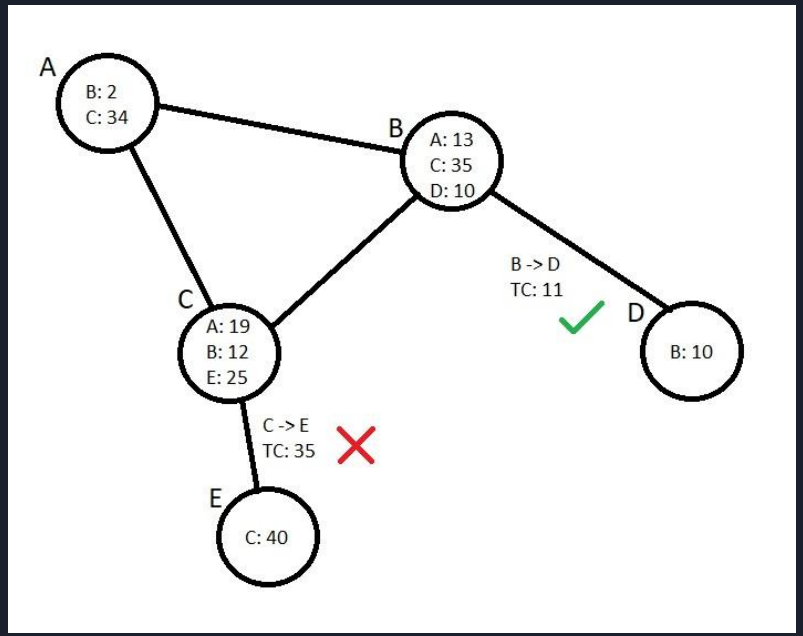
- Aufbau auf IEEE 802.15.4 (Definiert OSI Layer 1 und 2)
- Zigbee selbst definiert noch Layer 3 und 4
- Operiert auf ISM-Band (2,4 GHz, 915 MHz oder 868 MHz)
- Low-Power-Übertragung durch CSL (Coordinated Sampled Listening)



Verhindern von Replay Attacken

32 Bit transmission counter (TC) im Header

- Nodes speichern letzten bekannten TC aller Nachbarn
- Wird bei neuen Paketen aktualisiert
- TC von Nachricht kleiner als erwartet -> Paket wird verworfen



- Symmetrische 128-bit Schlüssel, basierend auf AES
  - Link Keys (für Unicast, auf je 2 Geräten)
  - Network Key (für Broadcasts, gleich auf allen Geräten)
- Trust Center:
  - meist der Router/Hub
  - zuständig für Sicherheit (Key distribution, Konfiguration, etc...)
- Trust Center Link Key
  - Verschlüsselt von Trust Center ausgehende Packete

TCLK Default Value

5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39

Z i g B e e A l l i a n c e 0 9

Meistens hard-coded.

"During initial key transport the keying material used for protection may be a well-known key, thus resulting in a brief moment of vulnerability where the key could be obtained by any device."

- Zigbee Alliance 2017

THREAD

- Aktuell am Aufschwung
- Entwickelt von der Matter-Group
  - Nativer Physical Layer
- “No Single Point of Failure”
  - Mesh-Architektur
  - Mehrere Border-Routers
- Nutzt 6LoWPAN
- OpenThread Bugtracker auf GitHub

Hardware-Layer

Hardware is secure, as long as nobody can touch it

Grundannahme: Firmware ist “firm”

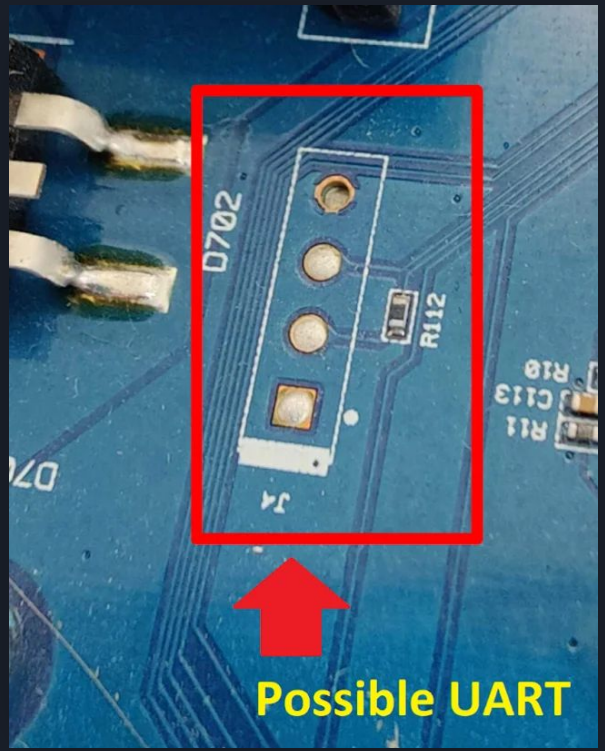
Erfordert:

- ROM schreibgeschützt
- Firmware signiert
- Kein Zugriff über
  - Konsole
  - SSH
  - Debug-Protokolle

(Das eine, obligatorische ChatGPT-Bild)

UART - Serielle Schnittstelle

- Vier Kabel
  - Spannung
  - Ground
  - Receive
  - Transmit
- Konsole am Gerät, meist ungesichert
- Von Debug Features bis Reflashing
- Rooting ”Speedrun Challenge”



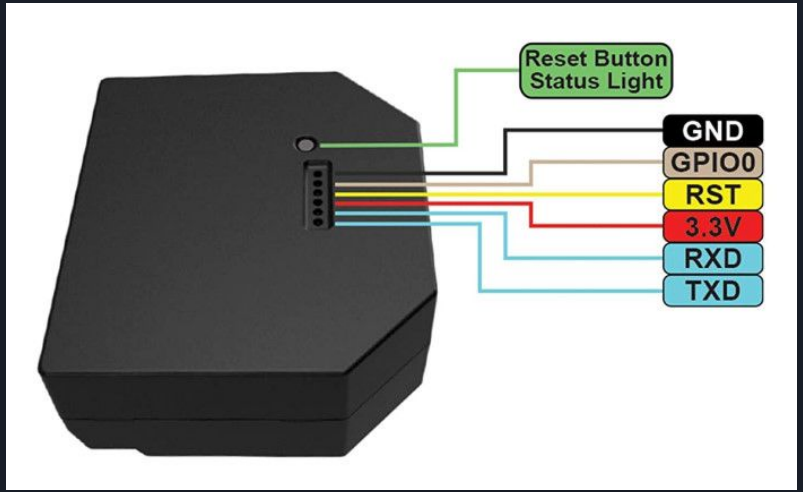
```
SONIX (main)>:
system

date              - Get/Set date time
phymem_rw         - read/write ASIC register
fps               - Get current frame rate
padio             - Get PADIO Config
wdt               - Watch Dog Timer Control
usbd              - USB Device Control
help              - Show usage message
back              - Back to prev level

SONIX (system)>:
SPK ON
```

Youtube: Low Level Learning

i hacked my son's baby monitor, for science.

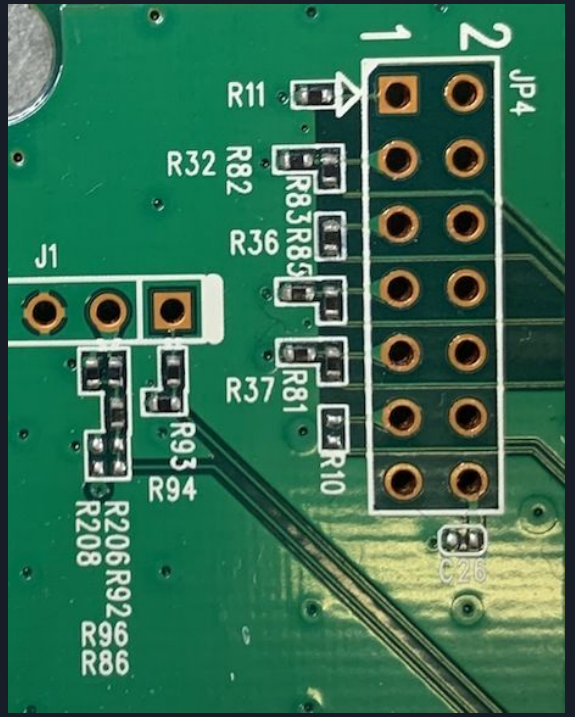
UART - Reflashing

- Bei vielen Chipsets “Standard-Feature”
- ESP8266, ESP32 etc.
- Firmware Download Mode über Knopf / Pin
- Abgesehen von Lötarbeit sehr schnell und einfach



JTAG Debug Interface

- Standardisierte Firmware- / PCB-Debug-Schnittstelle
- Typischerweise fünf oder mehr Pins
  - Test Data In (TDI)
  - Test Data Out (TDO)
  - Test Clock (TCK)
  - Test Mode Select (TMS)
  - Optional: Test Reset (TRST)
- Varianten: 2-Wire JTAG, SWD, etc.
- Hardware Zugriff auf Flash, Register etc.
- Firmware Down- und Uploads



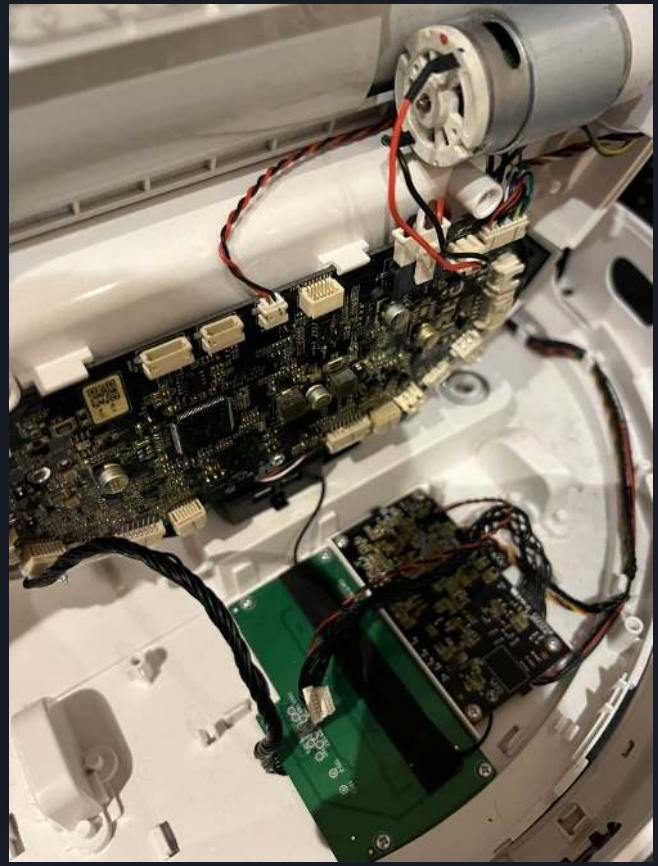
Viele Angriffsvektoren

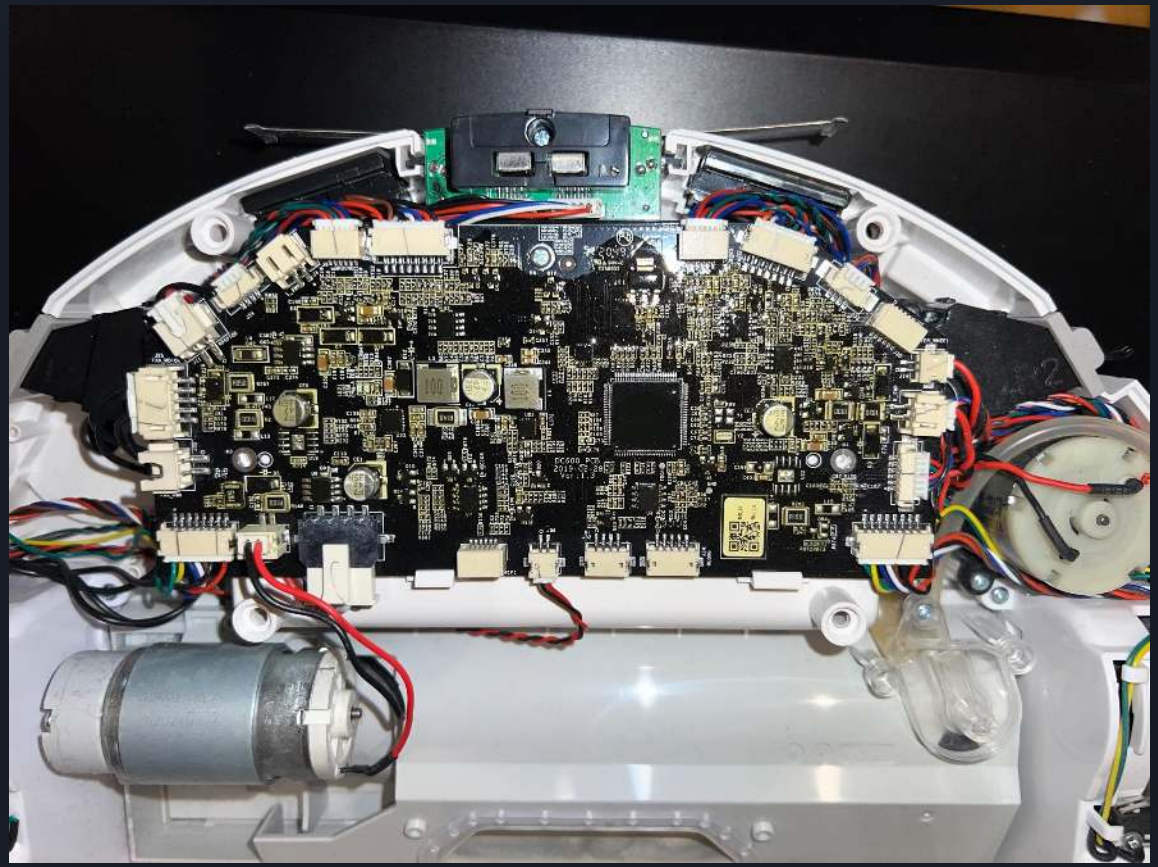
- Backdoor in private Netzwerke
- Illegaler Traffic (DDOS-Botnets, etc.)
- Einschleusung von Malware
- Ausspähen der Nutzer (“Wann zuhause”)

In Umlauf bringen trivial

- Gebrauchtmarkt
- Retouren
- Verschenken

Eufy RoboVac L70 Hybrid - a.k.a “Saugi”





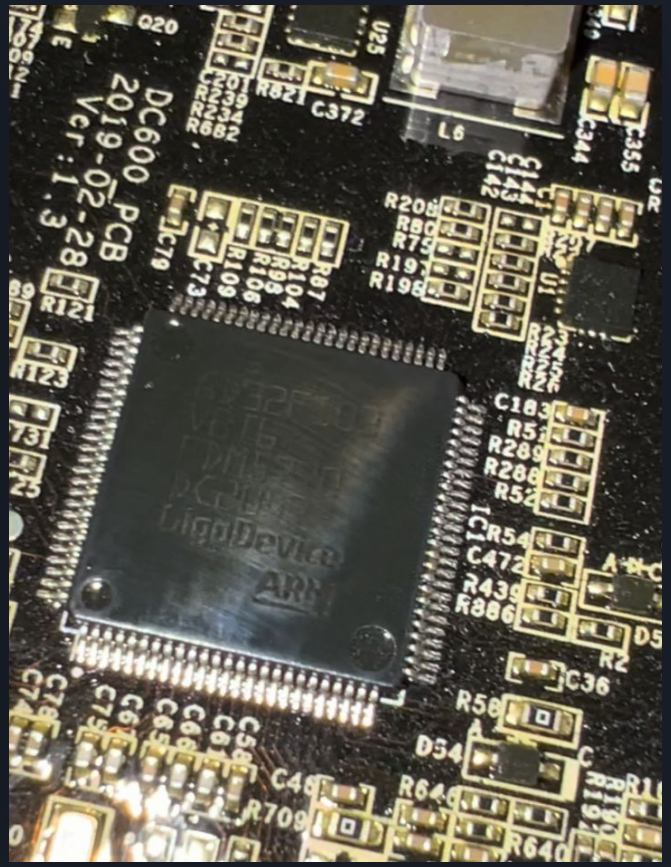
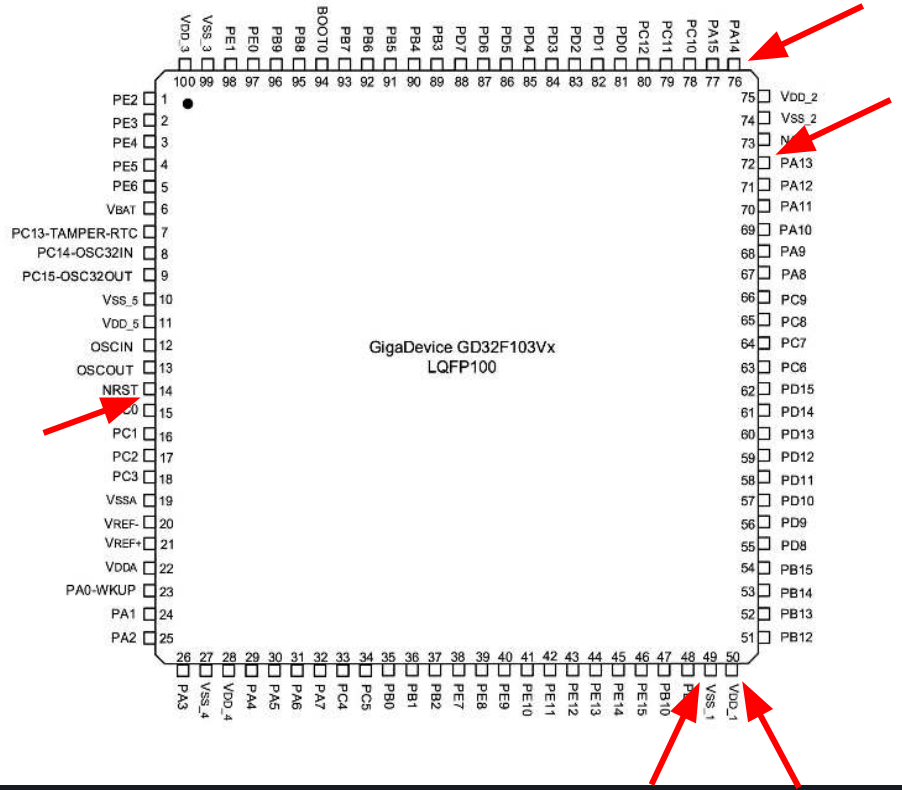
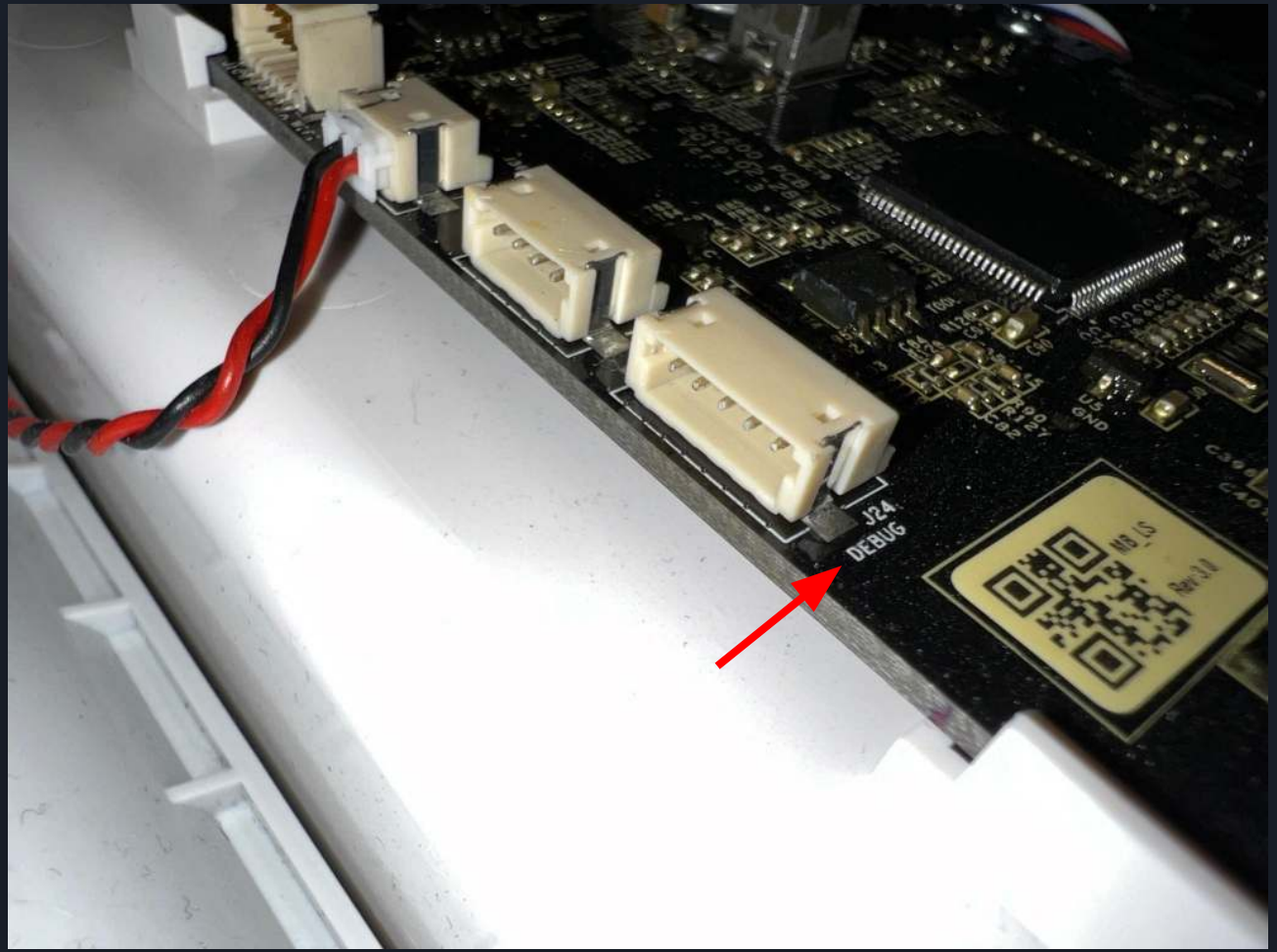

DC600
2019-02-28
PCB
Ver:1.3
GigaDevice

Figure 2-4. GD32F103Vx LQFP100 pinouts



PA8	67	I/O	5VT	Alternate: USART0_CK, TIMER0_CH0, CK_OUT0, USBFS_SOF
PA9	68	I/O	5VT	Default: PA9 Alternate: USART0_TX, TIMER0_CH1, USBFS_VBUS
PA10	69	I/O	5VT	Default: PA10 Alternate: USART0_RX, TIMER0_CH2, USBFS_ID
PA11	70	I/O	5VT	Default: PA11 Alternate: USART0_CTS, CAN0_RX, USBFS_DM, TIMER0_CH3
PA12	71	I/O	5VT	Default: PA12 Alternate: USART0_RTS, USBFS_DP, CAN0_TX, TIMER0_ETI
PA13	72	I/O	5VT	Default: JTMS Remap: PA13
NC	73			-
VSS_2	74	P		Default: VSS_2
VDD_2	75	P		Default: VDD_2
PA14	76	I/O	5VT	Default: JTCK Remap: PA14
PA15	77	I/O	5VT	Default: JTDI Alternate: SPI2_NSS, I2S2_WS Remap: TIMER1_CH0_ETI, PA15, SPI0_NSS
PC10	78	I/O	5VT	Default: PC10 Alternate: UART3_TX Remap: USART2_TX, SPI2_SCK, I2S2_CK
PC11	79	I/O	5VT	Default: PC11 Alternate: UART3_RX Remap: USART2_RX, SPI2_MISO
PC12	80	I/O	5VT	Default: PC12


J24
DEBUG

Fazit

Wie kann ich mich schützen?

IoT-Geräte mit Hausverstand einsetzen:

- Local-Only - weniger Angriffsfläche
- Vendor-Clouds sind gefährlich
- Keine veralteten Funkstandards
- IoT in eigenes VLAN
- Vorsicht am Gebrauchtmarkt

Open-Source-Alternativen: