Sicherheitsanalyse von Bluetooth Low Energy Geräten in der Heimautomatisierung

24. ITG Fachtagung Mobilkommunikation Osnabrück

Kevin Fröhlich, Michael Rademacher, Karl Jonas

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

16. Mai 2019

Inhalt

Einleitung

Heimautomatisierung:

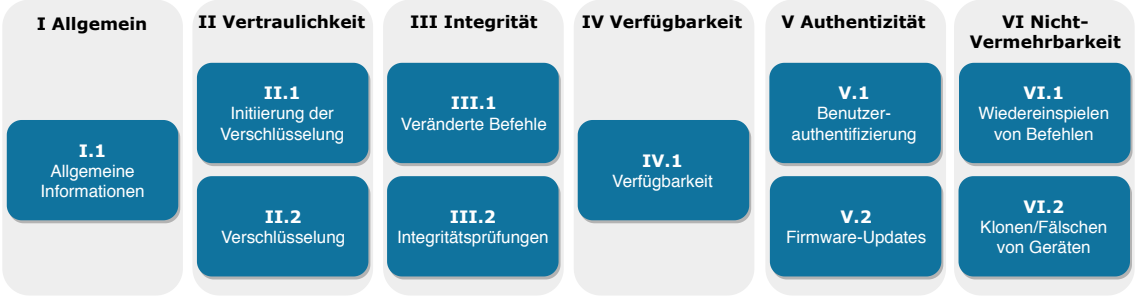
- Starker Anstieg von Geräten in der Heimautomatisierung
- Bluetooth Low Energy (BLE): Funkprotokoll in der Heimautomatisierung
- Angriffe auf verschiedene Funkprotokolle in Vergangenheit

Ziel:

- Vorstellung einer strukturierten Vorgehensweise zur Analyse
- Bewertung der Sicherheit von Geräten

Vorgehensweise

- Strukturierte Analyse der Sicherheit von BLE-Geräten
- **6 Kategorien**, mehrere Unterkategorien
- Fragestellungen zur Beurteilung



Vorgehensweise — Beispiel

II Vertraulichkeit

II.1
Initiierung der Verschlüsselung

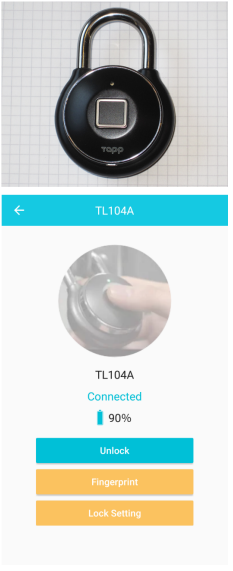
a) Schlüssel fest einprogrammiert oder bekannt?
b) Unverschlüsselte Schlüsselübertragung?
c) Manipulationsmöglichkeiten, sodass unsicheres Verfahren verwendet wird (Downgrade)?
d) Man-in-the-Middle (MITM) möglich?

II.2
Verschlüsselung

a) Wird Verschlüsselung eingesetzt?
b) Verschlüsselung unsicher oder bekannte Lücken?
c) Gleiche Befehle immer gleich verschlüsselt?
d) Rückschlüsse auf Inhalt anhand von Befehlslängen oder Zeichenfolgen möglich?

Vorhängeschloss

- **II Vertraulichkeit:** Keine Verschlüsselung
- **III Integrität:** Keine Integritätsprüfung
- **IV Verfügbarkeit:** Keine Probleme durch Geräteausfall
- **V Authentizität:** Keine Benutzerdaten, Updates manuell
- **VI Nicht-Vermehrbarkeit:** Statische Befehle, Replay möglich



Ergebnis

Keine Verschlüsselung, statische Befehle nachstellbar, Replay

Heizkörperthermostat

- **II Vertraulichkeit:** Verschlüsselung, aber Downgrade möglich
- **III Integrität:** Integritätsprüfung, keine Manipulation
- **IV Verfügbarkeit:** Keine Probleme durch Geräteausfall
- **V Authentizität:** Schlüssel, Updates manuell
- **VI Nicht-Vermehrbarkeit:** Schutz vor Replay

Ergebnis

Start der Verschlüsselung kann umgangen werden

Fazit

- Strukturierte Vorgehensweise ermöglicht Sicherheitsanalyse
- Sicherheitsfunktionen im BLE-Standard vorgesehen
- Umsetzung Herstellern überlassen
- **7 Geräte** untersucht, davon **5 Geräte** vollständig übernehmbar

Hauptprobleme

- Keine Verschlüsselung
- Unsichere oder keine Integritätsprüfung
- Kein Schutz vor Replay
- Implementierungsfehler

Ende

Danke für die Aufmerksamkeit!