Bite The Bytes - Informatik studieren in Weimar

Smart Home Hacking

Marcus Almert

Bauhaus-Universität Weimar

Fakultät Medien

4. November 2022

Vorwort

- „Hacken“ von dritten ist **illegal**!
- Experimentelle Angriffe ausschließlich auf eigene Geräte und Accounts

- Wieso beschäftigen wir uns mit „Hacken“?

→ Wissenschaftliche Untersuchungen weisen auf Missstände hin und tragen zur Verbesserung bei

Section 1

Was ist Smart Home?

Was ist Smart Home?

- Geräte, die miteinander kommunizieren, agieren und zentral gesteuert sind
- Kommunikation erfolgt meist über Bluetooth oder WIFI
- Steuerung durch Apps und Sprachassistenten

Vorteile von Smart Home

- Erhöhung der Lebens- und Wohnqualität (smarte Glühbirne)
- Steigerung der Energieeffizienz (smarte Thermostate)
- Verbesserung der Sicherheit (smarte Überwachungskameras)

Smarte Türklingeln

- Bestandteile:
  - Kamera
  - Bewegungssensor
  - Mikrofon und Lautsprecher
  - Klingeltaste
- Funktionen:
  - Fernzugriff via App (Account notwendig)
  - Live Video und Ton Stream
  - Benachrichtigungen bei Bewegungen
  - Anruf auf Smartphone bei Klingeln
  - Automatisches Aufnehmen von Fotos und Videos

[1]

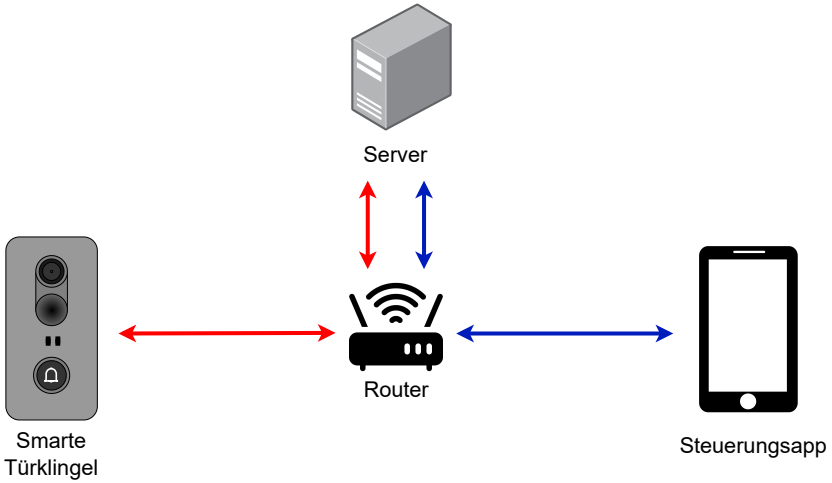
Section 2

Smart Home Hacking

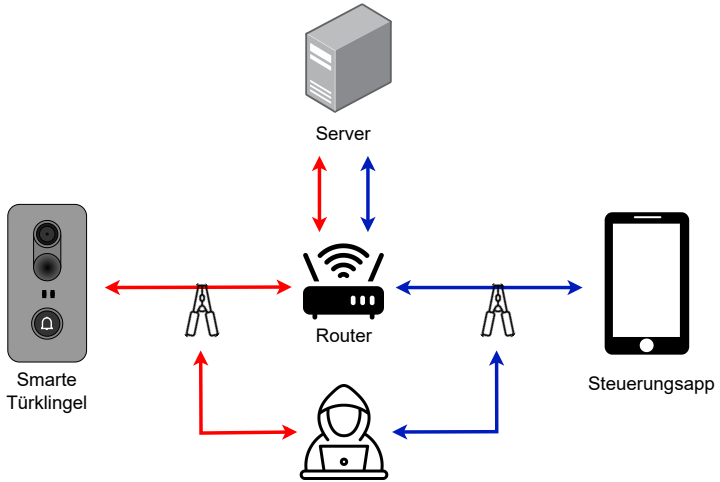
Ziele und Vorgehensweise

- Ziele:
  - Unerlaubter Zugriff auf Ressourcen (Daten und Funktionen)
  - Denial of Service
  - Einschleusen von Schadsoftware (z.B. Viren, Trojaner, Ransomware)
  - Infiltration von weiteren Geräten
- Vorgehensweise:
  - System und Gerät Verstehen
  - Angriffspunkte und Schwachstellen Identifizieren
  - Angriffe Ausführen
  - Auswertung

Vorgehensweise am Beispiel von smarten Türklingeln



Person-in-the-middle Attacke



Ergebnis der Person-in-the-middle Attacke

Kommunikation verletzt Prinzipien der Sicherheit:

- Vertraulichkeit
- Integrität
- Authentizität

Ergebnis der Person-in-the-middle Attacke

Kommunikation verletzt Prinzipien der Sicherheit:

- Vertraulichkeit
- Integrität
- Authentizität

Beispiel für abgehörte Daten:

```
POST /login HTTP/2.0
    Host:       api.gdxp.com
    username:   <zensiert>
    password:   <zensiert>
```

Auswertung des Angriffs I

Teil 1: Auf was haben wir unerlaubten Zugriff?

- Steuerungsaccount

→ Fotos und Videos im Cloudspeicher

→ Live Video und Audio Stream

→ Geräte und Account Einstellungen

Auswertung des Angriffs II

Teil 2: Was können wir damit machen?

- Identifizierung des Ortes (durch Kamera, WIFI, IP-Adresse)
- Bewegungsprofil Erstellen: Wann ist wer wo?
- Accounteinstellungen: Passwort ändern)
- Geräteeinstellungen (Kamera und Mikrofon ausschalten)
- Cloudspeicher: Diebstahl und Löschen von Daten,
- Zugriff zu Accounts mit gleichen oder ähnlichen Zugangsdaten

Fazit

- Smart Home Geräte können viele Sicherheitsrisiken mit sich bringen
- Es herrscht eine riesige Intransparenz was mit online gesammelten Daten passiert

→ Sicherheit der Geräte sollte nicht überschätzt werden

Vielen Dank für Eure Aufmerksamkeit!

Gibt es Fragen?