TECHNISCHE UNIVERSITÄT
BERGAKADEMIE FREIBERG
Die Ressourcenuniversität. Seit 1765.

Fakultät für Mathematik und Informatik
Institut für Informatik
Lehrstuhl für Betriebssysteme und Kommunikationstechnologien

Bakkalaureatsarbeit

Entwicklung einer Sicherheitsinfrastruktur zur Bluetooth-Kommunikation zwischen Smartphone und Mikrocontroller

Marian Käsemodel

Angewandte Informatik
Vertiefung: Technik

Matrikel: 62 412

14. Mai 2021

Betreuer/1. Korrektor:
Prof. Dr. Konrad Froitzheim

2. Korrektor:
M.Sc. Jonas Treumer

Eidesstattliche Erklärung

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen Hilfsmittel als die angegebenen benutzt habe. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, habe ich in jedem einzelnen Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht. Diese Versicherung bezieht sich auch auf die bildlichen Darstellungen.

14. Mai 2021 Marian Käsemodel

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Themenstellung

- BT als Kommunikationstechnolgie verbreitet -> BLE als Variante mit geringem Energieverbrauch ideal für batteriebetriebene Systeme -> überleiten zu SteigtUM
- Projekt SteigtUM
  - ist Hintergrund dieser Arbeit, erklären: Verleihdienst für elektrische Kleinfahrzeuge (u.a. Lastenfahrräder)
  - Individualverkehr für Kurzstrecken emissionsfrei gestalten
  - Kommunikation muss sicher sein, da Buchungsvorgänge, Datenschutz, verhindern von Manipulation, ...
- daraus auf allgemeine Lösung ableiten für eine sichere Infrastruktur basierend auf BLE zwischen MCU und Smartphone
- Infrastruktur beschränkt sich nicht zwangsweise nur auf MCU und Smartphone

1.2 Problemstellung

- Ziel ist Entwicklung einer Infrastruktur, die eine sichere Kommunikation zwischen MCU und Smartphone ermöglicht
- dabei sollen MCU und Smartphone nur mittels BLE miteinander kommunizieren
- BLE weißt einige Schwachstellen auf, weswegen eine Lösung gefordert ist um BLE sicher zwischen MCU und Smartphone zu nutzen
  - Schutz vor Außenstehenden und Software, die auf dem Smartphone agiert.
- Zum Beweis der Funktionsfähigkeit der Infrastruktur dient eine Implementierung, die sich auf den Ausleihprozess des Projektes SteigtUM bezieht
  - weitere Kommunikationsparteien (Backend) und deren Verbindungen werden nur simuliert dargestellt
  - Verbindung zwischen Fahrrad und Backend nicht zwingend erforderlich
  - bei Wiederherstellung einer abgebrochenen Verbindung soll die Verbindung zwische App und Backend nicht zwingend sein

2 Grundlagen zu Bluetooth Low Energy

2.1 Abgrenzung von Bluetooth Classic

- Wesentliche Unterschiede zwischen BLE und BT Classic

2.2 Aufbau

2.2.1 Controller Stack

- Funktionsweise der Layer: PHY und LL (Link Layer)

2.2.2 Host Controller Interface

2.2.3 Host Stack

- Funktionsweise der Layer: L2CAP (Logical Link Control and Adaption Protocol), GATT (Genric Attribute Profile), GAP (Generic Access Profile), Argumentation, wieso L2CAP (und nicht GATT) genutzt wird erst in Sektion Ïnfrastruktur"
- SMP (Security Manager Protocol)

2.3 Verbindungsaufbau / Pairing

- Pairing-Methoden vorstellen mit Unterschieden in den BT-Versionen

2.4 Sicherheitslücken

- Pairing-Methoden nicht in allen Versionen sicher (MITM, passives Abhören)
- Keine Application-Layer-Security
- ...

3 Grundlagen zu Transport Layer Security

- allgemeine Erläuterung
- sichere Versionen
- nicht nur für gewöhnliche Anwendungsbeispiele geeignet

3.1 Zertifikate

- Aufbau
- CAs
- Authentifikation/Authentifizierung

3.2 Algorithmen

- Schlüsselaustausch
- Verschlüsselung
- Datenintegrität
- Ciphersuits

3.3 Protokoll

- Handshake
- Record

3.4 Sicherheit

- Angriffe gegen TLS
- Forward Secrecy
- TLS Interception

4 Infrastruktur

4.1 Ziel der Infrastruktur

- sichere Kommunikation zwischen Smartphone und MCU mittels TLS über BLE
- ist unabhängig vom Projekt SteigtUM

4.2 Topologie

- Client, Server
- CA

4.3 Transport

- Verwendung von L2CAP (und warum GATT ungeeignet ist)

4.4 Sicherheit

- Positionierung und Begründung, dass Sicherheitsfeatures von BLE keinen vollständigen Schutz bieten (auch keine App-Layer-Security)
- deswegen TLS verwenden für MITM-Protection, Schutz gegen passives Anhören, Datenintegrität, Ende-zu-Ende-Verschlüsselung, App-Layer-Security

4.5 Verbindungsaufbau

- GAP (gewählte Pairing-Methode (nach BT-Version) dürfte keinen Einfluss haben)
- TLS-Handshake
- erst in Sektion Ïmplementierungäuf Subscription eingehen

5 Implementierung

5.1 Ziel der Implementierung

- Bezug zu SteigtUM / Verleih elektrischer Kleinfahrzeuge
- Subscription-Modell sorgt dafür, dass das Fahrzeug sicherstellen kann, dass es vom Nutzer ausgeliehen werden darf

5.2 Topologie

- Client
- Server
- Backend
- CA

5.3 Hardware und Software

- Android Smartphone, Android- und BT-Version
- Android Bibliotheken, ...
- MCU: ESP32... , BT-Version, weitere Eigenschaften/Features
- ESP Software: FreeRTOS, SPIFFS (Filesystem), nimBLE, mbedTLS (TLS Version angeben)

5.4 Transport und Sicherheit

- L2CAP
- Verwaltung des RX-Buffers
- Durchsatz
- Konfiguration (MTU, ...)
- gewählte Ciphersuites
- ...

5.5 Ausleihprozess

- Ausgangssituationen, Ablauf und Probleme des Ausleihprozesses

5.5.1 Verbindungsaufbau

- ähnlich wie bei Erklärung der Infrastruktur nur mit Subscription und deren Übertragung und Verifizierung
- erläutern was passiert, wenn Verbindung zum Fahrzeug abgebrochen ist (bspw. durch Abstellen des Fahrzeugs und kurzzeitiges Verlassen der BLE-Funkreichweite) und nun wiederhergestellt werden soll

5.5.2 Beenden des Ausleihprozesses

- erklären, wie sichergestellt wird, dass der Ausleihprozess vom Nutzer aus beendet wurde
- bzw. Beendigung der Verbindung durch das Fahrzeug, wenn die Standzeit (Nutzer verließ BLE-Funkreichweite) überschritten wurde

6 Ausblick

- Weiterführung der Arbeit

7 Zusammenfassung