

# Forensik im Smart-Home: Was weiß das Haus über seine Bewohner?

Ringvorlesung Cybersicherheit  
Hessisches Ministerium des Inneren und Heimatschutz  
Wiesbaden

Prof. Dr. Marc Stöttinger  
12.12.2024

# VORSTELLUNG

Marc Stöttinger

- Hintergrund:
  - Studium: Elektro- und Informationstechnik – TU Darmstadt
  - Promotion: Technische Informatik – TU Darmstadt, CASED
  - Post-Doc: Cryptographic Engineering -TemasekLabs@NTU
- Berufserfahrung:
  - Senior Hardware Security Expert bei Continental AG
  - Security Analyst im Landes CERT Hessen (Hessen3C)
  - Professor für Technische Informatik und Security an der Hochschule RheinMain
- Forschungsinteressen:
  - Post-Quanten Kryptographie
  - Hardware Sicherheit
  - Embedded Security



# AGENDA

- Motivation
- Smart-Home Geräte und Strukturen
- Forensik im Bereich Smart-Home
- Fallstudie zu einem Smart-Home System
- Zusammenfassung und Ausblick

# MOTIVATION

Wer von Ihnen hat einen Smart Speaker daheim?

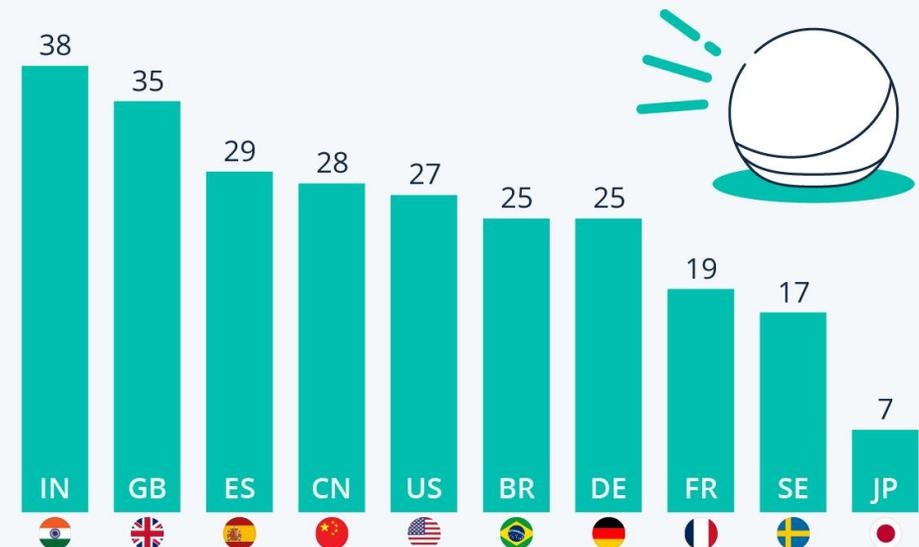
# MOTIVATION

## Schöne neues Zuhause

- Moderne Haushalte haben heutzutage immer mehr digitale Helferlein.
- Mit Hilfe von Smart Speaker Diensten von z.B. Alexa, Siri oder Google Assist werden immer mehr Geräte daheim gesteuert.
- Hierbei kommen die Fragen auf:
  - Wird permanent mitgehört?
  - Wer hört mit?
  - Wo und wie lange werden meine Daten gespeichert?
- Neben den Smart Speakern gibt es auch anderen Sensoren im Smart Home Bereich, die Daten über die Bewohner sammeln.

## Jede:r vierte Deutsche nutzt smarte Lautsprecher

Anteil der Befragten, die einen Smart Speaker besitzen (in %)



Basis: 2.000-10.000 Befragte (18-64 Jahre) je Land; Apr 2023-Mär 2024

Quelle: Statista Consumer Insights



**statista** 

Quelle: <https://de.statista.com/infografik/28745/anteil-der-befragten-die-einen-smart-speaker-besitzen/>

# SMART HOME

## Nutzen von SMART-Speaker zur Aufklärung von Kriminalfällen

- Transskripte und Daten von Smart Speakern dürfen für einige Delikte bei Gerichtsverfahren genutzt werden:
  - Tötungsdelikte
  - Gewaltdelikte
  - Vermögensstraftaten
  - Betrug
  - Geldwäsche
  - Doping
  - Falsche Asylverfahren

NEWS

### Alexa klärt Totschlag auf: Deutsches Gericht überführt Täter mit Echo-Aufnahmen

Zwei Sprachaufnahmen, die ein Echo-Gerät im Schlafzimmer machte, konnten nun dazu genutzt werden, einen 54-Jährigen zu überführen, der seine Ex-Freundin beim Sex erwürgt hatte. Amazon übergab die Daten freiwillig an die Staatsanwaltschaft.

Von **Dieter Petereit**

23.12.2020, 14:15 Uhr • ⌚ 2 Min.



Quelle: <https://t3n.de/news/alexa-aufnahmen-taeter-amazon-echo-1346525/>



# SMART HOME

Was ist eigentlich Smart Home?

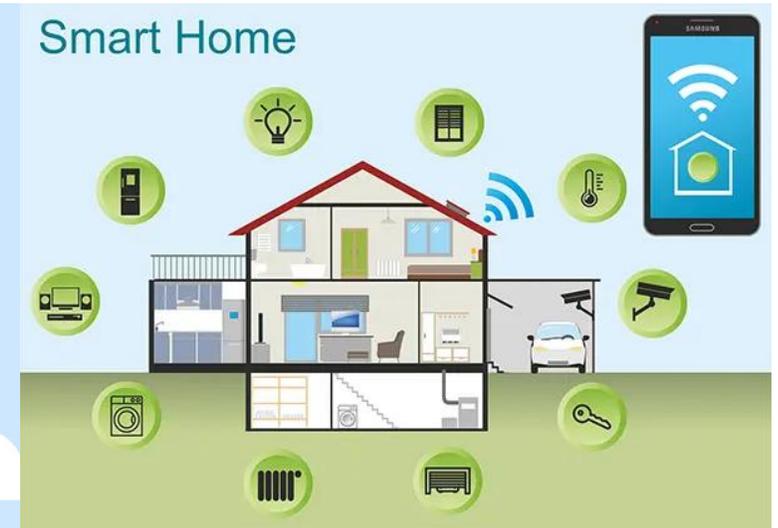
# SMART HOME

## Sensoren und Aktoren im Smart-Home Bereich

- Smart-Home ist keine Gebäudeautomatisierung:
  - Smart-Home fokussiert sich auf den Nutzer in den eigenen vier Wänden
  - Gebäudeautomatisierung fokussiert sich auf das Management des kompletten Gebäudes
- **Beispiel:** Gebäude Automatisierung sorgt für einen gleichmäßigen Betrieb der Heizung und stellt die Vorlauftemperatur sicher. Smart-Home kann das Thermostat nach entsprechenden Szenarien (Werktage/ Wochenende) einstellen.



Quelle: <https://www.mouser.de/design-with-infineon-smart-solutions/c>

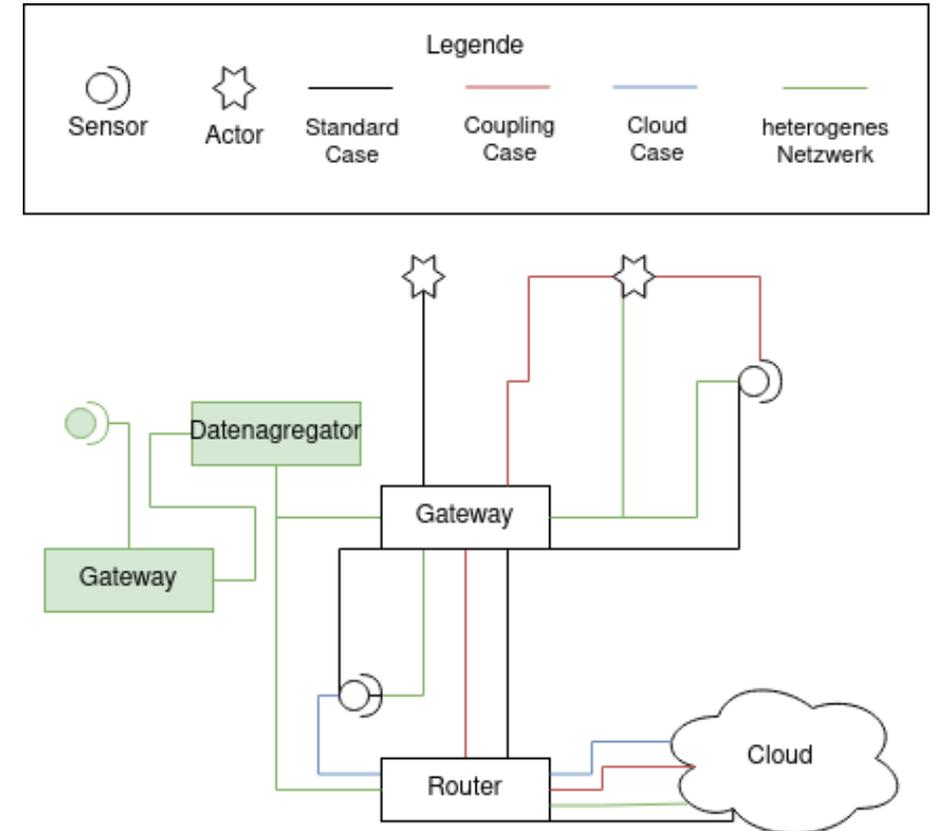


Quelle: <https://www.gatewayfiber.com/blog/how-much-internet-speed-do-you-need-for-a-smart-home/>

# SMART HOME

## Smart-Home Netzwerk-Topologien

- Verschiedenen Netzwerk Topologien möglich:
  - Gerät-zu-Gateway, Gerät-zu-Gerät, Gerät-zu-Cloud und alle Mischformen ...
- Verschiedene Kommunikationstechniken:
  - Wifi, Bluetooth, ZigBee, 434Mhz, 868 Mhz, Z-Wave, ...
- Verschiedene Kommunikationsprotokolle:
  - 802.11 b/g/n, Bluetooth 4.2 mit BLE, IO, RTS, ENOcean, KNX, BMX, M-Bus, Modbus, ...
- Standardisierungsbestrebungen mit Matter vorhanden, allerdings noch nicht realisiert



# SMART HOME

## Sensoren und Aktoren

- Sensoren:
  - Temperatursensor
  - Luftfeuchtigkeitssensor
  - Bewegungsmelder
  - Tür- und Fensterkontakte
  - Leistungsmesser
  - Smart Speaker, ...
- Aktoren:
  - Schaltbare Steckdosen
  - Thermostate
  - Smart Lights
  - Motoren für Jalousien oder Rollläden
  - Smart Speaker, ...



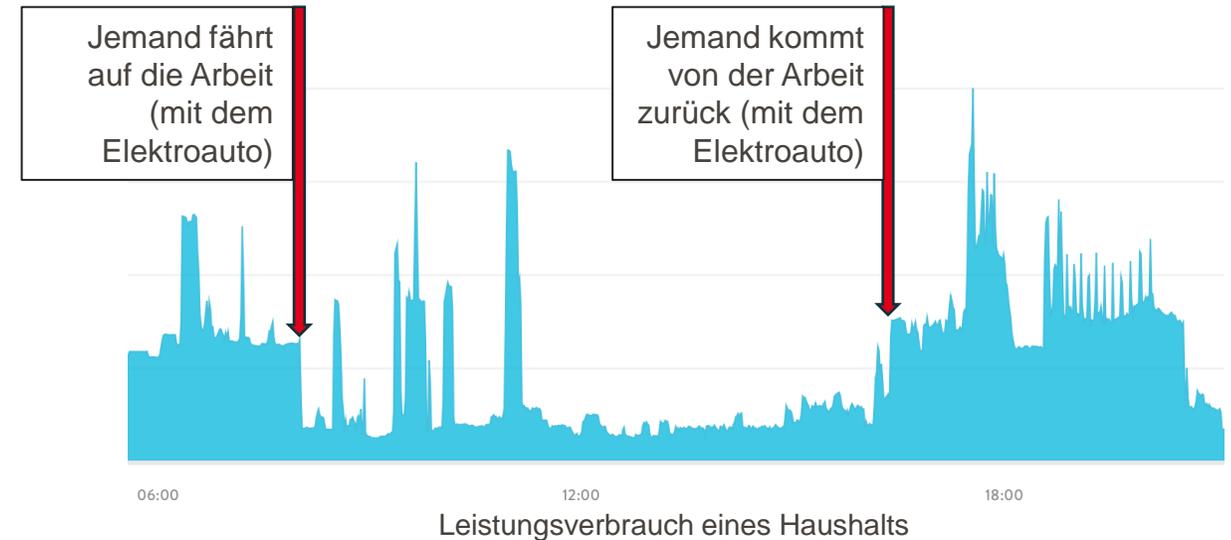
# FORENSIK IM BEREICH SMART-HOME

Warum sind SMART-Home Geräte interessant für die forensische Analyse?

# FORENSIK IM BEREICH SMART-HOME

## Relevante Sensordaten und Aktordaten

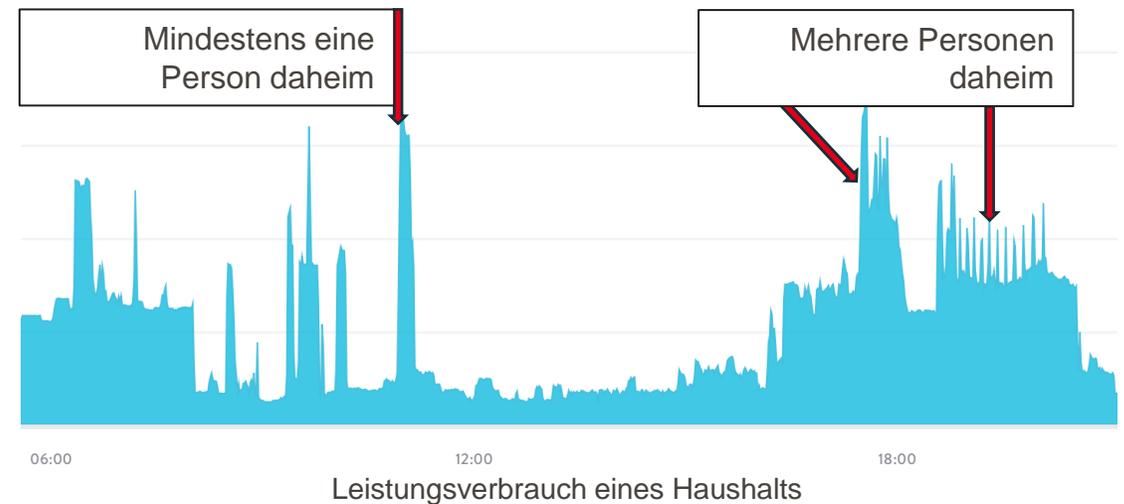
- Sensor- und Aktordaten können Rückschlüsse auf die Umgebung und Beteiligte zum Zeitpunkt der Tat geben:
  - Temperatursensor
  - Luftfeuchtigkeitssensor
  - Bewegungsmelder
  - Tür- und Fensterkontakte
  - Taster
  - Leistungsmesser
  - (Videomaterial von Kameras)



# FORENSIK IM BEREICH SMART-HOME

## Relevanz von Smart-Home für Forensik

- Rekonstruktion des Tathergangs mit Hilfe von Daten von Smart-Home Geräten:
  - Feststellen der physikalischen Umgebungsbedingungen zum Tatzeitpunkt – Raumtemperatur Todeszeitpunkt
  - Nachweis von der Präsenz von Personen – Betätigung eines Lichtschalters
  - Rekonstruktion des Tathergangs – Öffnen einer Tür oder Fensters im Einbruchfall
  - Nachweis des Vorsatzes durch Feststellen von Manipulationen – Änderung oder Löschung von Daten





# FORENSIK IM BEREICH SMART-HOME

## Forensische/Kriminalistische Herausforderungen

- Das Auffinden der Geräte im Netzwerk und physikalisch
- Nur beschränkt kommerzielle Werkzeuge vorhanden – Individuelle Analysetoolentwicklung
- Meistens Datenspeicherung irgendwo in der Cloud - Hoheitsgebiet in dem die Daten gespeichert werden außerhalb der Zuständigkeit
- Schlecht geschützte Kommunikation im Smart-Home Netzwerk – Authentizität der Daten ist eventuell fragwürdig

## DATENFREUNDE

Quelle: <https://datenfreunde.com/projects/smart-home-forensic-kit>



Quelle: <https://www.magnetforensics.com/de/products/magnet-axiom>



**AUTOPSY**  
DIGITAL FORENSICS

Quelle: <https://www.autopsy.com>

Basiert auf den Quelle:  
<https://www.polizei.hessen.de/icc/internetzentralQA/nav/95a/broker.jsp>  
<https://pixabay.com/de/vectors/belgien-land-europa-flagge-grenzen-1758814/>

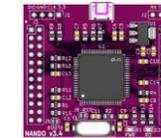
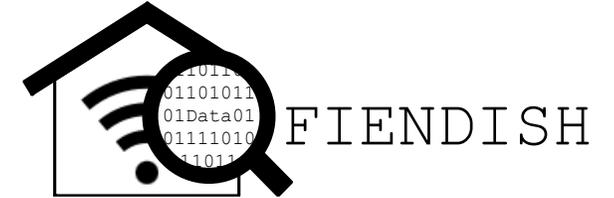


# FORENSIK IM BEREICH SMART-HOME

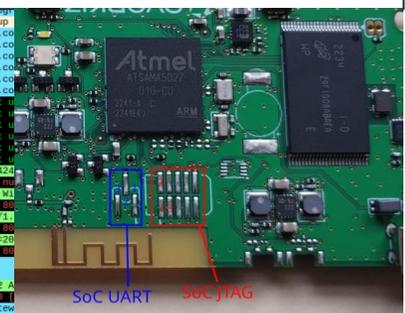
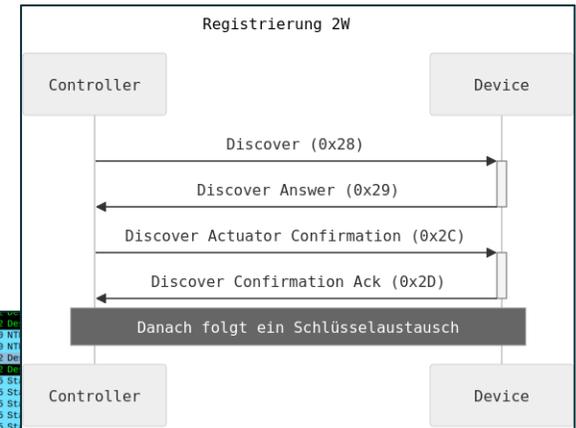
## Projekt FIENDISH



- Analyse des Datenmanagements von verschiedenen Smart-Home Geräten
- Rekonstruktion der herstellerspezifischen Kommunikationsprotokolle und Datagramme
- Identifikation von für die Forensik relevanten Sensoren oder Benutzerdaten
- Entwicklung von Werkzeugen zur Extraktion von Sensor- und Benutzerdaten



5897	112	969729248	10.18.217.213	195.72.96.254	ICMP	122 Da
5910	112	974965672	10.18.217.213	10.18.41.31	NTP	90 NT
5911	112	97496783	10.18.217.213	10.18.41.31	NTP	90 NT
5914	112	971407256	10.18.217.213	10.18.40.24	ICMP	122 Da
5915	112	971407256	10.18.217.213	10.18.40.24	ICMP	122 Da
5916	112	972149694	10.18.217.213	10.18.40.22	DNS	95 St
5917	112	972159886	10.18.217.213	10.18.40.22	DNS	95 St
5922	112	989132215	10.18.217.213	10.18.40.24	DNS	95 St
5923	112	989133698	10.18.217.213	10.18.40.24	DNS	95 St
5924	112	989814938	10.18.217.213	195.72.96.254	DNS	95 St
5925	112	989816142	10.18.217.213	195.72.96.254	DNS	95 St
5926	112	989973966	10.18.217.213	224.0.0.22	IGMPv3	60 Membership Report / Join group
5931	113	011961914	10.18.217.213	10.18.40.22	DNS	78 Standard query 0xcd5f A ipv4.co
5932	113	011863117	10.18.217.213	10.18.40.22	DNS	76 Standard query 0xcd5f A ipv4.co
5933	113	012110242	10.18.217.213	10.18.40.24	DNS	76 Standard query 0xcd5f A ipv4.co
5934	113	012110783	10.18.217.213	10.18.40.24	DNS	76 Standard query 0xcd5f A ipv4.co
5935	113	012832932	10.18.217.213	195.72.96.254	DNS	76 Standard query 0xcd5f A ipv4.co
5936	113	012834154	10.18.217.213	195.72.96.254	DNS	76 Standard query 0xcd5f A ipv4.co
5943	113	047829188	10.18.217.213	10.18.40.22	ICMP	108 Destination unreachable (Port u
5944	113	047829188	10.18.217.213	10.18.40.22	ICMP	108 Destination unreachable (Port u
5945	113	048895658	10.18.217.213	10.18.40.24	ICMP	108 Destination unreachable (Port u
5946	113	048895658	10.18.217.213	10.18.40.24	ICMP	108 Destination unreachable (Port u
5947	113	048879491	10.18.217.213	195.72.96.254	ICMP	108 Destination unreachable (Port u
5948	113	048879491	10.18.217.213	195.72.96.254	ICMP	108 Destination unreachable (Port u
5949	113	050403873	10.18.217.213	82.105.8.211	TCP	74 41340 - 80 [SYN] Seq=0 Win=6424
5950	113	050403873	10.18.217.213	82.105.8.211	TCP	74 [TCP Out-of-Order] [TCP Port nu
5951	113	050762524	10.18.217.213	82.105.8.211	TCP	66 41340 - 80 [ACK] Seq=1 Ack=1 Ki
5952	113	050763786	10.18.217.213	82.105.8.211	TCP	66 [TCP Dup ACK 0501e1] 41340 - 80
5953	113	060324774	10.18.217.213	82.105.8.211	HTTP	177 GET /online/status.html HTTP/1.
5954	113	060324774	10.18.217.213	82.105.8.211	TCP	177 [TCP Duplicate Seq] 41340 - 80
5955	113	068878643	10.18.217.213	82.105.8.211	TCP	66 41340 - 80 [ACK] Seq=112 Ack=20
5976	113	068879495	10.18.217.213	82.105.8.211	TCP	66 [TCP Dup ACK 0575a1] 41340 - 80
5977	113	074204647	10.18.217.213	10.18.41.31	NTP	90 NTP Version 4, Client
5978	113	074204647	10.18.217.213	10.18.41.31	NTP	90 NTP Version 4, Client
5979	113	091940784	10.18.217.213	82.105.8.211	TCP	66 41340 - 80 [FIN, ACK] Seq=112 A
5980	113	091941255	10.18.217.213	82.105.8.211	TCP	66 [TCP Out-of-Order] 41340 - 80
6081	113	365865645	10.18.217.213	224.0.0.251	MDNS	245 Standard query 0x0000 ANY gatew



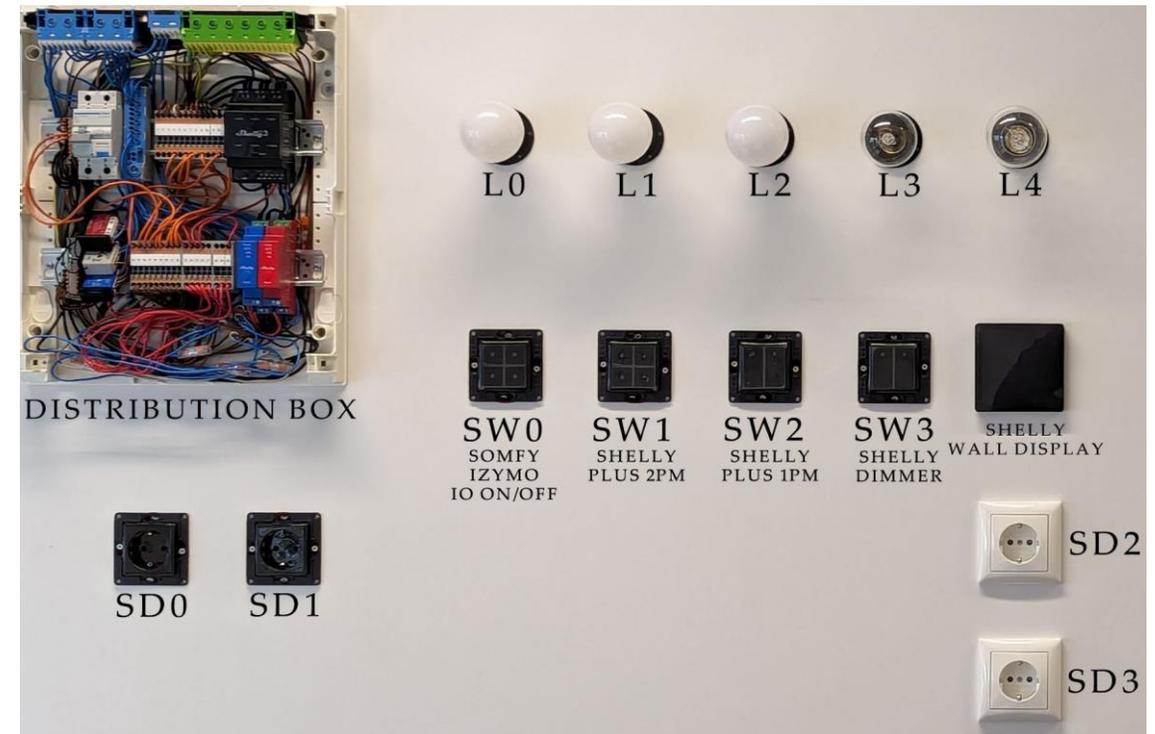
# FALLSTUDIE ZU EINEM SMART-HOME SYSTEM

Wie sieht das jetzt in der Praxis aus?

# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Untersuchtes System im Rahmen des Projekts FIENDISH

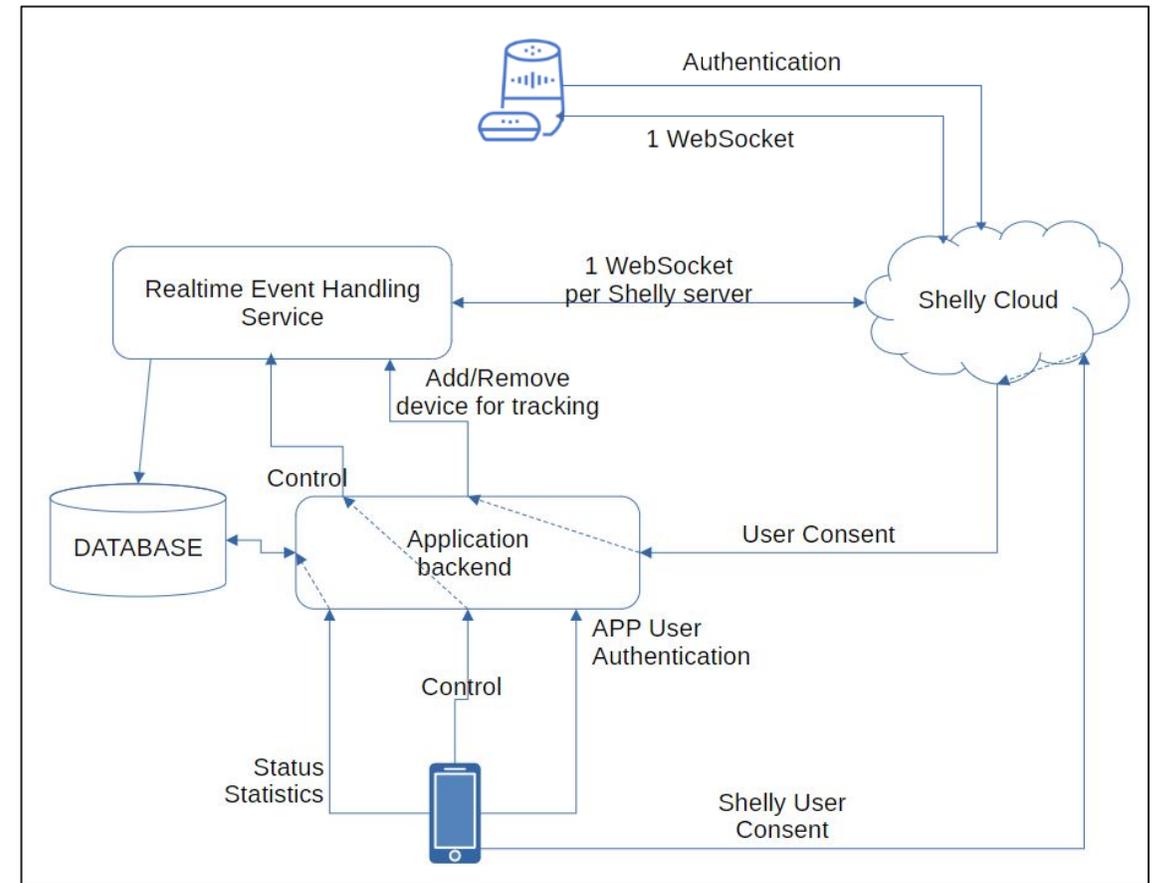
- Zur Untersuchung von verschiedenen Smart-Home Geräten einiger Hersteller haben wir ein eigenes Labor eingerichtet:
  - Bewegungsmelder und Tür/Fenstersensoren im Raum angebracht
  - Eine Verteilerbox wurde mit Smart-Home Hutschienenmodulen ausgestattet.
  - Schaltwand mit Schaltern, Smart-Lights, Steuereinheiten und schaltbaren Steckdosen aufgebaut
- Fokus der Beispielfallstudie liegt auf den Produkten des Herstellers Shelly



# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

## Netzwerkstruktur

- Direkte Einbindung über die Shelly Cloud, Alternative über MQTT Broker mit eigener Infrastruktur nutzbar, z.B. Home Assist
- Sensoren und Aktoren kommunizieren nie direkt sondern immer über die Cloud oder über den MQTT Broker
- Interface zum Abfragen der Daten wird über einen API zur Cloud-Infrastruktur hin angeboten
- Die Daten werden zur Cloud hin mit TLS verschlüsselt gesendet; Authentifizierung zur Cloud hin mit einem OAuth Token



Quelle: <https://shelly-api-docs.shelly.cloud/integrator-api/>

# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

## Smart-Home Shelly Cloud



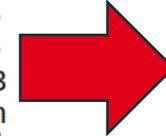
Quelle: <https://www.shelly.com/pages/info-board>

# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

## Auffinden von Shelly Geräten in einem Heimnetzwerk

- Entwicklung eines Werkzeugs zum Auffinden vom im Gebäude verbauten spezifischen Smart-Home Gerät
- Identifikation der Geräte über einen signifikanten Fingerabdruck der Hersteller-ID und der Software Version ähnlich zu dem Werkzeug nmap.
- Für die Identifikation der Geräte können drei verschiedenen Kommunikationsprotokolle genutzt werden:
  - MQTT
  - HTTP
  - mDNS

```
MQTT 30
TCP 30
captured (2472 hits) 0
00 h...$...;...E.
12 'yM@.@.L.....
18 L.[.&.0...f...
e8 .....+
33 ..1$.sh ellypro3
6e -c8f09e8 8ca3c/on
6c linetrue 1$.shel
36 lypro1-e c62608a6
27 1ac/onli netrue1'
2d '!shelly plus2pm-
6c b48a0a1c 09d4/onl
6c inettrue1 &. shell
32 ypro1pm- 30c6f782
31 3bac/onl inettrue1
33 '!shell y1minig3
6e -5432044 0f74c/on
6c linetrue 1+%Shel
30 lyWallDi splay-00
6e 0822D233 24/onlin
etrue
```



```
Answer from: 10.18.221.13
device_id: shellypro3-c8f09e88ca3c
online: true
device_id: shellypro1-ec62608a61ac
online: true
device_id: shellyplus2pm-b48a0a1c09d4
online: true
device_id: shellypro1pm-30c6f7823bac
online: true
device_id: shelly1minig3-54320440f74c
online: true
```

MQTT

```
Answer from 10.18.221.217
Device Information:
device_id: shellypro3-c8f09e88ca3c
mac: C8F09E88CA3C
model: SPSW-003XE16EU
gen: 2
fw_id: 20240223-142037/1.2.2-g7c39781
ver: 1.2.2
app: Pro3
auth_en: False
vendor: Espressif Inc.
device_name: Shelly Pro 3
```

HTTP

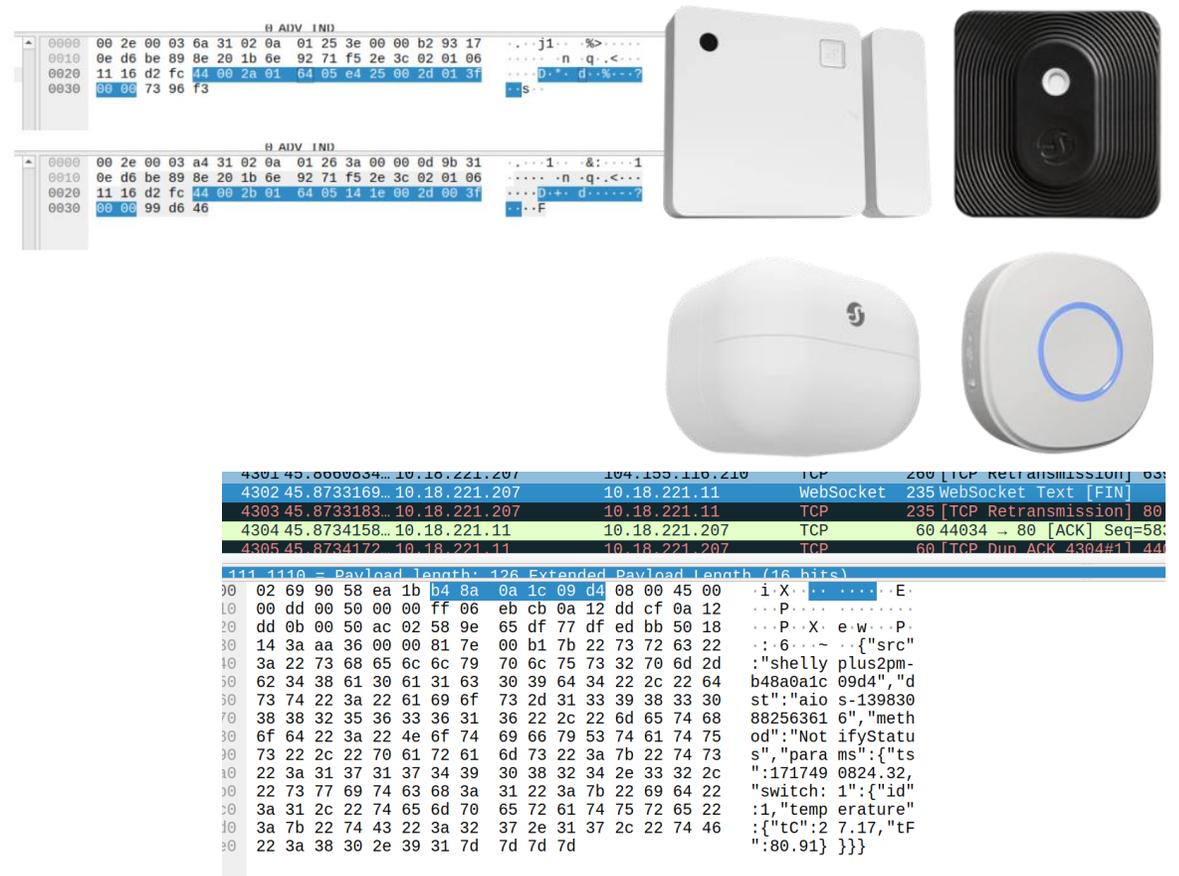
```
Answer from 10.18.221.227:80
Weight: 0, priority: 0
Server: Shelly1MiniG3-54320440F74C.local.
Device Information:
gen: 3
ver: 1.3.2
app: Mini1G3
```

mDNS

# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

## Kommunikationsanalyse

- Sicherheitskonzept fokussiert sich nur im Bezug auf die Absicherung der Daten in der Cloud
- Bluetooth Devices können über andere Shelly-Geräte an die Cloud angebunden werden
- Nachrichten werden unverschlüsselt als Advertisement per Broadcast gesendet
- Keinerlei Nachweis auf die Authentizität der Daten, somit nicht für die forensische Analyse verwertbar



```
0000 00 2e 00 03 6a 31 02 0a 01 25 3e 00 00 b2 93 17  ....j1...%>....
0010 0e d6 be 89 8e 20 1b 6e 92 71 f5 2e 3c 02 01 06  ....n q.<...
0020 11 16 d2 fc 44 00 2a 01 64 05 e4 25 00 2d 01 3f  ....D.-+ d.-x...?
0030 00 00 73 96 f3  ....S...

0000 00 2e 00 03 a4 31 02 0a 01 26 3a 00 00 0d 9b 31  ....1...&:....1
0010 0e d6 be 89 8e 20 1b 6e 92 71 f5 2e 3c 02 01 06  ....n q.<...
0020 11 16 d2 fc 44 00 2b 01 64 05 14 1e 00 2d 00 3f  ....D.-+ d.-...?
0030 00 00 99 d6 46  ....F...

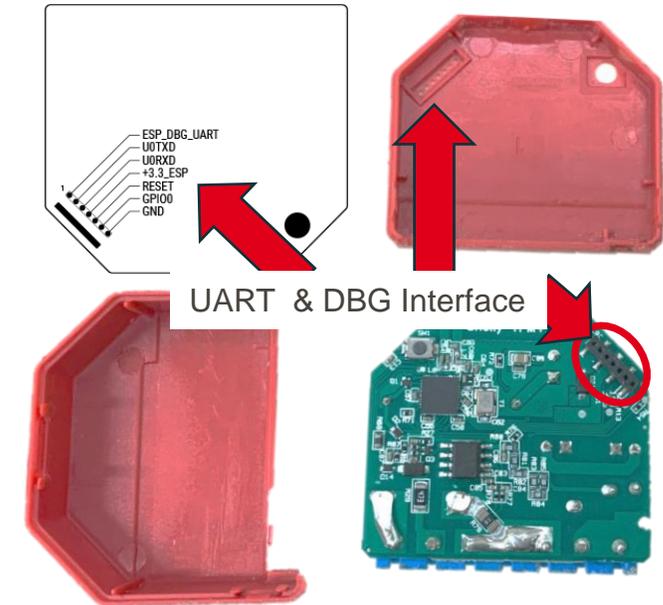
4301 45.8800834... 10.18.221.207 104.155.116.210 TCP 200 [TCP Retransmission] 63
4302 45.8733169... 10.18.221.207 10.18.221.11 WebSocket 235 WebSocket Text [FIN]
4303 45.8733183... 10.18.221.207 10.18.221.11 TCP 235 [TCP Retransmission] 80
4304 45.8734158... 10.18.221.11 10.18.221.207 TCP 60 44034 -> 80 [ACK] Seq=58
4305 45.8734172... 10.18.221.11 10.18.221.207 TCP 60 [TCP Dup ACK 4304#1] 44

111 1110 - Payload length: 126 Extended Payload Length (16 bits)
00 02 69 90 58 ea 1b b4 8a 0a 1c 09 d4 08 00 45 00  .i.X...E
10 00 dd 00 50 00 00 ff 06 eb cb 0a 12 dd cf 0a 12  .P...
20 dd 0b 00 50 ac 02 58 9e 65 df 77 df ed bb 50 18  .P.X e.w.P
30 14 3a aa 36 00 00 81 7e 00 b1 7b 22 73 72 63 22  .:6...-{"src"
40 3a 22 73 68 65 6c 6c 79 70 6c 75 73 32 70 6d 2d  :shelly plus2pm-
50 62 34 38 61 30 61 31 63 30 39 64 34 22 2c 22 64  b48a0a1c 09d4", "d
60 73 74 22 3a 22 61 69 6f 73 2d 31 33 39 38 33 30  st": "aio s-139830
70 38 38 32 35 36 33 36 31 36 22 2c 22 6d 65 74 68  88256361 6", "meth
80 6f 64 22 3a 22 4e 6f 74 69 66 79 53 74 61 74 75  od": "Not ifyStatu
90 73 22 2c 22 70 61 72 61 6d 73 22 3a 7b 22 74 73  s", "para ms": {"ts
10 22 3a 31 37 31 37 34 39 30 38 32 34 2e 33 32 2c  ":171749 0824.32,
20 22 73 77 69 74 63 68 3a 31 22 3a 7b 22 69 64 22  "switch: 1": {"id"
30 3a 31 2c 22 74 65 6d 70 65 72 61 74 75 72 65 22  :1, "temp erature"
40 3a 7b 22 74 43 22 3a 32 37 2e 31 37 2c 22 74 46  : {"tC": 2 7.17, "tF
50 22 3a 38 30 2e 39 31 7d 7d 7d 7d  ....{":80.91} ]}}}
```

# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Analyse der Schnittstellen und Hardware von den Geräten

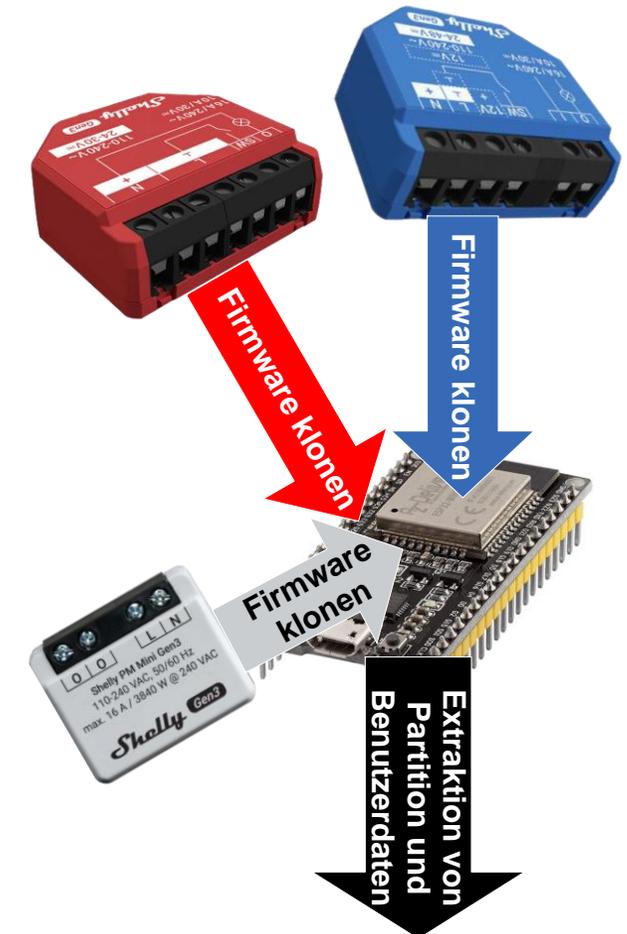
- Hauptprozessor ist entweder ein ESP8266 oder ESP32 von Xtensa
- Wifi und Bluetooth Kommunikation direkt über ESP-Chip
- Keinen zusätzlichen Speicherbausteine, nur die interne Speichernutzung des ESP
- Bei geschlossenem Gehäuse von Außen erreichbares Kommunikations- und Wartungsinterface Interface:
  - UART
  - RESET
  - Versorgungsspannung
  - Debug-Ports



# FALLSTUDIE AN EINEM SMART-HOME SYSTEM

## Dumpen, Klonen und Analysieren der Firmware

- Entwicklung eines Werkzeuges zur Extraktion der Firmware durch das Erweitern bestehender Werkzeuge in der Embedded Entwicklung
- Analyse von frei zugänglichen und unverschlüsselten Firmware Updates zur Rekonstruktion der Firmwarestruktur und Identifikation der relevanten Datensegmente
- Softwarewerkzeug zum Klonen der Firmware für die Untersuchung von Asservaten auf alternativen Plattformen zur manipulationsfreien Analyse





# ZUSAMMENFASSUNG UND AUSBLICK

Welche Informationen werden im Haus gespeichert?

# ZUSAMMENFASSUNG UND AUSBLICK

Das Haus weiß nicht viel über seine Bewohner, aber die Cloud!

- Nicht nur Smart-Speaker sammeln unerlässlich Daten über die Hausbewohner, auch andere Sensoren sammeln Daten und speichern sie möglicherweise in einer Cloud-Infrastruktur.
- Über die Daten von Sensoren lassen sich sehr gut digitale Spuren von nicht-digitalen Delikten verfolgen, jedoch bedarf es noch einer Verbesserung der Werkzeugunterstützung.
- Sehr oft müssen existierende Werkzeuge angepasst oder selbst geschrieben werden, hierfür wird interdisziplinär geschultes Personal benötigt.

Vielen Dank für Ihre Aufmerksamkeit.