

Phase 3

SSL-Stripping und Verwandtes

Seminar: Das Internet der Dinge (IoT) - ein Hackerparadies?

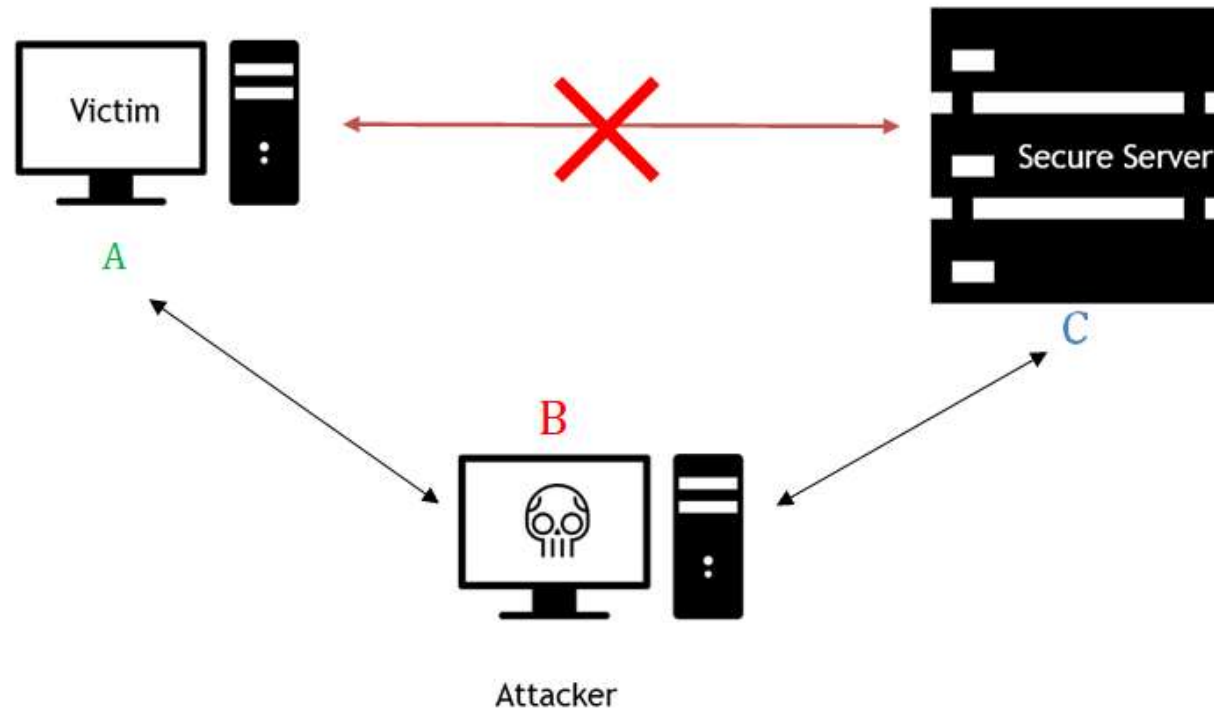
9 Dezember 2017

Alexander Korff Sergej Maul Yannik Stöckin Sebastian Philipp
Daniel Seidinger Fabian Neumeier Lukas Stöcklin Manuel Rickli
Desirée Nusch Samuel Hugger Clement Francois Joel Grossenbacher

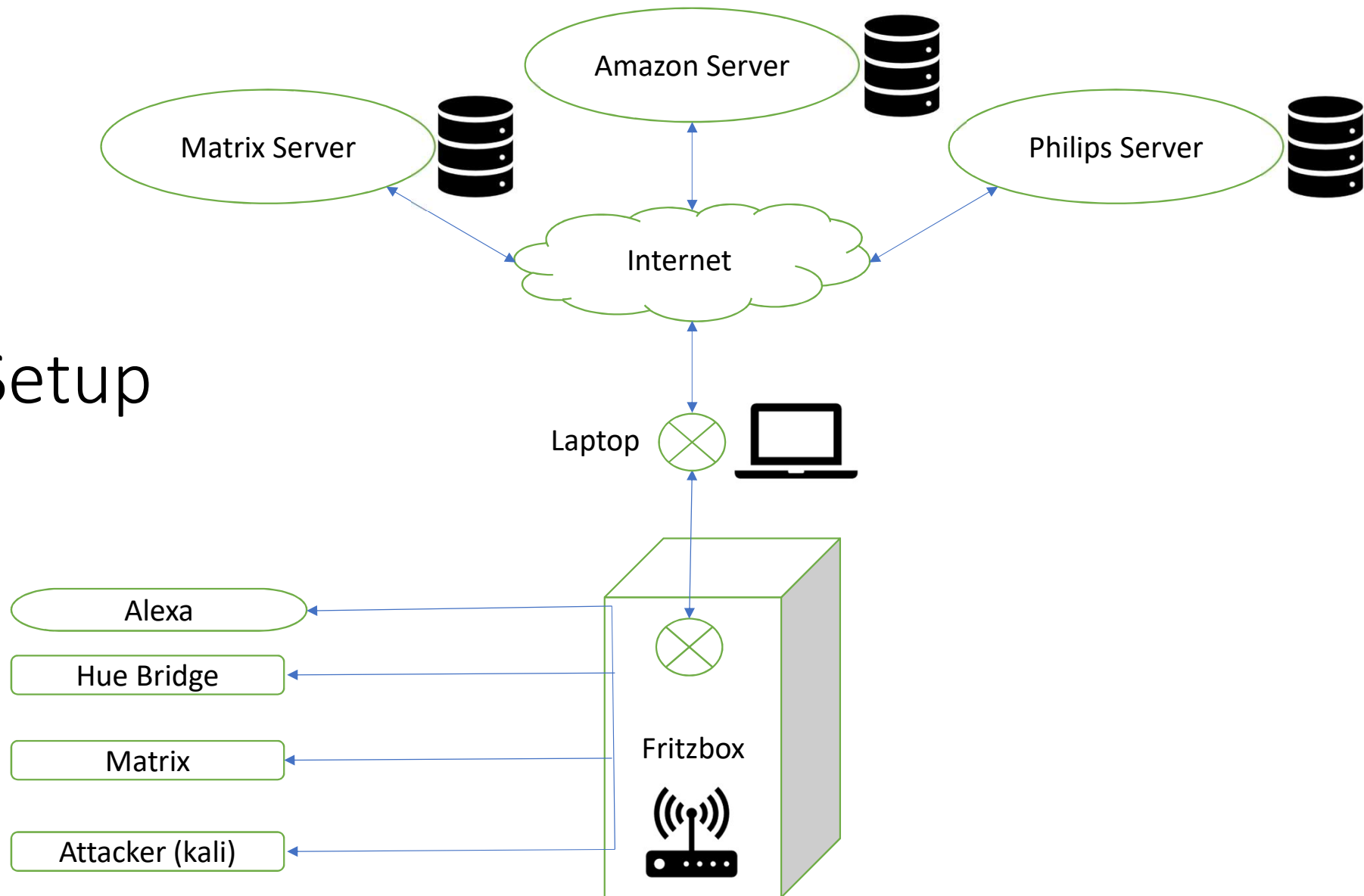
Inhalt

- I. Wiederholung
- II. Setup
- III. Philips Hue
 - i. ARP-Spoof | SSL Strip
 - ii. Playback
- IV. LED-Matrix
- V. Was nun?
- VI. Schlussfolgerungen

I. Wiederholung



II. Setup



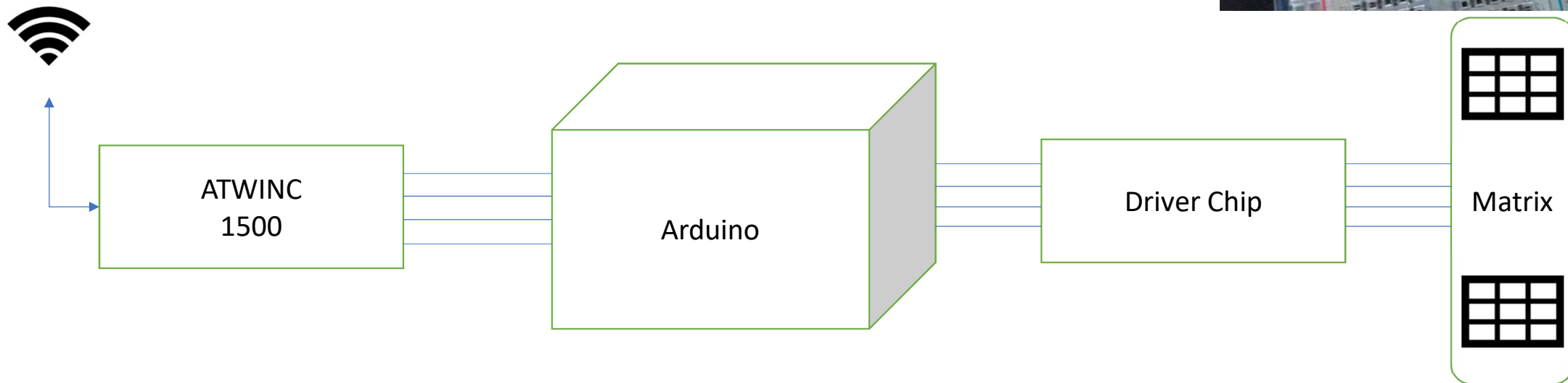
III. Philips Hue

- Faking the Gateway | ARP spoofing
 - Fritzbox ↔ Hue
 - DNS
 - TCP: Hue ↔ rackspace.com
 - TLSv1.2
- SSL Strip
 - SSDP
 - HTTP: GET Request Handler

Philips Hue cont.

- Blockieren Port 443, Ausweichen auf Port 80
 - HTTP: Hue ↔ bridge.meethue.com
 - Single Sign On Session
- TCP-Replay `tcpreplay -intf=wlan0 capt.pcap`
 - REVERSE ENGINEERING
 - ARP-spoof: Alexa ↔ Hue
 - Anschaltungsbeefehl abgefangen

IV. LED-Matrix



- Umbau von Ethernet zu Wifi
- Wifi-Chip ATWINC 1500 ermöglicht durch Auslagerung SSL-Verschlüsselung

LED-Matrix cont.

- Blockieren Port 443, Ausweichen auf Port 80
 - Keine Verbindung
- ARP-Spoof & SSL-Strip
 - nutzlos
- SSL-Sniff
 - Auch nicht

V. Was nun?

- Philips Hue: HTTP Protokoll
- Angriffe auf SSL/TLS
- Downgrade auf ältere Versionen
- Bekannte Bugs ausnutzen (DROWN, POODLE)

VI. Schlussfolgerungen

✗ Philips Hue

- Kommunikation mit den Servern ist verschlüsselt
ABER
- Im Netzwerk kann man HTTP Pakete verschicken

“Reducing security for the sake of interoperability”

✓ LED-Matrix

- Nicht manipulierbar (mit versuchten Mitteln)

⇒ SSL-Strip das falsche Tool