Hochschule RheinMain

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

Hochschule RheinMain

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

Hochschule RheinMain

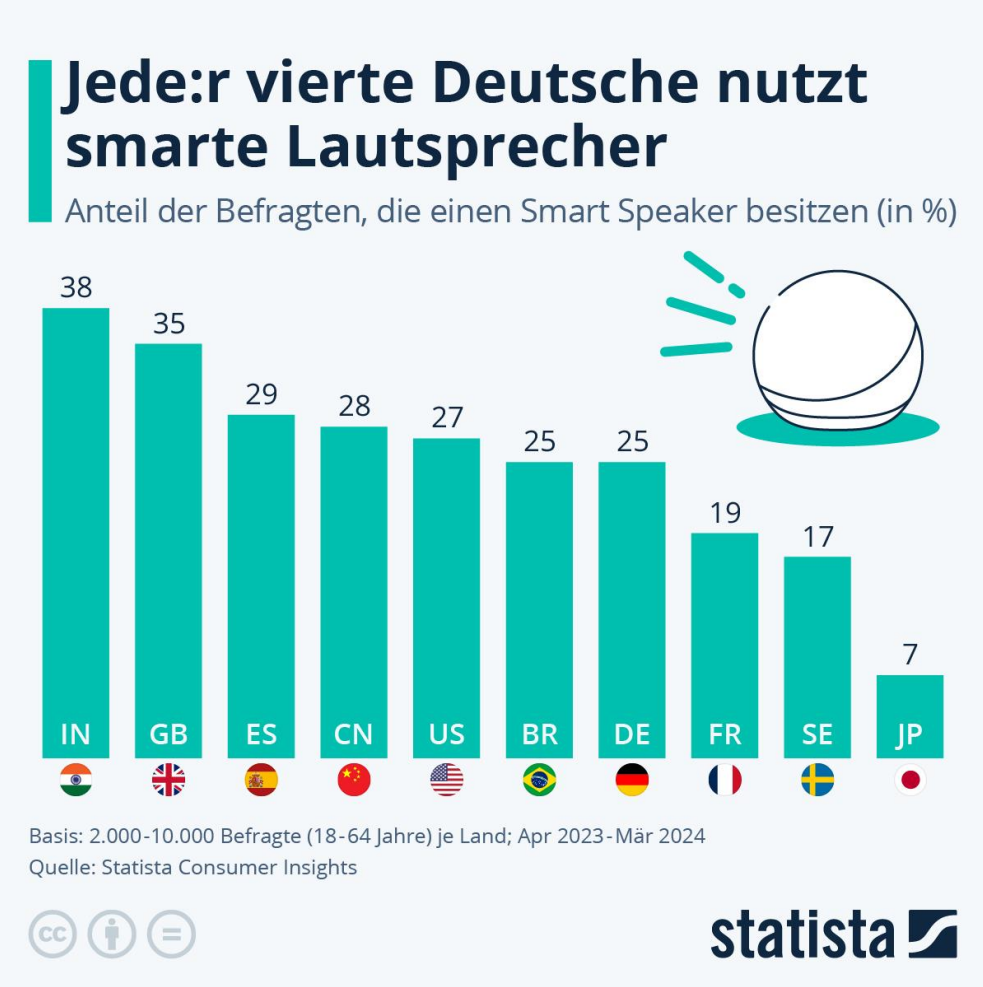
MOTIVATION

Wer von Ihnen hat einen Smart Speaker daheim?

MOTIVATION
Schöne neues Zuhause

Hochschule RheinMain

- 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.



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

Hochschule **RheinMain**

- Transskripte und Daten von Smart Speakern dürfen für einige Delikte bei Gerichts-verfahren 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/

Quelle: https://www.zdf.de/nachrichten/video/alexa-siri-smart-speaker-sprachassistenten-datenschutz-faktencheck-backgroundcheck-100.html

Hochschule RheinMain

SMART HOME

Was ist eigentlich Smart Home?

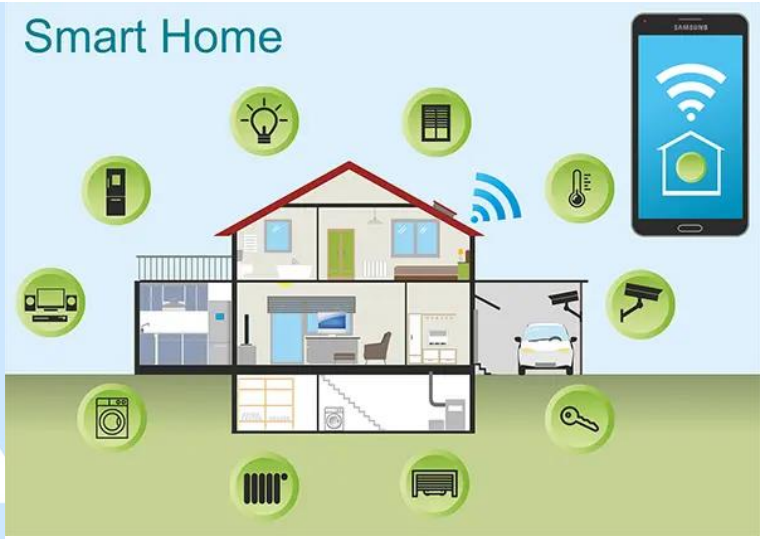
SMART HOME

Sensoren und Aktoren im Smart-Home Bereich

Hochschule **RheinMain**

- Smart-Home ist keine Gebäude-automatisierung:
  - 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/ç



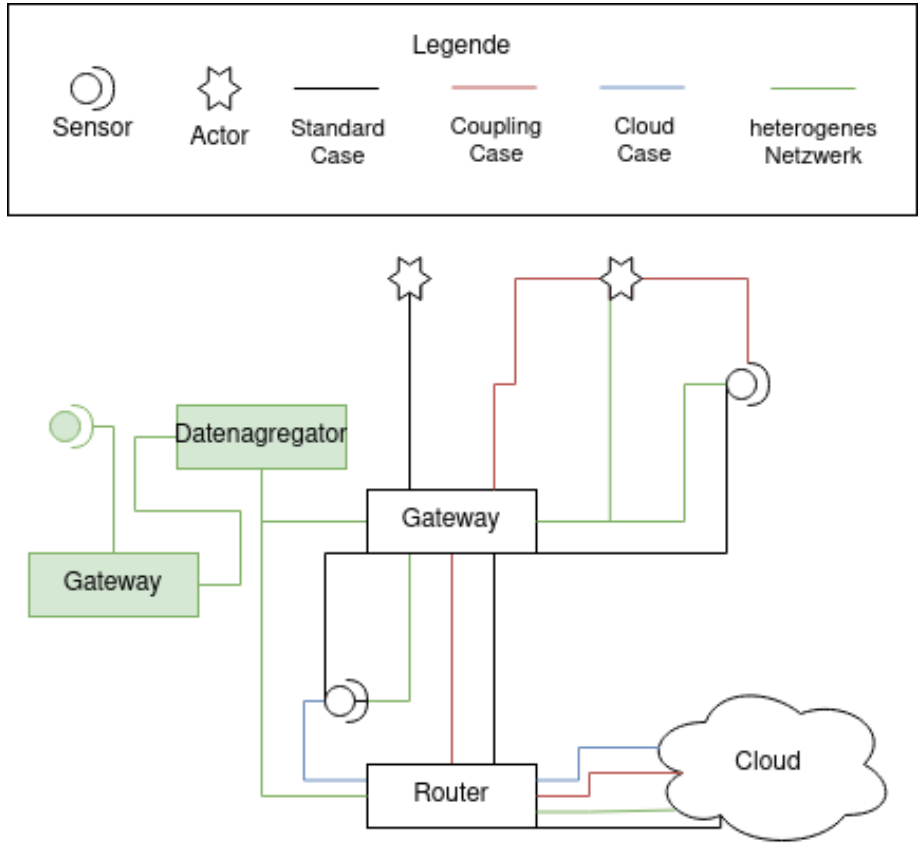
Quelle: https://www.gatewayfiber.com/blog/how-much-internet-speed-do-you-need-for-a-smart-home/

SMART HOME

Smart-Home Netzwerk-Topologien

Hochschule **RheinMain**

- 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

Hochschule RheinMain

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

Hochschule RheinMain

FORENSIK IM BEREICH SMART-HOME

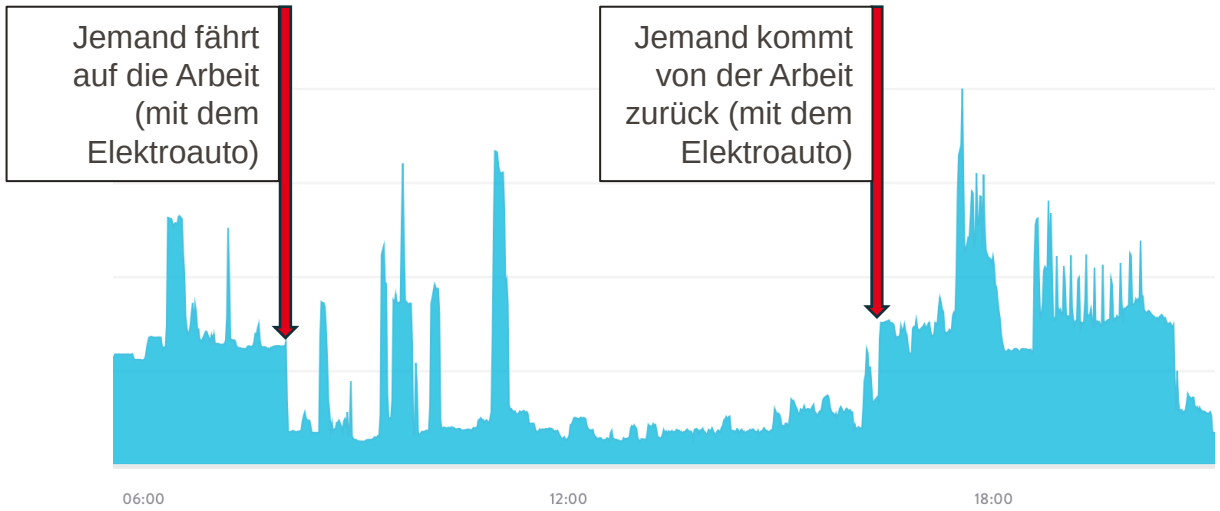
Warum sind SMART-Home Geräte interessant für die forensische Analyse?

FORENSIK IM BEREICH SMART-HOME

Relevante Sensordaten und Aktordaten

Hochschule **RheinMain**

- 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)



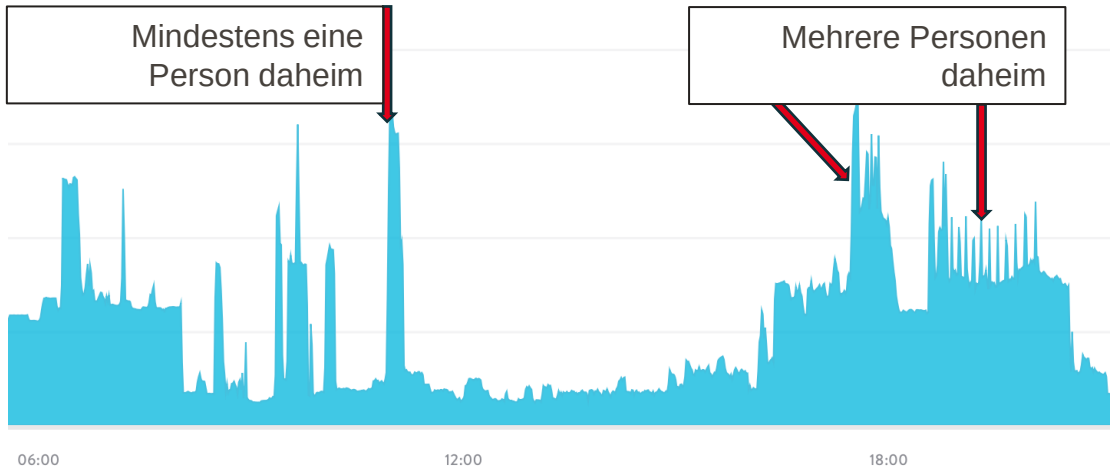
Leistungsverbrauch eines Haushalts

FORENSIK IM BEREICH SMART-HOME

Relevanz von Smart-Home für Forensik

Hochschule **RheinMain**

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



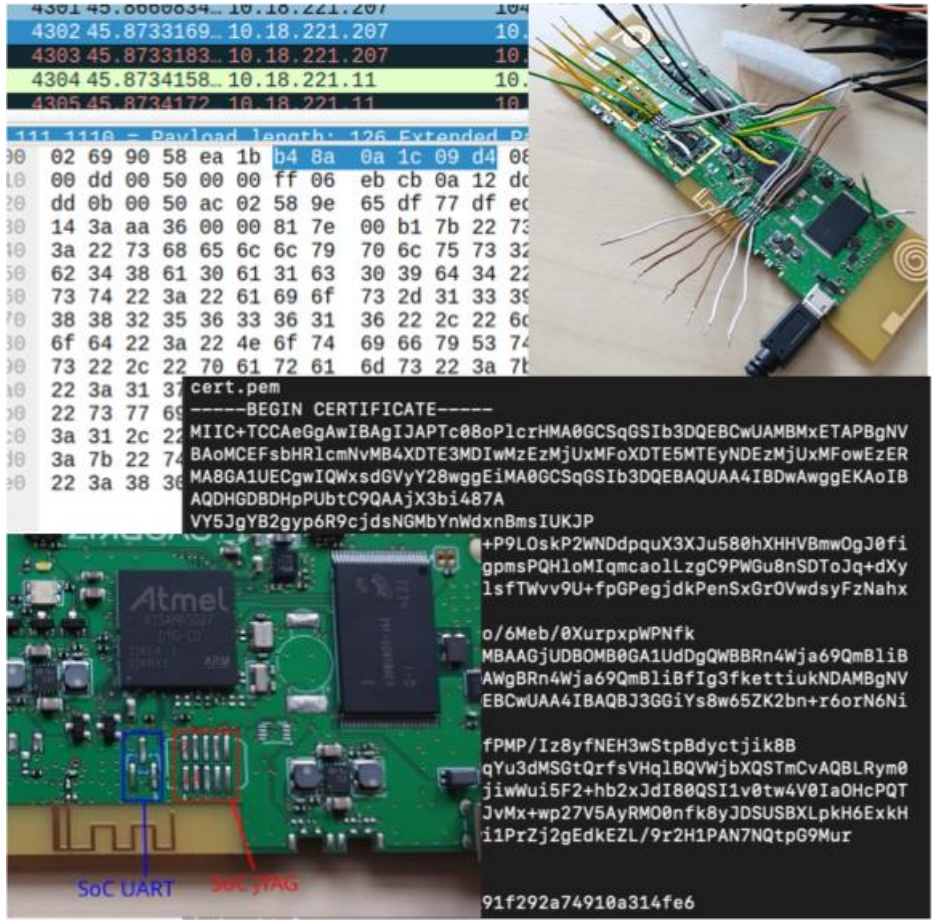
Leistungsverbrauch eines Haushalts

FORENSIK IM BEREICH SMART-HOME

Technische Herausforderungen

Hochschule RheinMain

- Kommunikation Heterogenität - keine standardisierten Schnittstellen
- Extraktion der Daten - Schlecht oder gar nicht dokumentierte, herstellerspezifische Protokolle und Datenverwaltung
- Flüchtigkeit der Daten - Langzeitspeicherort der Daten muss nicht auf dem Gerät sein
- Nicht-dokumentierte Sicherheitsmechanismen
- Limitierter Austausch und öffentliche Informationen - Keine Forschungscommunity, da meistens nur behördliches Interesse vorhanden ist



FORENSIK IM BEREICH SMART-HOME

Forensische/Kriminalistische Herausforderungen

Hochschule **RheinMain**

- Das Auffinden der Geräte im Netzwerk und physikalisch
- Nur beschränkt kommerzielle Werkzeuge vorhanden – Individuelle Analysetool-entwicklung
- 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/

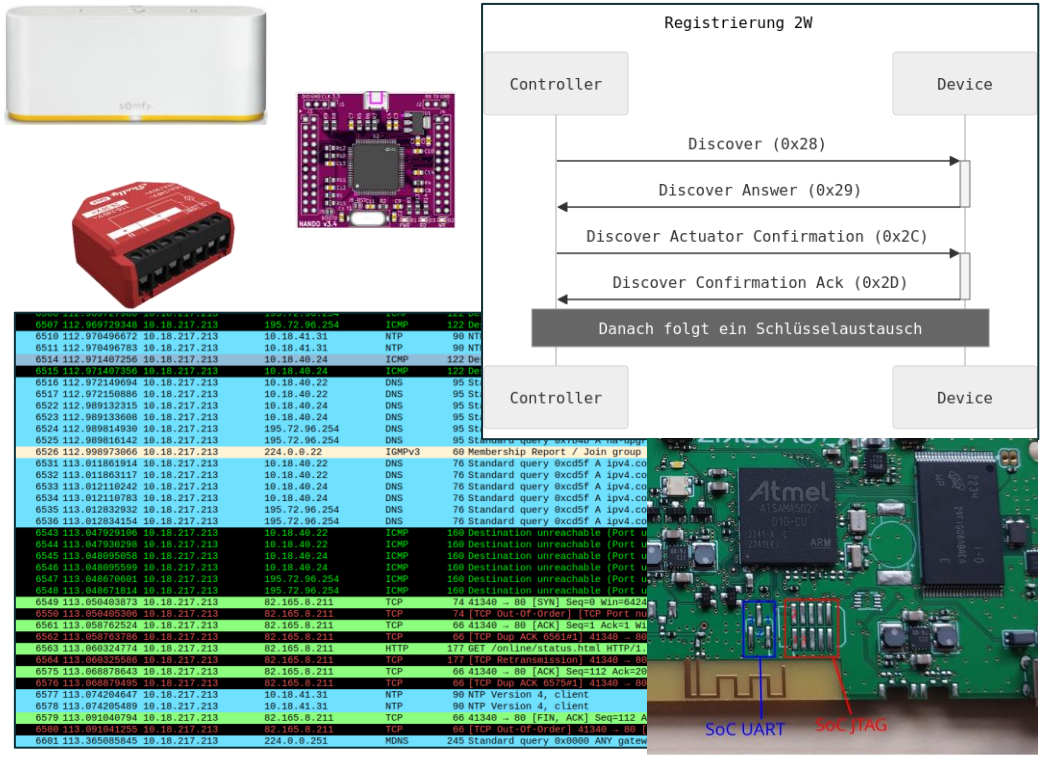
FORENSIK IM BEREICH SMART-HOME

Projekt FIENDISH

Hochschule **RheinMain**

- 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

FIENDISH



Hochschule RheinMain

FALLSTUDIE ZU EINEM SMART-HOME SYSTEM

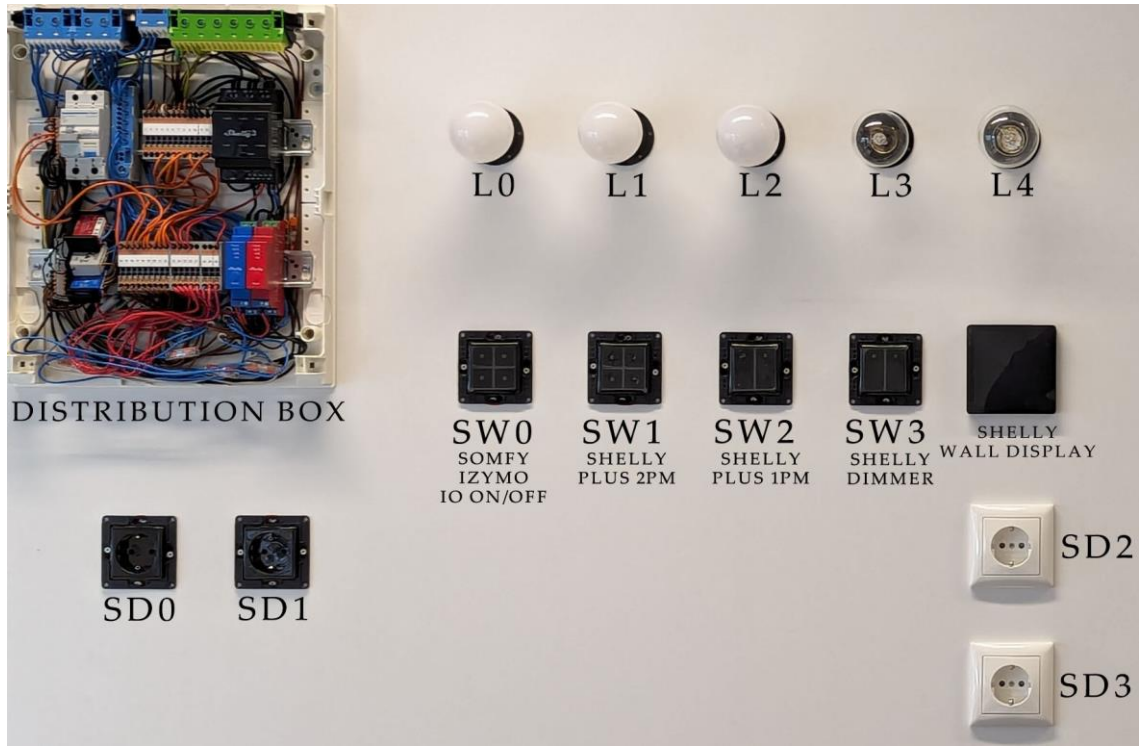
Wie sieht das jetzt in der Praxis aus?

FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Untersuchtes System im Rahmen des Projekts FIENDISH

Hochschule RheinMain

- 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

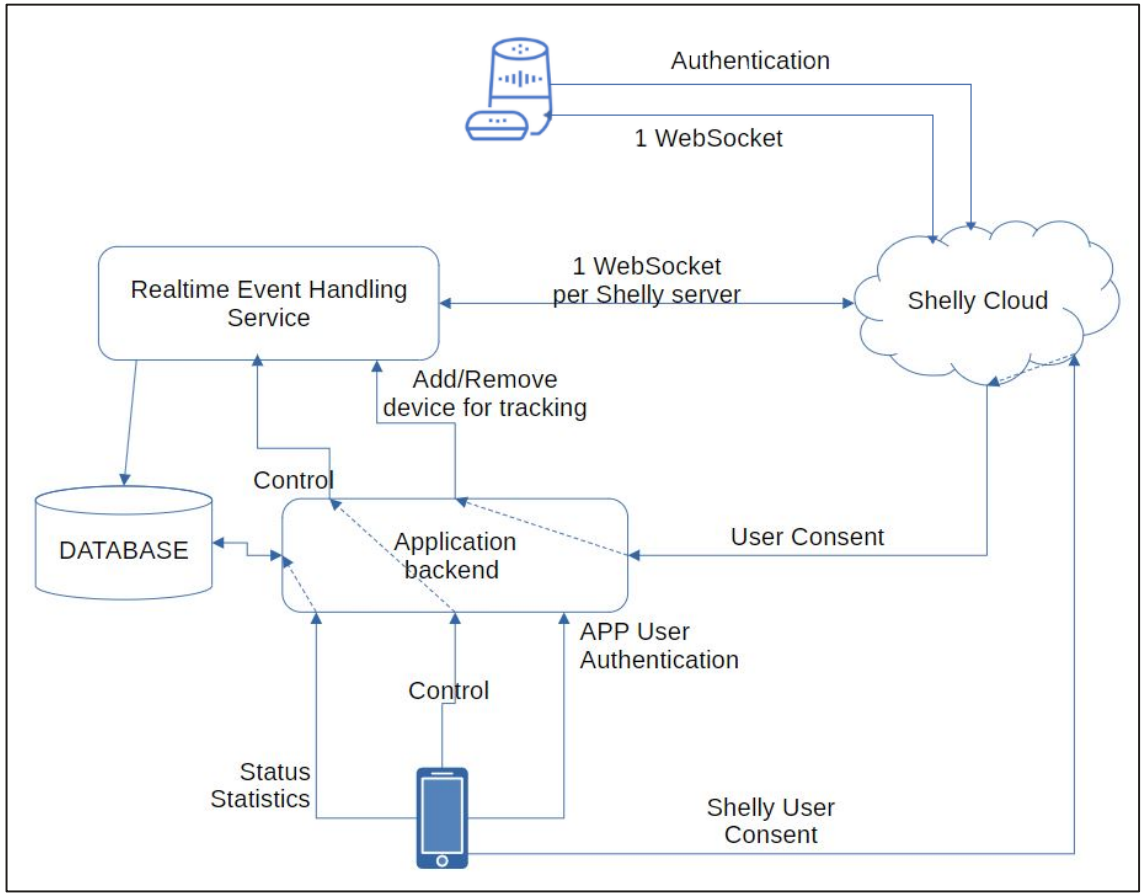


FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Netzwerkstruktur

Hochschule RheinMain

- 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 einen OAuth Token

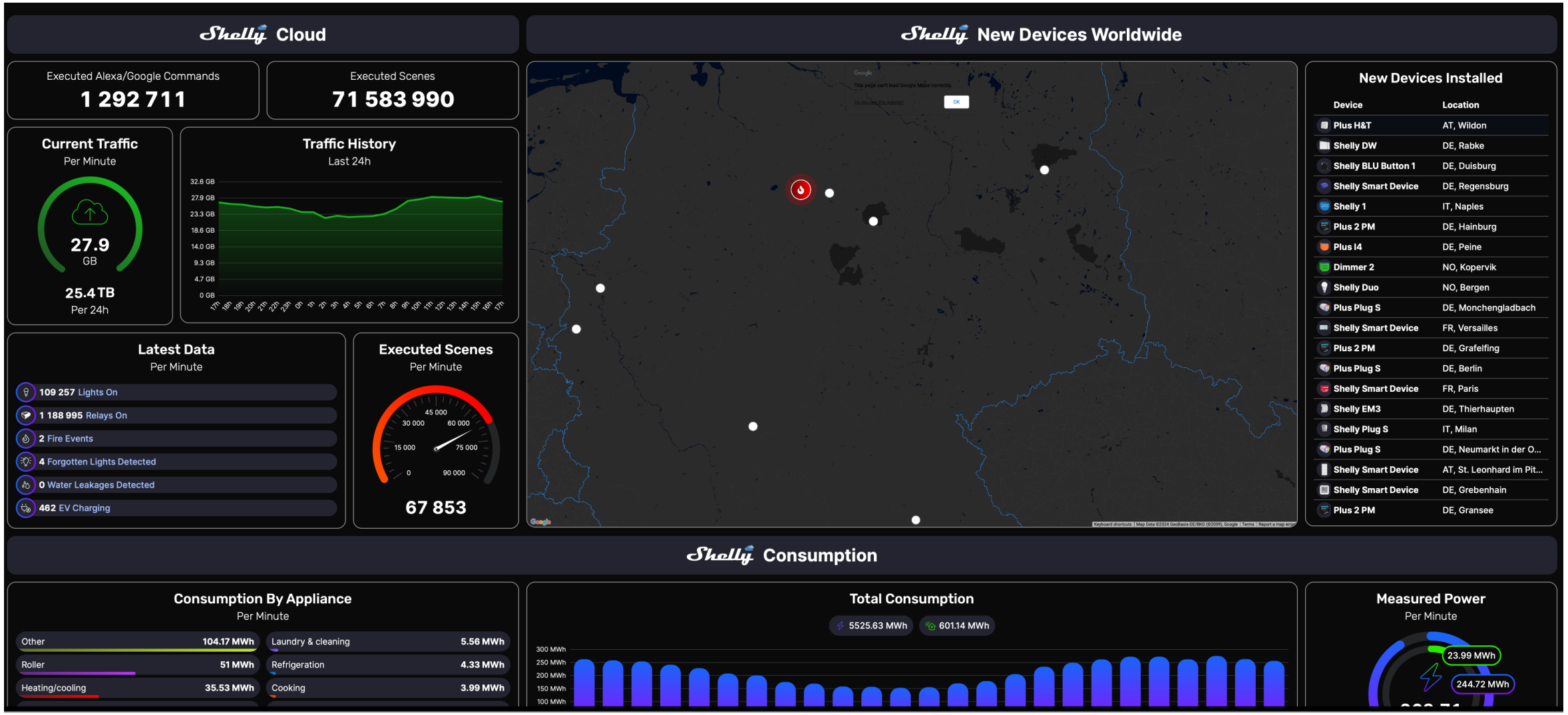


Quelle: https://shelly-api-docs.shelly.cloud/integrator-api/

FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Smart-Home Shelly Cloud

Hochschule RheinMain



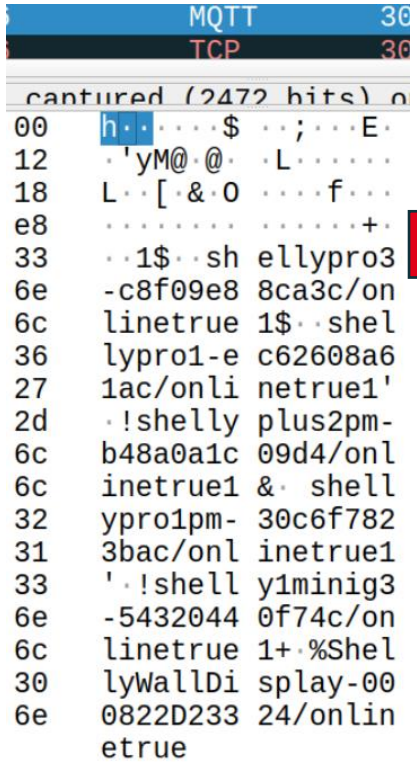
Quelle: https://www.shelly.com/pages/info-board

FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Auffinden von Shelly Geräten in einem Heimnetzwerk

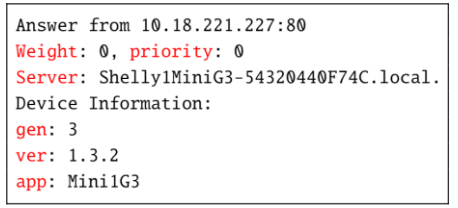
Hochschule RheinMain

- 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

HTTP



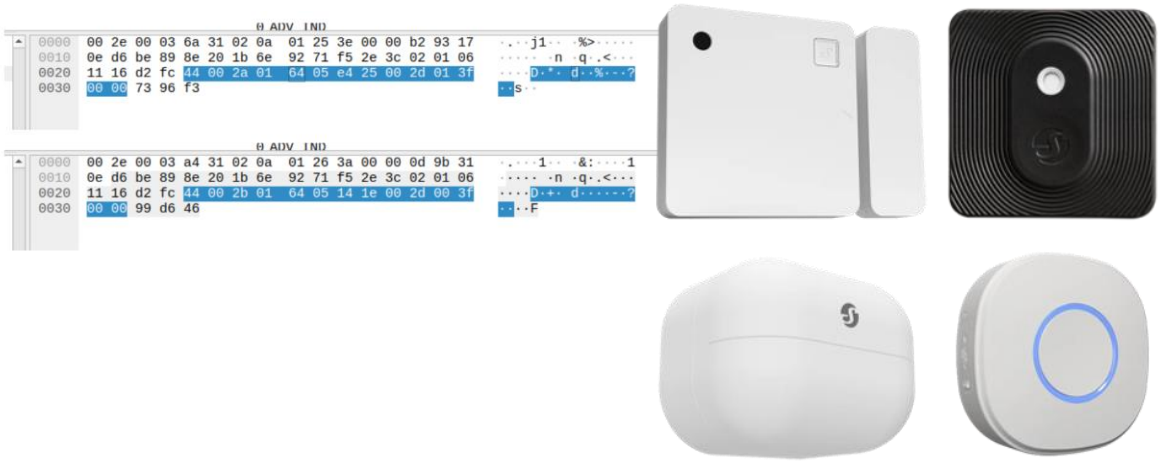
mDNS

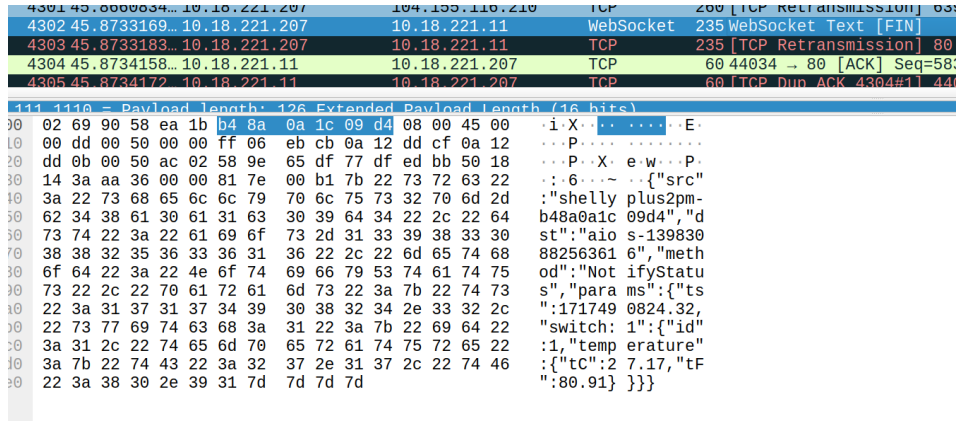
FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Kommunikationsanalyse

Hochschule RheinMain

- 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



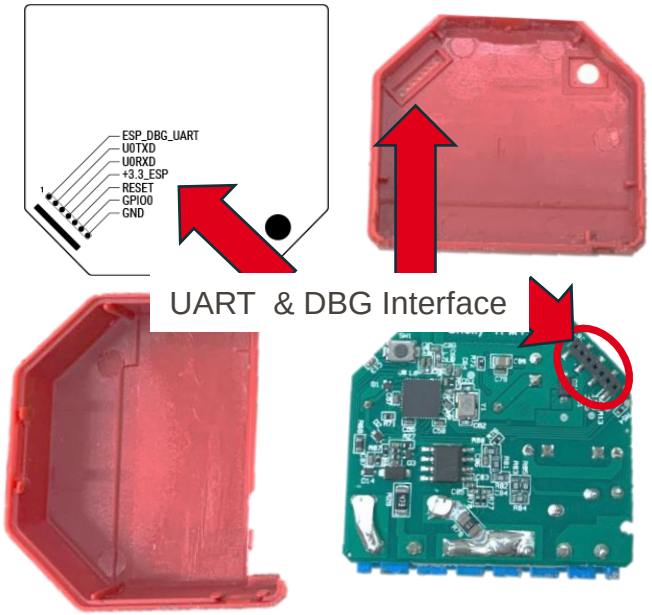


FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Analyse der Schnittstellen und Hardware von den Geräten

Hochschule **RheinMain**

- 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

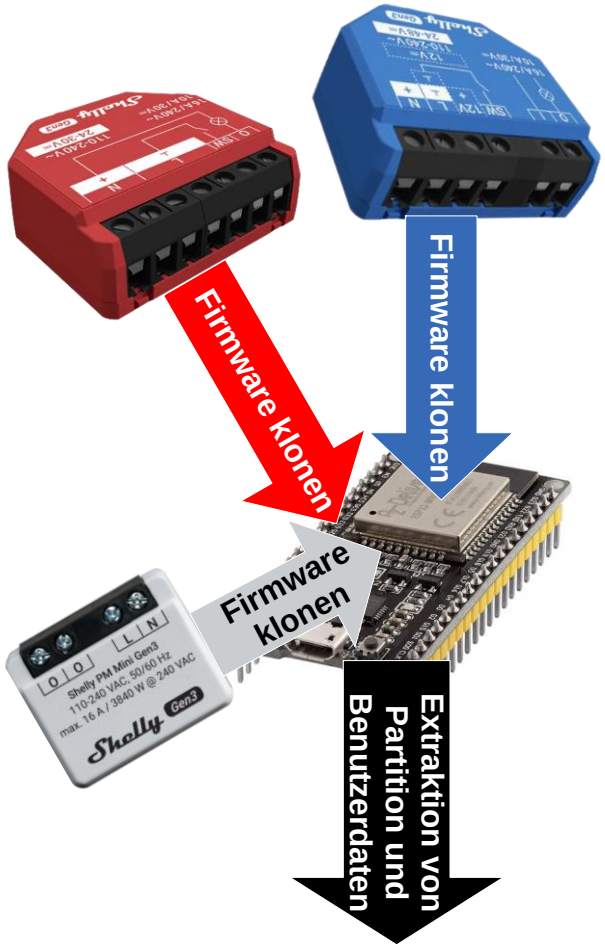


FALLSTUDIE AN EINEM SMART-HOME SYSTEM

Dumpen, Klonen und Analysieren der Firmware

Hochschule **RheinMain**

- 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

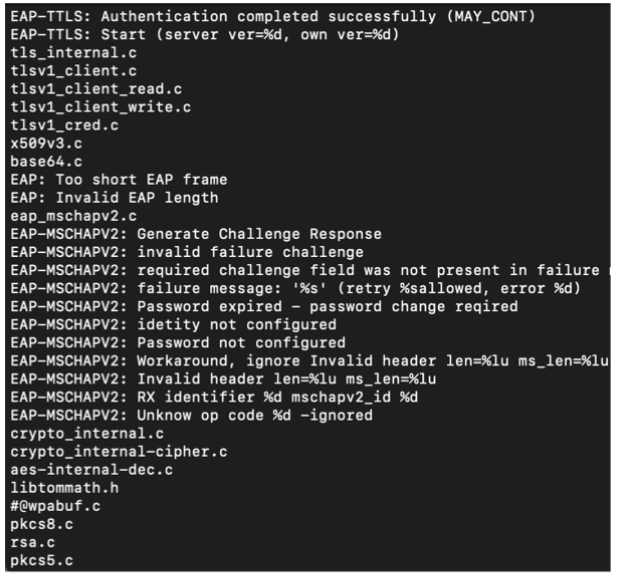


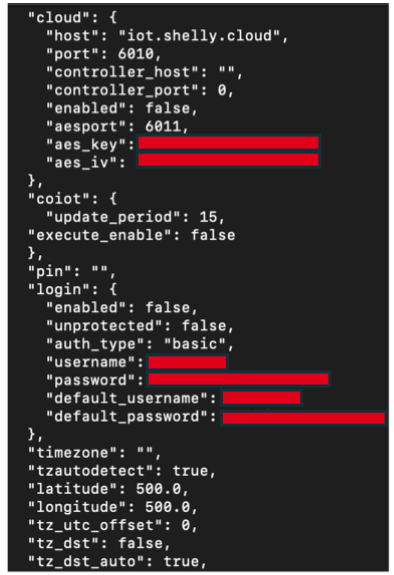
FALLSTUDIE AN EINEM SMART-HOME SYSTEM

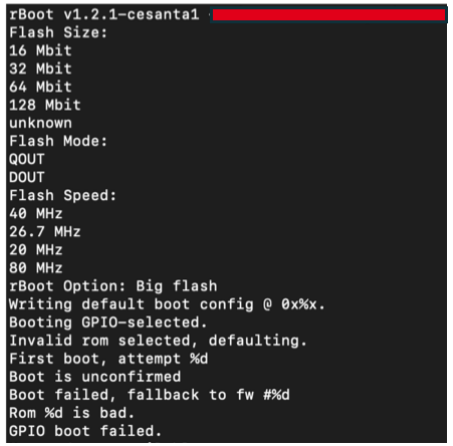
Datenanalyse

Hochschule RheinMain

- Die Sensor-/Aktordaten werden direkt an den Server (Could oder MQTT-Broker) übertragen
- Nur die Benutzerkontodaten und Verbindungsdaten zum Server werden auf dem Shelly-Gerät gespeichert:
  - Zertifikate
  - Passwörter
  - Geheime Schlüssel für die sichere Kommunikation
- Einzelne Logdaten über die Verbindungen sind auf dem Shelly-Gerät nur flüchtig gespeichert







ZUSAMMENFASSUNG UND AUSBLICK

Welche Informationen werden im Haus gespeichert?

ZUSAMMENFASSUNG UND AUSBLICK

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

Hochschule **RheinMain**

- 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.

Hochschule **RheinMain**

Vielen Dank für Ihre Aufmerksamkeit.