Proseminar Kryptographische Protokolle SS 2009

Bluetooth

Medin Imamovic

1 Einleitung

Bluetooth ist eine Technologie zur drahtlosen Kommunikation. Die Idee geht zurück ins Jahr 1994, als *Ericsson* mögliche Wege erforschen ließ um Kabelverbindungen zwischen Geräten überflüssig zu machen. Seit 1998 wird von der *Bluetooth Special Interest Group* (SIG) eine Bluetooth-Spezifikation entwickelt. Diese neue Technologie wurde zu Ehren des Wikinger-Königs Harald Blauzahn (Blaatand) Bluetooth genannt.

1.1 Technische Grundlagen

Bluetooth verwendet zwei verschiedene Kommunikationstypen bzw. physikalische Verbindungen zwischen Geräten :

- die leitungsvermittelte synchrone Kommunikation (SCO) und
- die paketvermittelte asynchrone Kommunikation (ASL).

SCO wird zur Übertragung von Sprachdaten verwendet. Und alles außer Sprachen wird über ASL übertragen. Bluetooth-Datenpakete bestehen aus einem 72 Bit Zugriffscode, einem 54 Bit Header sowie einem variablen Nutzdatenfeld von 0 – 2745 Bit.

Netze in denen sich Geräte mittels Bluetooth zusammenfinden werden *Piconetze* genannt. In so einem Netz teilen sich max. 8 Geräte den gleichen Funkkanal. Es agiert ein Gerät als *Master*, die restlichen als *Slaves*. Will ein neues Gerät beitreten so sendet es eine Inquery-Nachricht und alle erreichbaren Geräte antworten. Abhängig von den Sicherheitseinstellungen kann das Gerät nun eine direkte Kommunikation mit dem Master aufnehmen.
Mehrere Piconetze bilden ein *Scatternetz*. Hierbei ist es Möglich das ein Slave mit verschiedenen Mastern in den verschiedenen Piconetzen verbunden ist. Jedoch kann auch ein Master eines Piconetzes ein Slave eines anderen Netzes sein.

1.2 Protokollstack

Die Grundlage des Bluetooth-Protokollstacks bildet die ISO-OSI Schichtung. Es werden neben den Bluetooth-spezifischen *Link Manager Protokoll* (LMP) und dem *Logical Link Control and Adaption Layer* (L2CAP) Protokollen auch allgemein verwendete Protokolle wie *OBEX* (Object Exchange Protocol), UDP, TCP oder WAP benutzt. Durch das Basisband, das gemäß ISO-OSI Schichtung als Protokoll für die Bitübertragung definiert ist, ermöglicht SCO und ACL Verbindungen. Audiodateien können direkt ohne Beteiligung des L2CAP vom Basisband übertragen werden. Die Protokolle LMP und L2CAP sind auf der nächst höheren Schicht. Die zentralen Aufgaben des LMP sind der Aufbau und die Steuerung der Verbindung zwischen den Geräten. In ihm sind auch die wichtigsten Sicherheitsdienste wie Authentifikation, Verschlüsselung und Schlüsselaustausch verankert. Das L2CAP ist nur für die ACL-Verbindungen und für das Senden und Empfangen von Datenpaketen der höhere Ebene definiert. Über das Basisband können Datenpakete mit max. 341 Byte übertragen werden, daher müssen vom L2CAP größere Datenpakete vor der Übertragung in kleinere

zerlegt und wieder korrekt zusammengefügt. Ein weiteres Protokoll, das Geräteinformationen, Dienste und Leistungsdaten erfragen kann ist das Service Discovery Protokoll (SDP). Die Protokolle RFCOMM und TCS BIN sind für die herkömmliche Kabelverbindung verantwortlich.
OBEX wurde ursprünglich zur Infrarot-Kommunikation entwickelt, aber im Prinzip ist es eine vereinfachte Form des http Protokolls zum Austausch von Objekten.
Für den Aufbau und die Verwaltung von Verbindungen zwischen Bluetooth-Geräten ist der Link Manager verantwortlich. Diese Software läuft auf jedem Bluetooth-Gerät. Die Manager tauschen Nachrichten über das LMP.

2 Schlüsselmanagement

Alle Sicherheitsmaßnahmen auf der Verbindungsebene basieren auf 128 Bit *Verbindungsschlüsseln*. Diese werden zwischen zwei Partnern vereinbart und sind die Basis zur Durchführung der Geräteauthentifikation. Aus ihm wird der geheime Authentifikationsschlüssel abgeleitet. Durch die Trennung zwischen Authentifikations- und Verbindungschlüssel ist es möglich für die Datenvermittlung auch kürzere Schlüssel zu verwenden. Die Länge wird bei der Herstellung festgestellt und kann nicht verändert werden. Verbindungschlüssel können temporär oder semi-permanent sein.
Da ein Verbindungsschlüssel für verschiedene Aufgaben verwendet wird, werden 4 Typen von Verbindungsschlüsseln unterschieden. Nämlich, der *Geräte-*, der *Initialisierungs-*, der *Kombinations-* und der *Masterschlüssel*. Der Geräteschlüssel wird aus einer 128 Bit Zufallszahl sowie der 48 Bit Geräteadresse BD_ADDR, die von der IEEE eindeutig definiert wird, gebildet. Dieser Schlüssel ist gerätespezifisch und wird auf dem Gerät gespeichert und nicht mehr geändert. Wenn zwei Geräte noch keinen gemeinsamen Schlüssel ausgetauscht haben, so erfolgt beim erstmaligen Kontakt das s.g. Pairing. Dieses erfordert von den Geräten dass sie über eine gemeinsame PIN verfügen, um daraus den benötigten Schlüssel zu berechnen. Beim Pairing wird die PIN, deren Länge zwischen 1 und 16 Byte variieren kann, auf beiden Geräten eingegeben z.B. Handy-Laptop. Nach der erfolgreichen PIN-Eingabe wird mit dem Schlüsselgenerierungsverfahrens E22 der Initialisierungsschlüssel erzeugt. Dieser ist 128 Bit lang und wird aus der PIN, der Geräteadresse des angefragten Geräts und der Zufallszahl RAND gebildet: IK = E22 (PIN, BD_ADDR, RAND). Der IK wird zum sicheren Austausch von Informationen in der Vereinbarung eines Verbindungsschlüssels verwendet und danach vernichtet. Im Verlauf des Initialisierungsprozesses wird von Informationen, die von zwei Geräten A und B stammen, der *Kombinationsschlüssel* abgeleitet. Dazu generieren beide Geräte jeweils eine Zufallszahl, anschließend unter Verwendung der Geräteadresse einen Schlüssel K_A bzw. K_B. Im nächsten Schritt werden die Zufallszahlen ausgetauscht, indem man den IK mittels XOR verknüpft. Durch eine erneute XOR Verknüpfung mit IK können die Geräte die Zufallszahlen ihres Partners wiederherstellen. Damit berechnet A den Schlüssel K_B, und B K_A. Zum Schluss wird durch eine XOR Verknüpfung der beiden Schlüssel der Kombinationsschlüssel erzeugt. Der Masterschlüssel ist ein temporärer Schlüssel der benötigt wird wenn Informationen zu mehreren Geräten übertragen werden müssen. Dieser wird mittels E22 und zweier Zufallszahlen gebildet.

2.1 Authentifikation

Die Authentifikation basiert auf einem *Challenge-Response Protokoll*. Dazu wird eine 128 Bit Zufallszahl als Challenge gesendet. Der Partner antwortet in dem er eine Antwort berechnet die aus der eigenen Geräteadresse und einem 128 Bit Verbindungsschlüssel K besteht. Aus diesem symmetrischen Schlüssel berechnen die Partner den Authentication Ciphering Offset Wert, der später bei der Erzeugung des Kommunikationsschlüssels verwendet wird. Besteht

beim Pairing kein solcher Schlüssel so die Nachricht LMP_not_accepted mit dem Grund key_missing gesendet. Ist eine Authentifikation fehlgeschlagen so muss ein Zeitintervall abgewartet werden bevor eine neue Anfrage gestellt werden kann. Dieses Zeitintervall verlängert sich exponentiell mit jedem Fehlversuch.

3 Sicherheit

Die Sicherheitsdienste laufen auf der Schicht 2 gemäß des ISO-OSI Protokolls. Diese umfassen die Authentifikation der Kommunikationspartner, Verschlüsselung der transferierten Daten und Autorisierung von Dienstnutzungen. Zu achten ist das die die Subjekte in Bluetooth Geräte sind und das die Autorisierung und Authentifikation auf Gerätebasis laufen. Bei Bluetooth werden drei Sicherheitsmodi unterschieden. Bei einer Anfrage wird überprüft in welchen Sicherheitsmodus sich die Geräte befinden und abhängig davon werden unterschiedliche Dienste angestoßen. Der Modus 1 ist der unsichere Modus der keine Sicherheitsdienste der Übertragungsebene vorsieht. Jedoch reagiert ein Gerät in diesem Modus auf eine Authentifizierungsanforderung eines anderen Geräts mit einer Authentifizierung. Daher wird dieser Modus nur für sicherheitsunkritische Anwendungen eingesetzt. Im zweiten Modus werden Sicherheitsdienste auf der Dienstebene angeboten. Zunächst muss eine L2CAP-Verbindung aufgebaut werden und festgestellt werden dass dieser Dienst auf dem Gerät erlaubt ist. So ist bei einem als vertrauenswürdig eingestuftem Gerät keine Authentifikation mehr erforderlich und eine Verbindungsanfrage wird akzeptiert. Der Modus 3 wird am häufigstem in der Praxis verwendet und ist für Sicherheitsdienste auf der Link-Ebene verantwortlich. Er liefert Grundschutz der für alle Anwendungen gleich ist. Zunächst ist eine Verbindung mittels des Link Managers erforderlich. In diesem Modus wird eine Authentifizierung durchgeführt und die Kommunikation wird verschlüsselt. Bei erstmaliger Kommunikation wird eine gemeinsame PIN vereinbart, die entweder in-band oder out-band gespeichert wird.

3.1 Sicherheitsmängel

Obwohl die Sicherheitsarchitektur und das Design der Protokolle von Bluetooth sehr viel besser sind als des IEEE 802.11 Standards bzw. WLAN, weist auch Bluetooth einige Schwächen und Angriffspunkte auf. Als eine Hauptschwachstelle ist der Einsatz von PINs. Die PIN ist die Basis aller Sicherheitsmaßnahmen. Von dieser hängt die Vertraulichkeit des beim Pairing generierten IK. Die Schwachstelle ist das wiederholte Eingeben der PIN, das sicherlich schnell lästig sein kann. So ist zu befürchten dass entweder nur vier stellige PINs verwendet werden oder dass sie fest auf dem Gerät gespeichert werden. Ein vierstelliger PIN-Code erlaubt nur 10.000 unterschiedliche PINs. Deshalb sollten Benutzer für Anwendungen mit sensiblen Daten eine mindestens 64 Bit PIN wählen.

4 Ausblick

Bei allen Schwächen die Bluetooth aufweist sollte man nicht vergessen dass Bluetooth zum Aufbau kabelloser Personal Area Networks entwickelt wurde. In solchen PANs werden in der Regel Daten innerhalb einer Reichweite von 5-10 Metern zwischen Geräten übertragen. Daher sind die Sicherheitsanforderungen dementsprechend relativ niedrig. Jedoch gilt Bluetooth als eine der meist genutzten Technologien zur Datenübermittlung, die immer weiter entwickelt wird. Die aktuellste Version ist Bluetooth 3.0 - Seattle Release mit der Daten mit 480 Mb/s transferiert werden können.

Literatur

- [Q1] Claudia Eckert: *IT-Sicherheit: Konzepte, Verfahren, Protokolle*
5. überarbeitete Auflage, R. Oldenbourg-Verlag, 2007.
- [Q2] www.bluetooth.com