Phase 3
SSL-Stripping und Verwandtes

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

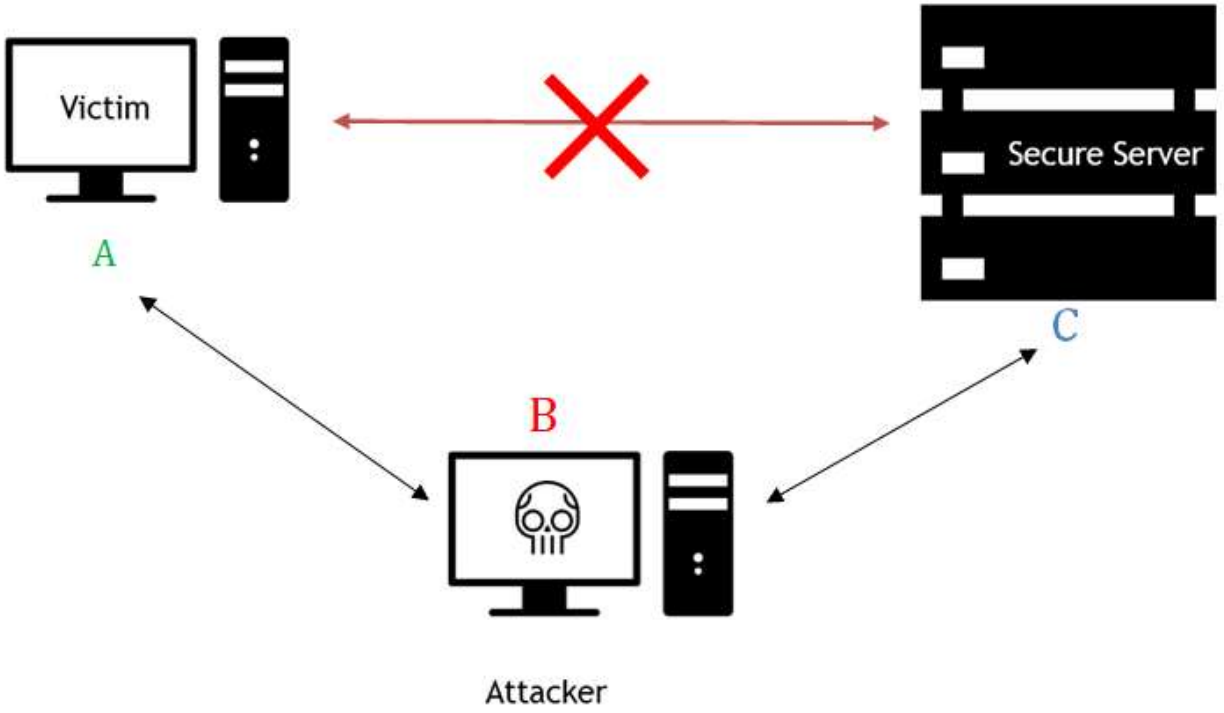
9 Dezember 2017

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

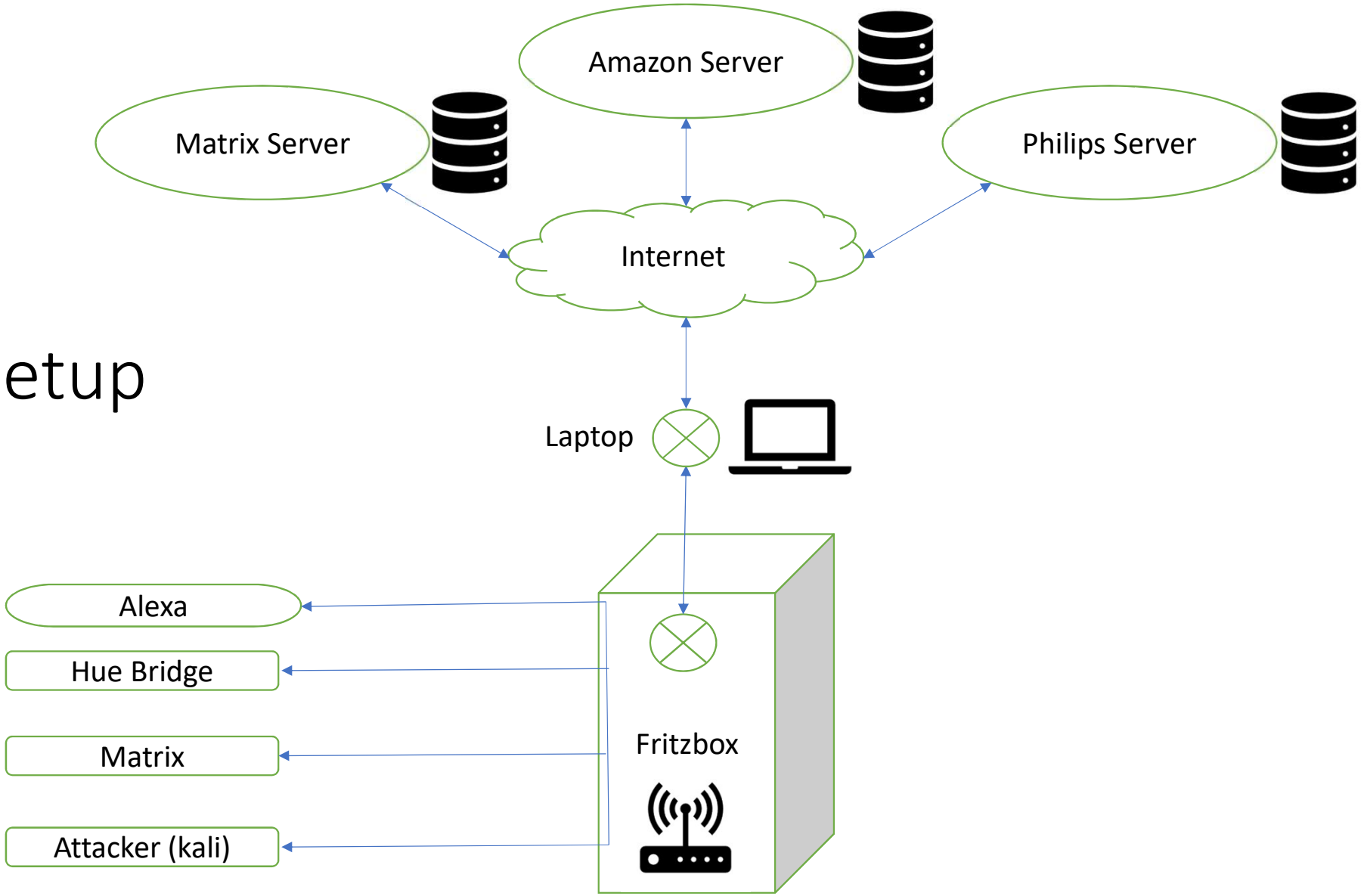
Inhalt

I. Wiederholung
II. Setup
III. Philips Hue
IV. LED-Matrix
V. Alexa
VI. Schlussfolgerungen
VII. Was nun?

I. Wiederholung



II. Setup


Amazon Server
Matrix Server
Philips Server
Internet
Laptop
Alexa
Hue Bridge
Matrix
Attacker (kali)
Fritzbox

III. Philips Hue

✓ Faking the Gateway | ARP spoofing
- Fritzbox ↔ Hue
  - DNS
  - TCP: Hue ↔ rackspace.com
  - TLSv1.2

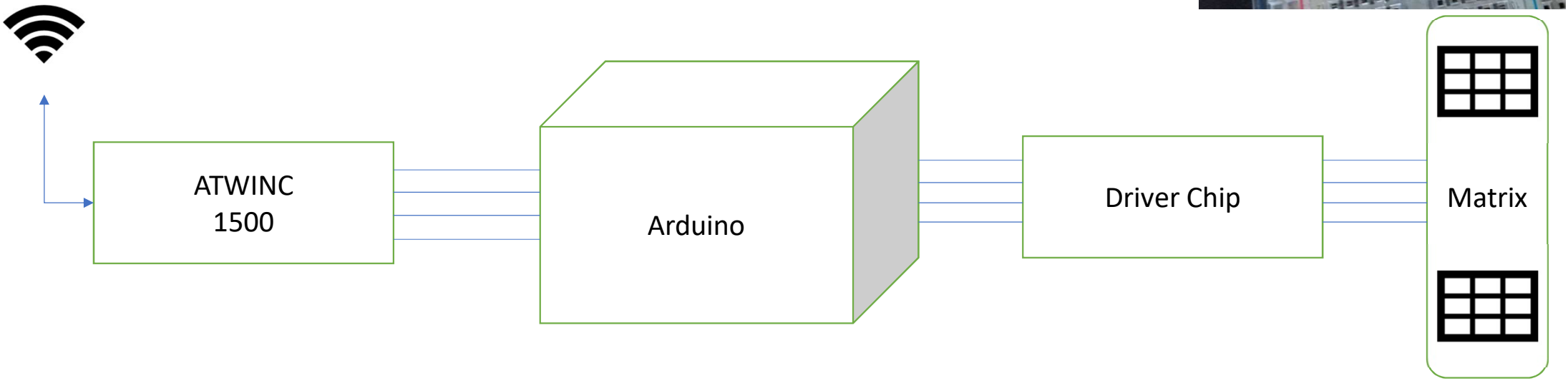
✓ SSL Strip
- SSDP
- HTTP: GET Request Handler

Philips Hue cont.

✓ Blockieren Port 443, Ausweichen auf Port 80
- HTTP: Hue ↔ bridge.meethue.com
- Single Sign On Session

✓ Reverse engineering
- ARP-spoof: Alexa ↔ Hue
- Anschaltungsbefehl abfangen

IV. LED-Matrix



- Umbau von Ethernet zu Wifi
- Wifi-Chip ATWINC1500 ermöglicht durch Auslagerung SSL-Verschlüsselung

LED-Matrix cont.

× blockieren Port 443, Ausweichen auf Port 80
  - Keine Verbindung

× ARP-Spoof & SSL-Strip
  - nutzlos

× SSL-Sniff

V. Alexa

- Versucht: Resultate wie bei LED-Matrix

- Certificate Pinning

  SSL-Sniff

  - ähnlich auch auf ATWINC1500

VI. Schlussfolgerungen

✗ Philips Hue

- Kommunikation mit den Servern ist verschlüsselt

  ABER

- Im Netzwerk kann man HTTP Pakete verschicken

✓ LED-Matrix | Alexa

- Nicht manipulierbar (mit versuchten Mitteln)

⇒ SSL-Strip das falsche Tool

⇒ *“Reducing security for the sake of interoperability”*

VII. Was nun?

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