Hacking von I LOCK IT

Marius Würstle

May 13, 2021

Contents

1 Motivation

2 Grundbegriffe

CRCInit

3 Problemstellung

4 Bluetooth Technologie

Bluetooth ist der Industriestandard für die drahtlose Datenübertragung über kurze Distanz. Die Slaves lauschen auf 32 unterschiedlichen Hop-Kanälen, dieser Modus nennt sich Scan-Modus. Der Verbindungsaufbau geht von einem Master Gerät aus und wird mittels einer Inquiry-Nachricht und einer anschließenden Page-Nachricht hergestellt. Falls die Hardware-Adresse(48-Bit lange eindeutige ID) den Geräten bekannt ist wird keine Page Nachricht mehr versendet. In der Page Phase sendet der Master 16 identische Page Nachrichten auf 16 verschiedene Channels.
Bluetooth Low Energy (BLE) wurde für Systeme entwickelt, die auf einem Akku basieren und mit einem möglichst geringen Stromverbrauch funktionieren müssen. Dies wird durch kurze Aktivitätszeiten erreicht, das heißt es wird nur gesendet bzw. gelauscht solange es notwendig ist. Zusätzlich werden die Datenpakete gesammelt und alle zusammen versandt. Darüber hinaus spart die geringe Übertragungsgeschwindigkeit Strom.

4.1 Advertising

BLE nutzt 40 verschieden Channels im Bereich von 2402 MHz bis 2480 MHz. Die einzelnen Channels sind 2 MHz voneinander entfernt, davon werden Channel 37, 38 und 39 nur für das Advertisement verwendet.
Die sogenannten Adveritsements sind die Pakete, die von den Peripherie Geräten ausgesendet werden, um auf sich aufmerksam zu machen. Es gibt noch einige Spezifikationen, der einzelnen Advertisment-Pakete, dies würde allerdings den Rahmen der Arbeit sprengen. Meist sind in diesem Paket der Gerätename, die Service-UUID und die RSSI (RSSI Pegel und Signalstärke). Falls die 31 Bytes an Advertisement-Data des Pakets nicht ausreichen, um alle Informationen zu versenden, kann ein Scan-Request gesendet werden. Welcher logischerweise mit den restlichen Daten in einem Scan-Response beantwortet wird. Allerdings muss das Zentrale System die Anfrage auslösen, um die Daten zu bekommen.

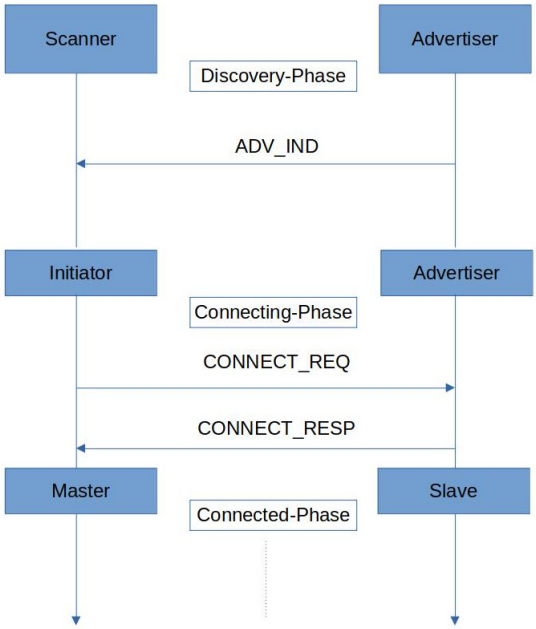

Abbildung 1: Verbindungsaufbau unter BLE

4.2 Discovery-Phase

Die Peripherie Geräte senden ihre Advertisements in dieser Phase auf die 3 oben gennanten Channel mit den auch oben genannten Informationen. Hier könnte auch ein Scan-Request getätigt werden.

4.3 Connection-Phase

Der Scanner wird jetzt "Initiatior" gennannt und intiert mit einem "CONNECT_REQ" den Verbindungsaufbau. Dieses Paket beinhaltet die Frequency hopping sequence, Connection Intervall, Slave Latency, Supervision Timeout. Nach dem Versenden oder dem Erhalten dieses Pakets gelten die Systeme als verbunden. [1]

4.4 Connected-Phase

Nachdem dem Verbindungsaufbau wird der Initiator zum Master und der Advertiser zum Slave und es können Daten ausgetauscht werden. Bei BLE wird dies über den Linked-Layer gemacht, welcher auch verschlüsselt werden kann. Die beiden Geräte tauschen in regelmäßigen Abständen Daten Pakete aus, diese werden "connection events" genannt

4.5 Security

Die Datenpakete können, wie oben schon erwähnt, verschlüsselt werden. Diese Pakete enthalten zusätzlich einen MIC (message Integrity Check), der den Sender authentifiziert. Auch enthält das Paket einen Packet Zähler, um einen replay-Angriff zu verhindern. Verschlüsselt wird mit dem AES-128 Algorithmus und den CCM Modus (Cipher Block Chaining-Message Authentication Code). Eine solche Verbindung kann erst nach dem Aufbau der Connection erstellt werden. Hierfür mussen die geräten sich pairen, wie dies funktioniert gehe ich später ein.

4.5.1 Pairing

Paring wird dann gestartet sobald zwei Geräte miteinander verbunden sind und sie etwas ausführen wollen, dass Security benötigt.
Das Pairning beinhaltet drei wichitige Schritte:

- Authentifizierung von 2 Geräten:
  Zu Beginn werden die Input und Output Fähigkeiten der geräte ausgetauscht. Anhand dieser wird ausgewählt wie die Geräte gepaired werden können und welche Art von Keys in der letzten Phase versandt werden.

- Erstellen und Austauschen eines Short-Term-Keys(STK):
  In diesem Schritt einigen sich die beiden Systeme auf eine Art den STK zu berechnen. Hierbei spielen die I/O Fähigkeiten der Geräte eine große Rolle.

- Austauschen eines Long-Term-Keys(LTK):
  Zunächst prüft der Intiator, ob das gegenüberliegende Gerät dazu fähig ist sich zu binden. Danach wird der LTK über den durch den STK encrypteten Kanal versendet.

5 Sicherheitsanalyse

Herausfinden der encrypt Methode beim Austausch des STK, manche sind nicht MTM sicher?
Untersuchung nach Connection erstellung, ob derk LTK geknackt werden kann?

6 Umsetzung

Denial of Service Angriff mit BtleJack durch übernahme der Verbindung. (funktioniert schon)

7 Fazit/Ausblick

Nennung der Sicherheitslücken und Ideen wie man diese verhindern kann.

References

[1] Microchip Technology, Inc., 2021. `https://microchipdeveloper.com/wireless:ble-link-layer-connections` [aufgerufen am 12.05.2021].

https://www.rfwireless-world.com/Terminology/BLE-Connection-Establishment-Procedure.html 20 März 2021
https://microchipdeveloper.com/wireless:ble-link-layer-security