FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Sicherheitsanalyse von SMART Steckdosen über MQTT

Andre Klonowski

Einleitung

"Despite continued security problems, the IoT will spread and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive."

Richard Adler

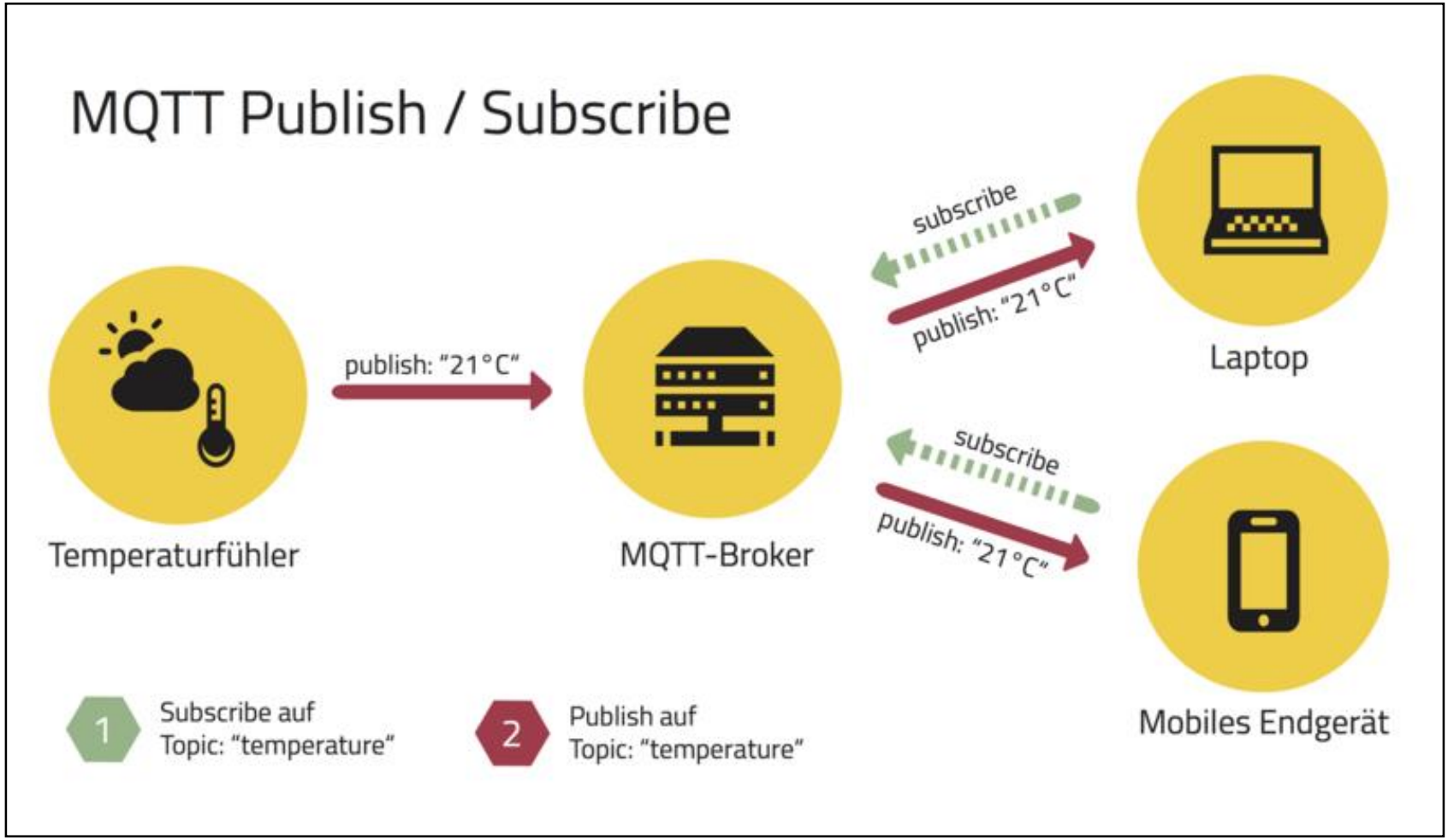
Gliederung

- Motivation
- MQTT
- Untersuchung
- Angriffsszenarien
- Zusammenfassung
- Fazit

Motivation

Warum ?

MQTT


MQTT Publish / Subscribe
publish: "21°C"
Temperaturfühler
MQTT-Broker
subscribe
publish: "21°C"
Laptop
subscribe
publish: "21°C"
Mobiles Endgerät
1
Subscribe auf
Topic: "temperature"
2
Publish auf
Topic: "temperature"

Untersuchung: Nmap

```
Not shown: 131015 closed ports, 53 filtered ports
Reason: 65534 port-unreaches, 65481 resets and 53 no-responses
PORT      STATE         SERVICE REASON          VERSION
80/tcp    open          http    syn-ack ttl 255
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store, must-revalidate
|     Pragma: no-cache
|     Expires: -1
|     Access-Control-Allow-Origin: *
|     Content-Length: 2767
|     Connection: close
```

- Suche nach offene TCP und UDP Ports

Offene Ports: TCP 80
Service: http

Untersuchung: Wireshark - Steckdose 1

```
MQ Telemetry Transport Protocol, Publish Message
▶ Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 28
  Topic Length: 24
  Topic: cmnd/sonoff-B07610/POWER
  Message: ON
```

- Topic und Nachricht in Klartext

Topic:	cmnd/sonoff-B07610/POWER
Nachricht:	ON

Untersuchung: Wireshark - Steckdose 2


```
MQ Telemetry Transport Protocol, Publish Message
▸ Header Flags: 0x32, Message Type: Publish Message, QoS Level: At least once delivery (Acknowledged deliver)
  Msg Len: 212
  Topic Length: 37
  Topic: smart/device/out/07200068dc4f223ec9ad
  Message Identifier: 145
  Message: 2.1e6b4d23543ebfbc0R19MBJrlPrdGeoQPC15yyhw0ji8PRX0EaVGAe9xfEMFw5VBw3zCczKXzIjkYVeOSFXpYqjCFetJ4zFFF…
```

- Topic und Nachricht in Klartext
- Nachricht unlesbar

Topic:	smart/device/out/072000…
Nachricht:	2.1e6b4d23543ebfb…

Untersuchung: Wireshark - Steckdose 2

```
    Key: uid
  ▼ Member Key: devEtag
    String value: 0000000br5
    Key: devEtag
  ▼ Member Key: secKey
    String value: 5eda14b3a2c4c10e
    Key: secKey
  ▼ Member Key: schemaId
    String value: 0000000bvb
    Key: schemaId
  ▼ Member Key: localKey
    String value: fc3fec81020d7d08
    Key: localKey
```

- Verschiedene Schlüssel in Klartext

secKey: 5eda14b3a2c4c10e
localKey: fc3fec81020d7d08

Untersuchung: Wireshark - Steckdose 2

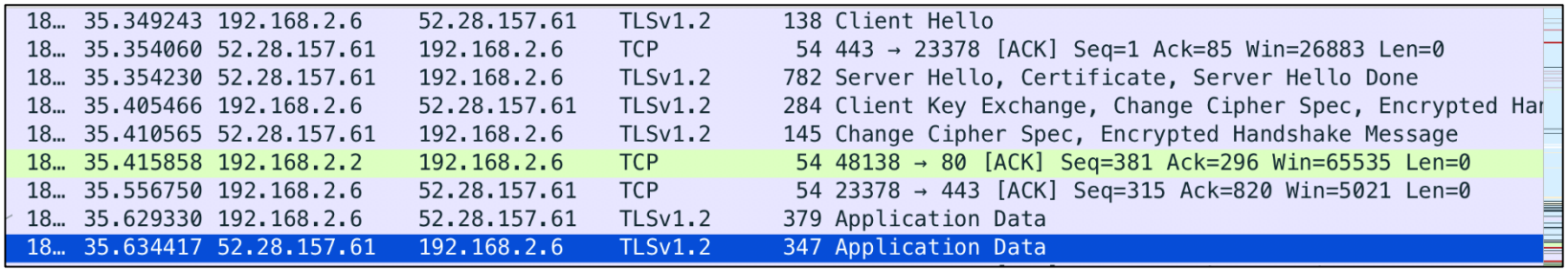
- Diverse Decrypter mit secKey und localKey testen
- AES 128 Decrypter

Zeichenfolge: 2.1e6b4d23543ebfbc0 R19MB…

- Schlüssel: localKey

Decrypted Text: {„protocol“:4,“t“:153229…}

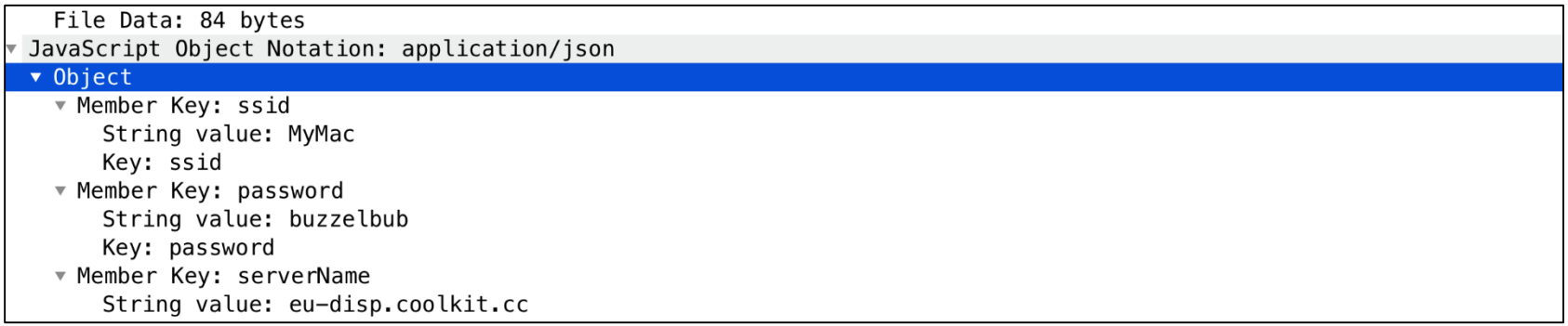
Untersuchung: Wireshark - Steckdose 3



18…	35.349243	192.168.2.6	52.28.157.61	TLSv1.2	138 Client Hello
18…	35.354060	52.28.157.61	192.168.2.6	TCP	54 443 → 23378 [ACK] Seq=1 Ack=85 Win=26883 Len=0
18…	35.354230	52.28.157.61	192.168.2.6	TLSv1.2	782 Server Hello, Certificate, Server Hello Done
18…	35.405466	192.168.2.6	52.28.157.61	TLSv1.2	284 Client Key Exchange, Change Cipher Spec, Encrypted Har
18…	35.410565	52.28.157.61	192.168.2.6	TLSv1.2	145 Change Cipher Spec, Encrypted Handshake Message
18…	35.415858	192.168.2.2	192.168.2.6	TCP	54 48138 → 80 [ACK] Seq=381 Ack=296 Win=65535 Len=0
18…	35.556750	192.168.2.6	52.28.157.61	TCP	54 23378 → 443 [ACK] Seq=315 Ack=820 Win=5021 Len=0
18…	35.629330	192.168.2.6	52.28.157.61	TLSv1.2	379 Application Data
18…	35.634417	52.28.157.61	192.168.2.6	TLSv1.2	347 Application Data

- Kein Zugriff auf Topic oder Nachrichteninhalt
- Verschlüsselung über TLS v1.2

Untersuchung: Wireshark - Steckdose 3

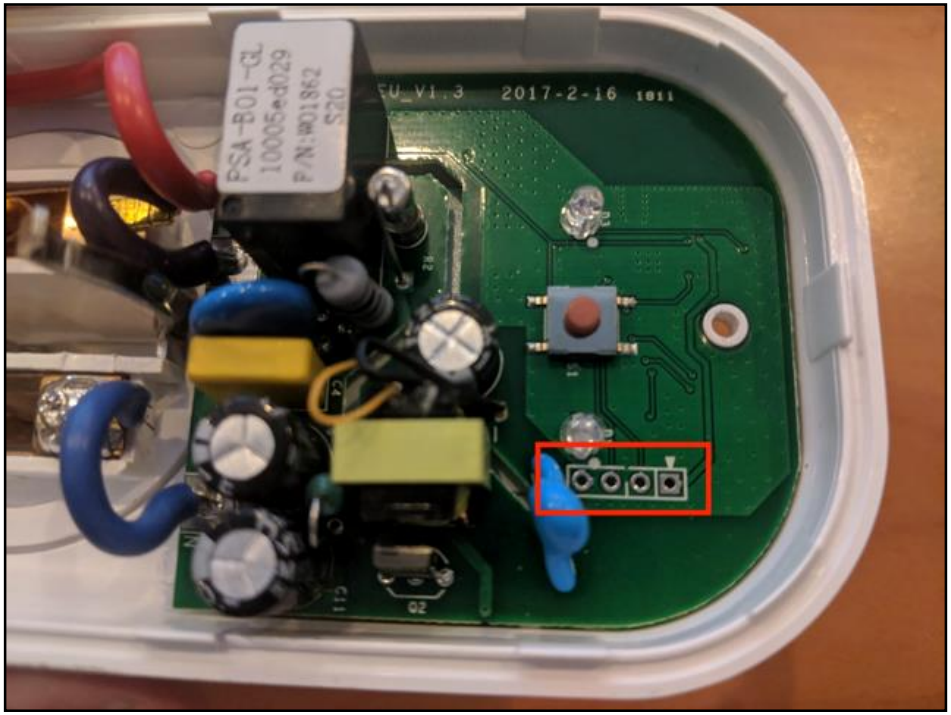


- WLAN Zugangsdaten in Klartext

SSID: MyMac
Passwort: buzzelbub

Untersuchung: Firmware

- Serielle Verbindung ermöglicht Auslesen der Firmware
- Espressif Chip
- Esptool



Untersuchung: Firmware

```
00077FE0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00077FF0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00078000  79 6F 67 69 00 00 00 00 00 00 00 00 00 00 00 00  yogi............
00078010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00078020  62 75 7A 7A 65 6C 62 75 62 00 00 00 00 00 00 00  buzzelbub.......
00078030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00078040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00078050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

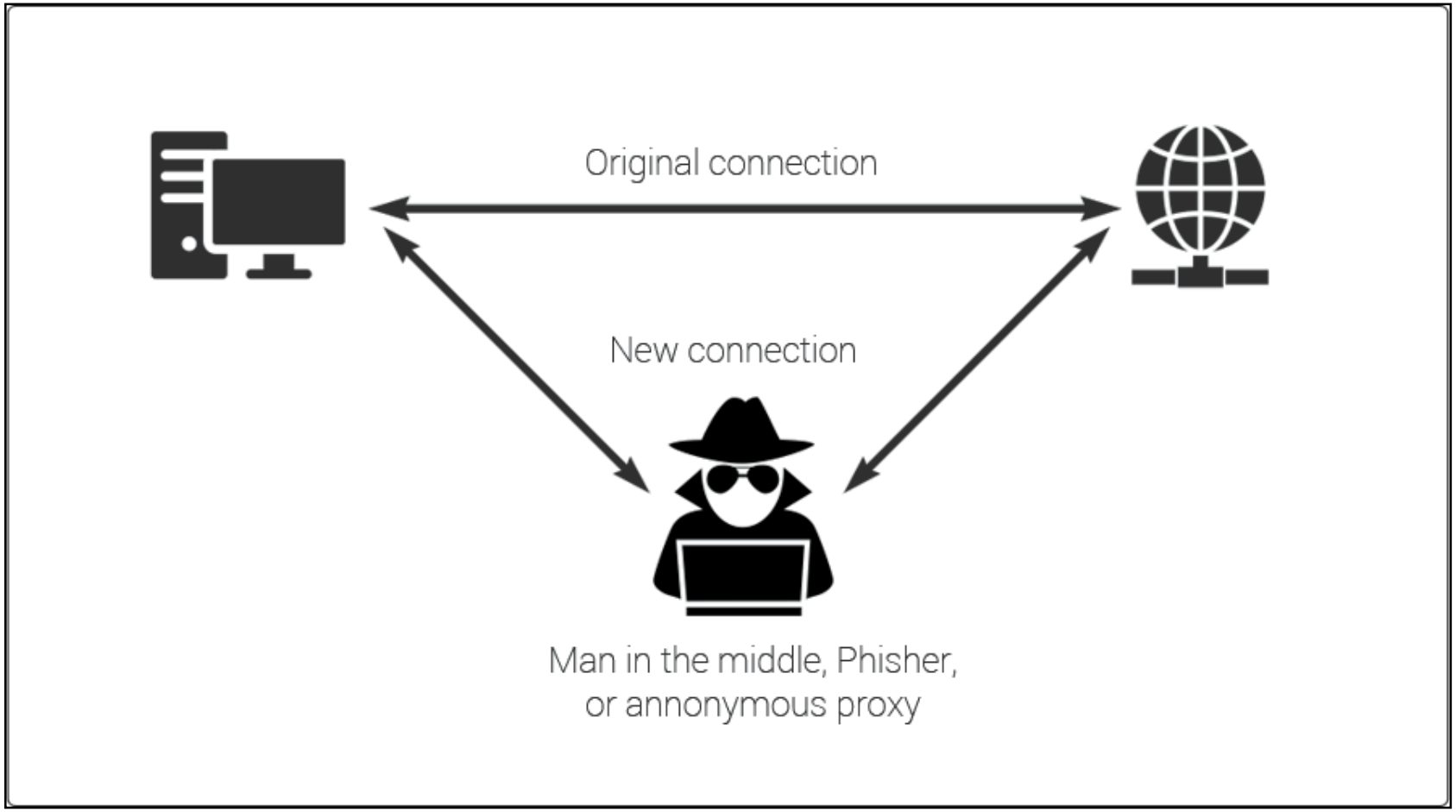
- WLAN Zugangsdaten in Klartext

SSID: yogi
Passwort: buzzelbub

Untersuchung: Steuerungssoftware - Android

- Gerooteter Android Emulator gibt Zugriff auf System und Applikationsdateien
- Untersuchung liefert keine sensiblen Daten

Angriffsszenarien: Man in the middle



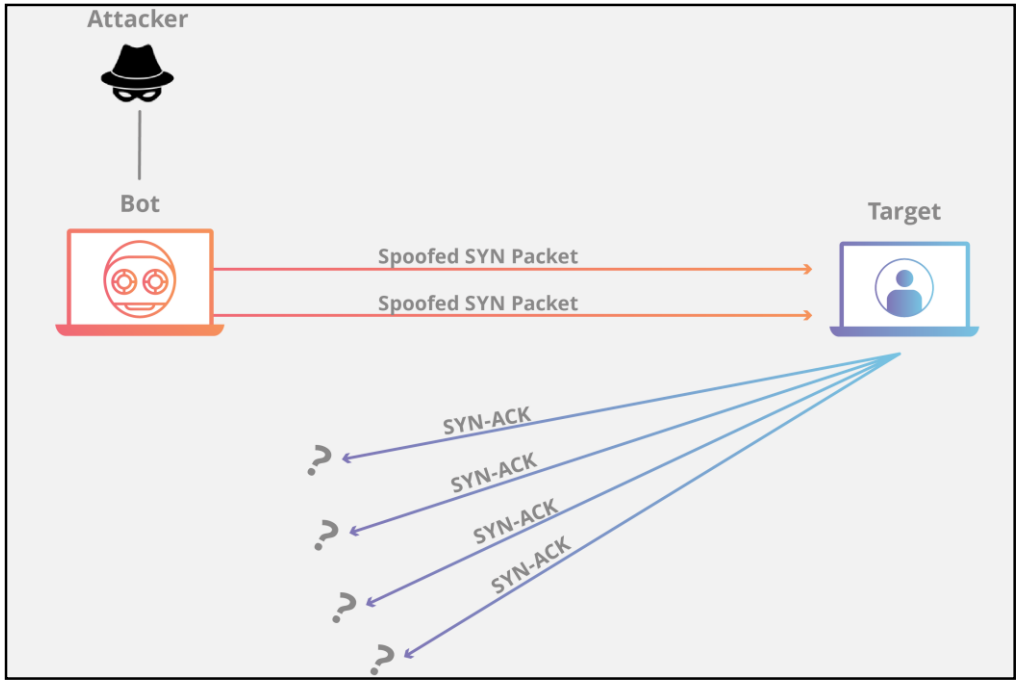
Angriffsszenarien: Man in the middle - Ergebnisse

- Steckdose 1
  Topic, Nachrichteninhalt (Klartext) =>
  Steuerung möglich

- Steckdose 2
  Topic, Nachricht (verschlüsselt), localKey =>
  Auskunft über Betriebstatus

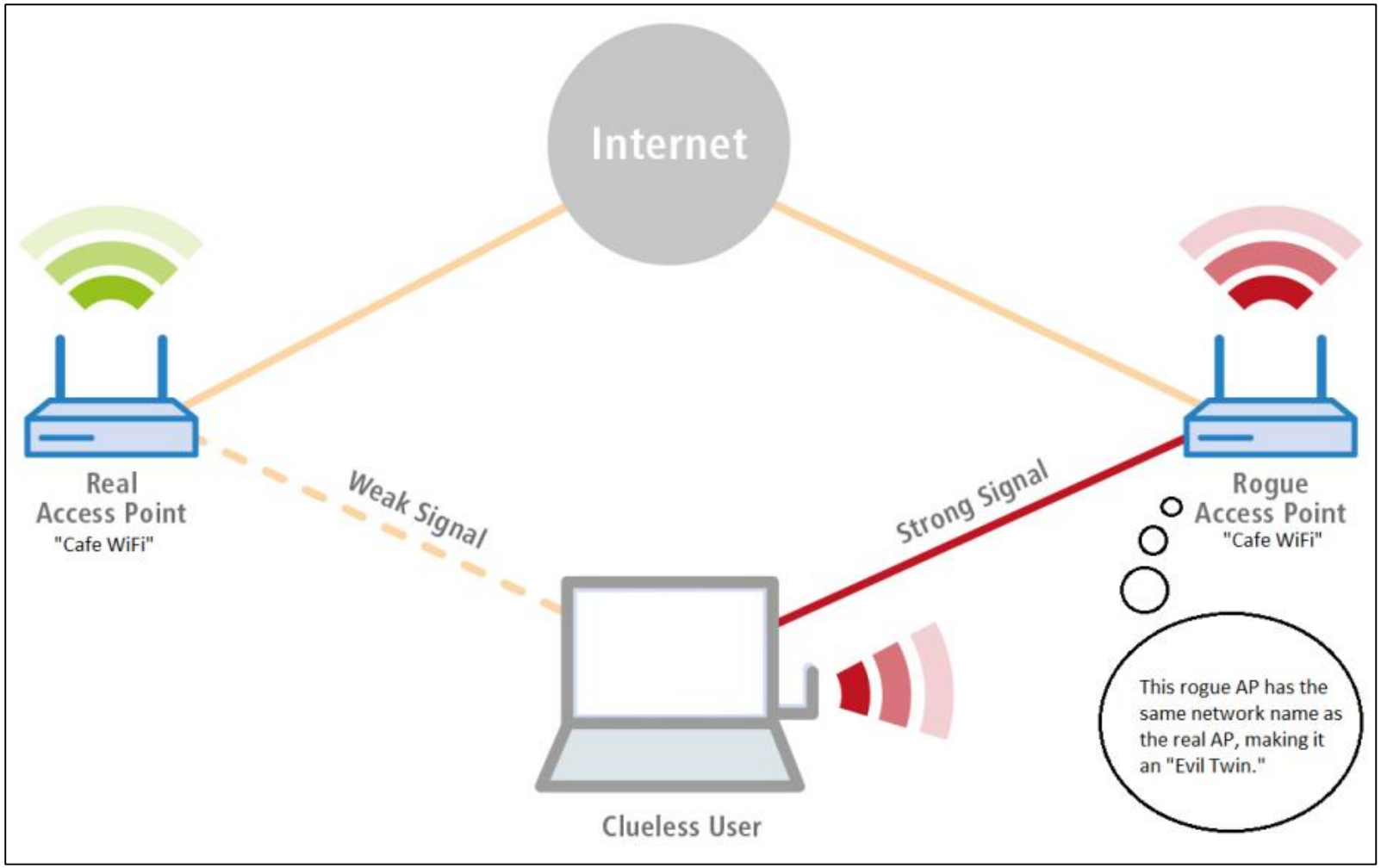
- Steckdose 3
  Zugangsdaten zum WLAN Netzwerk =>
  weitere Netzwerkteilnehmer werden zu potentiellen Zielen

Angriffsszenarien: Denial of Service

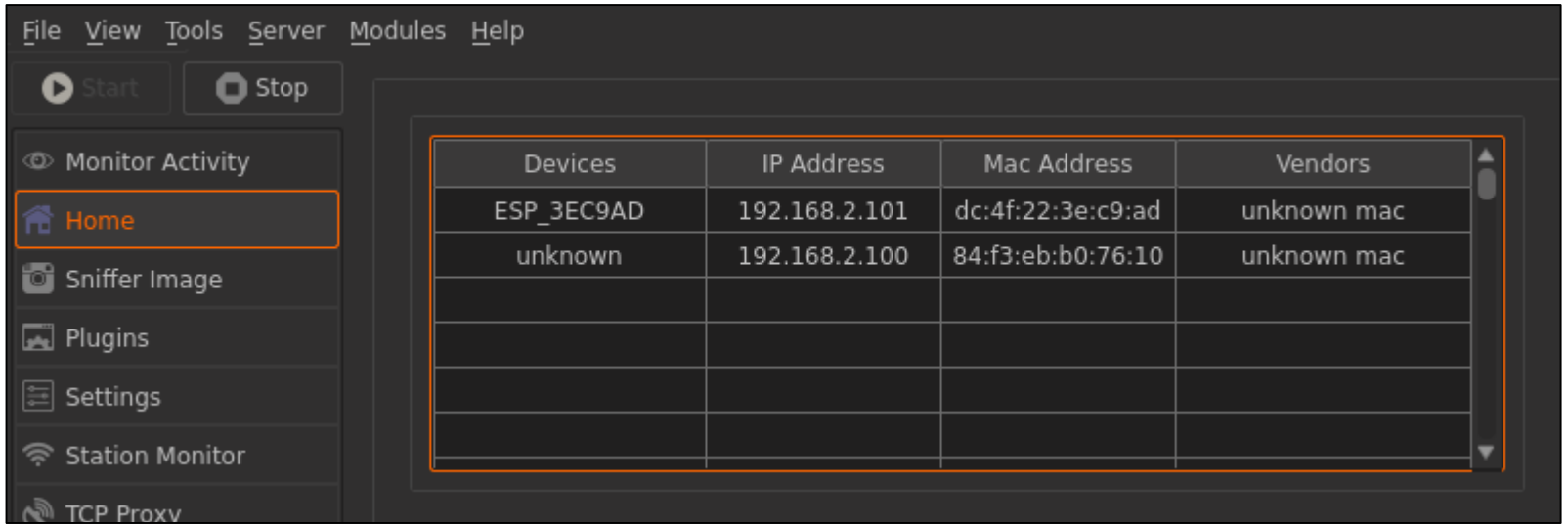


- Keine Kontrolle über das Gerät

Angriffsszenarien: Evil Twin



Angriffsszenarien: Evil Twin



- Stärkeres Signal mit gleicher SSID veranlasst Steckdosen zur Verbindung mit Evil Twin
- Steckdosen verbinden sich mit MQTT Broker beim Evil Twin

Angriffsszenarien: Evil Twin - Ergebnisse

- Keine Kontrolle vom rechtmäßigen Besitzer
- Kontrolle über Gerät möglich

Zusammenfassung

- Information zum Betriebstatus
- Kontrollentzug
- Kontrollübernahme
- Auslesen der WLAN Zugangsdaten

Fazit

- Jede Steckdose wies Sicherheitslücken auf
- Kein Standard in der Sicherheit
- TLS 1.2 möglich, aber nicht konsequent genutzt

Vielen Dank für Ihre Aufmerksamkeit !

Quellenangaben

Marc Mai. MQTT für Dummies. URL: https://blog.doubleslash.de/mqtt-fuer-dummies, 2016. Geladen am 10.04.2019

SecureBox. What is Man-in-the-Middle Attack?. URL: https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/. Geladen am 10.04.2019

Cloudflare. syn-flood-ddos-attack. URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/. Geladen am 10.04.2019

Thecybersecurityman. PenTest Edition: Creating an Evil Twin or Fake Access Point Using Aircrack-ng and Dnsmasq [Part 1 – Setup]. URL: https://thecybersecurityman.com/2018/08/11/pentest-edition-creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-1-setup/, 2018. Geladen am 10.04.2019