Sicherheit bei Bluetooth

Dennis Siegert & Martin Gebel

Inhalt:

1.0 Einführung

2.0 Grundlagen
- 2.1 Frequenzband
- 2.2 Verbindungsarten & Reichweite
- 2.3 Die Komponenten
- 2.4 Die Gliederung in Profile
- 2.5 Die Verbindungsarten

3.0 Sicherheitsaspekte
- 3.1 Die Verbindungsaufnahme
- 3.2 Die Sichtbarkeitsmodi
- 3.3 Das Pairing
- 3.4 Die Sicherheitsbetriebsarten
- 3.5 Die Authentisierung
- 3.6 Die Verschlüsselung
- 3.7 Der Verschlüsselungsalgorithmus E0

4.0 Angriffe auf Bluetooth
- 4.1 Sicherheit der Stromchiffre E0
- 4.2 Man-in-the-middle-Angriff
- 4.3 Angriffe auf die Bluetooth-Implementierung
  - 4.3.1 Bluebugging
  - 4.3.2 Bluejacking
  - 4.3.3 Bluesnarfing (Snarf Attack)
  - 4.3.5 Backdoor Attack
- 4.4 Schutzmaßnahmen
- 4.5 Fazit

5.0 Ausblick

6.0 Quellenangaben

1.0 Einführung

1994 hatten die Ericsson-Ingenieure die Vision einer einfachen Funkübertragungstechnologie die preiswert, robust, schnell und energiesparend arbeiten sollte.
Da sich eine solche Vision nicht im Alleingang realisieren lässt, gründete die Ericsson Mobile Communications in Kooperation mit Intel Corporation, IBM Corporation, Toshiba Corporation, Nokia Mobile Phones, Agere Systems, Microsoft Corporation und Motorola Inc. die sogenannte Bluetooth SIG (Special Interest Group), die die Spezifikationen für Bluetooth festlegt.
Der SIG sind 136 Unternehmen angeschlossen, die sogenannten „Associates“. Diese lassen verschieden Ideen einfließen und können bei den neuen Standarts mitbestimmen.
Schließlich gibt es im Moment über 2500 Unternehmen die Bluetooth in ihre Produkte implementieren. Diese werden von der SIG als Adaptors bezeichnet. Ihre Zahl steigt ständig.
Der Name Bluetooth geht im übrigen auf den dänischen König Harald Blåtand (wörtlich „blauer Zahn“, Englisch: „Blue tooth“) zurück, der im zehnten Jahrhundert regierte. So wie Harald Dänemark und Norwegen vereinte, soll die drahtlose Bluetooth-Technologie heute unterschiedliche Geräte zusammenbringen.

Bezogen auf den aktuell verwendeten Standart (Version 1.1) bietet Bluetooth folgende Features:

– Frequenzband 2.400 – 2.4835 GHz im ISM-Band (Industial, Scientific, Medical)
– 79 Kanäle, je 1MHz breit
– Bis zu 1600 Kanalwechsel pro Sekunde
– Identifizierung der Geräte durch eindeutige 48 Bit große Adresse (ähnlich MAC)
– max. 0,1W Sendeleistung (~80 mal weniger als ein Handy)

Man unterscheidet 3 Klassen von Geräten, die nach ihrer Sendeleistung klassizifiert werden:

Leistungsklasse	Maximale Ausgangsleistung (Pmax)	Reichweite
1	100mW (20dBm)	~ 100m
2	2.5mw (4dBm)	~ 10m
3	1mW (0dBm)	~ 2m

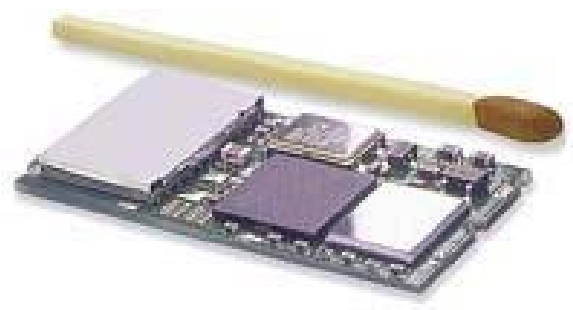


Abbildung: Typischer Chip der ersten Generation

2.0 Grundlagen

2.1 Frequenzband

Bluetooth arbeitet wie oben in der Übersicht dargestellt im 2,4-GHz-ISM-Frequenzband auf 79 Kanälen bei den Frequenzen f =(2402 + k) MHz, k = 0,...,78. Die Übertragung der GFSK-modulierten Datenpakete erfolgt zeitschlitzgesteuert (TDD) in Verbindung mit einem Frequenzsprungverfahren (FHSS). Dies dient zur Reduzierung der Empfindlichkeit gegenüber Störungen. Die Zeitschlitzlänge beträgt 625µs; daraus resultiert eine Frequenzwechselhäufigkeit von bis zu 1600 hops/s (für 1-slot-Pakete). Die Hopping-Sequenz ist pseudozufällig und wiederholt sich nach ca. 23,3 Stunden.

2.2 Verbindungsarten & Reichweite

Bluetooth unterstützt asynchrone verbindungslose (ACL-)Übertragung mit maximal 723,2 kbit/s in der einen und 57,6 kbit/s in der anderen Richtung (asymmetrisch) bzw. mit maximal 433,9 kbit/s in beide Richtungen (symmetrisch). Für Sprachübertragung stehen bei Bluetooth bis zu drei synchrone verbindungsorientierte (SCO-) Kanäle mit je 64 kbit/s zur Verfügung; die Sprachkodierung erfolgt entweder über PCM oder CVSD-Modulation.
Die Reichweite hängt von der Sendeleistung ab und reicht von bis zu 2 Metern bei Klasse3-Geräten (bis 1mW Sendeleistung) bis zu ca. 100 Metern bei Klasse1-Geräten mit bis zu 100mW Sendeleistung. Zur Senkung des Stromverbrauchs sind Spar-Modi (Sniff-, Park- und Hold-Mode) und Sendeleistungsregelung (Power Control) spezifiziert.

2.3 Die Komponenten

Generell besteht ein Bluetooth System aus drei Komponenten:
1. Bluetooth Radio: Sender, Empfänger und analoge Radioelektronik
2. Bluetooth Link Controller: Kontrolliert und steuert den Kommunikationsaufbau, Verbindungsverwaltung, Fehlerbehandlung, Identifikation und Zugriff
3. Bluetooth Link Manager: Bereitet die Daten auf und stellt die Kommunikation mit dem Endgerät sicher, in dem das Bluetooth-Modul verwendet wird.

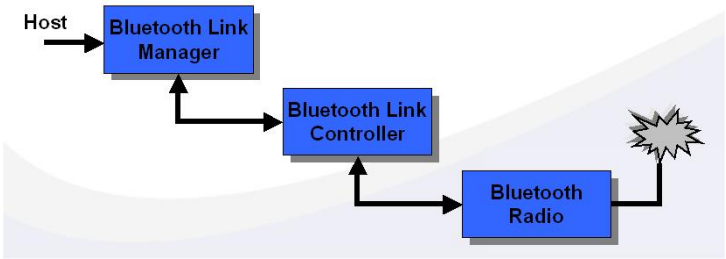


Abbildung: Die 3 Komponenten eines Bluetoothsystems

2.4 Die Gliederung in Profile

Die Interoperabilität zwischen Bluetooth-Geräten verschiedener Hersteller wird durch sogenannte Profile gewährleistet, die für bestimmte Anwendungsbereiche festgelegt sind. Wenn eine Bluetooth Verbindung aufgebaut wird, tauschen die Systeme ihre Profile aus und legen damit fest, welche Dienste sie für die jeweiligen anderen Partner zur Verfügung stellen können und welche Daten oder Befehle sie dazu benötigen. Das Headset Profil fordert beispielsweise von einem Bluetooth kompatiblen Mobiltelefon einen Audiokanal an und steuert über zusätzliche Datenkanäle die Lautstärkeregelung.

2.5 Die Verbindungsarten

Wenn sich mehr als zwei Geräte zu einer Point-to-Point Verbindung zusammenschließen, wobei ein Gerät steuert (Master) und das andere gehorcht (Slave), wird von einem Piconet gesprochen. Bis zu sieben Slaves können in einem Piconet aktiv sein. Zusätzlich können bis zu 255 Slaves im sogenannten Parkmodus im Piconet eingebucht sein. Diese parkenden Bluetooth-Komponenten können von sich aus keine Daten senden, synchronisieren sich aber laufend mit dem Master und können von diesem aus dem Parkmodus in den regulären Kommunikationsstatus aktiviert werden. In einem Piconet kommunizieren die verschiedenen Netzteilnehmer gleichzeitig miteinander, während hintereinander abgearbeiteter Datenaustausch mit verschiedenen Bluetooth Systemen als Multipoint Verbindungen bezeichnet werden. Viele Bluetooth Anwendungen, die als Profile bezeichnet werden, werden aus technischen Gründen den Piconet Modus nicht unterstützen: Bei der Faxübertragung müssen zum Beispiel in der Kommunikation enge Zeitfenster eingehalten werden, die beim gleichzeitigen Betrieb einer Piconet Applikation nicht garantiert werden können. Daher ist die Fax Übertragung eine ausschließliche Point-to-Point Verbindung. Mehrere Piconets mit sich überlappenden Bereichen werden als Scatternet bezeichnet. In jedem Piconet kann nur ein Master festgelegt werden, aber Slaves können in mehreren Netzen eingebucht sein.

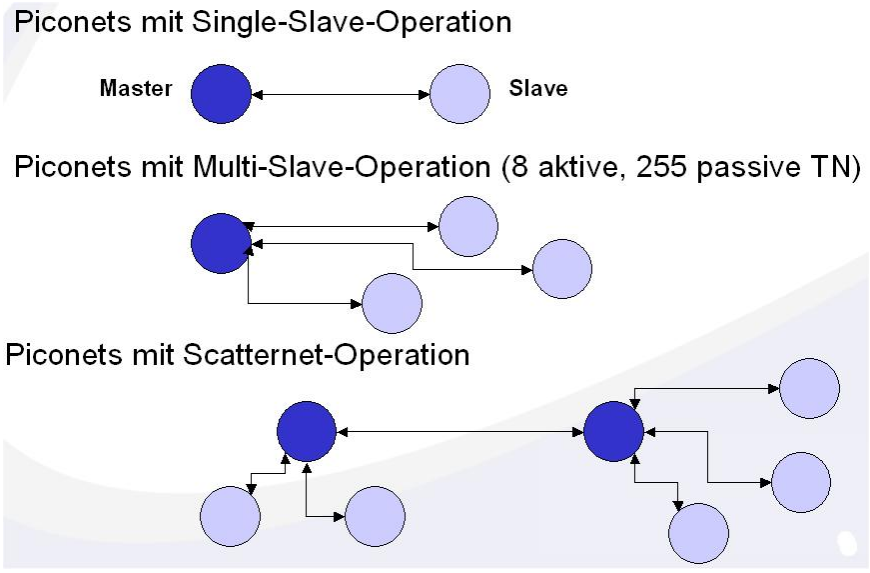


Abbildung: Die Verbindungsarten

3.0 Sicherheitsaspekte

3.1 Die Verbindungsaufnahme

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die so genannte Bluetooth Device Address.
Der Verbindungsaufbau erfolgt über Inquiry und Paging.

• **Inquiry:**
- Per Inquiry-Prozedur kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Nach einem Inquiry liegen alle Geräteadressen und Zeittakte der gefundenen kommunikationsbereiten Geräte vor.

• **Paging:**
- Durch eine Paging-Anforderung kann nun eine Kommunikationsverbindung zu einem dieser Geräte aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Für den Verbindungsaufbau wird die Sprungsequenz des Slaves verwendet, die so genannte Page-Hopping-Sequence. Während des Pagings sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave. Für die weitere Kommunikation wird anschließend die Sprungsequenz des Masters verwendet, die so genannte Channel-Hopping-Sequence.

3.2 Die Sichtbarkeitsmodi

Man unterscheidet bei Bluetooth in der Version 1.1 zwischen drei verschieden Modi in denen sich ein Bluetooth-Gerät befinden kann:

• **Discoverable Mode:**
- discoverable: Es wird auf Inquiry Anfragen gelauscht und immer geantwortet
- non-discoverbale: kein Inquiry Scan, direkte Anfragen werden aber beantwortet

• **Connectable Mode:**
- Connectable: Es wird ein Page Scan zur Annahme von Verbindungen durchgeführt.
- non-connectable: kein Page Scan

• **Pairing Mode:**
- pairable: Zur Authentifikation wird die PIN verwendet
- non-pairable: keine PIN Eingabe

Hierbei fällt gleich auf, dass es keinen Modus gibt in dem sich ein Gerät wirklich verstecken kann. Selbst wenn das Gerät nur im Discoverable-Mode läuft und dort auf keine Inquiry-Scans reagiert, kann man es zu einer Antwort zwingen, indem es direkt mit seiner Geräteadresse angesprochen werden kann.

3.3 Das Pairing

Wenn zwei Bluetooth-Geräte kryptographische Sicherheitsmechanismen nutzen wollen, müssen sie zuvor miteinander "gepaart" werden. In der Regel wird dabei ein nur für die Ver-bindung dieser beiden Geräte genutzter, 128 Bit langer Kombinationsschlüssel (Combination Key) erzeugt und in jedem Gerät für die zukünftige Nutzung als Verbindungsschlüssel gespeichert.
Bei der Erzeugung dieses Kombinationsschlüssels gehen die Geräteadressen und von beiden Geräten je eine Zufallszahl ein. Für die gesicherte Übertragung dieser Zufallszahlen wird ein Initialisierungsschlüssel verwendet, der sich aus einer weiteren (öffentlichen) Zufallszahl, einer Geräteadresse und einer PIN berechnet. Dazu muss in beide Geräte die gleiche PIN eingegeben werden. Die PIN kann 1 bis 16 byte lang sein und ist entweder durch den Nutzer konfigurierbar oder fest voreingestellt.
Verfügt eines der Geräte über einefeste PIN, so muss diese in das andere Gerät eingegeben werden. Zwei Geräte mit fest vor-eingestellter PIN können nicht gepaart werden.

3.4 Die Sicherheitsbetriebsarten

Die Spezifikation beschreibt im 3 Sicherheitsmodi:

Sicherheitsmodus 1: Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheits-mechanismen, reagiert aber auf Authentisierungsanfragen anderer Geräte.
Sicherheitsmodus 2: Auswahl und Nutzung von Sicherheitsmechanismen werden abhängig vom Bluetooth-Gerät ("trusted" oder "non-trusted") und vom Dienst auf Anwendungsebene festgelegt. Das Gerät leitet erst dann Sicherheitsprozeduren ein, wenn es eine Aufforderung zum Verbindungsaufbau erhalten hat.
Sicherheitsmodus 3: Es ist generell eine Authentisierung beim Verbindungsaufbau erforderlich; die Verschlüsselung der zu übertragenden Daten ist optional.

3.5 Die Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet.
Das Challenge-Response-Verfahren läuft wie folgt ab:
Das Zielsystem gibt eine zufällig generierte Parole (Challenge) aus. Der Nutzer, der sich gegenüber dem Zielsystem authentisieren möchte, antwortete mit einem passenden Gegenstück (Response). Dieses Gegenstück wird auf Basis der Challenge von Software errechnet. Das Verfahren ist der Verwendung herkömmlicher Passwörter weit überlegen, da jede Response nur für einen Zugriff gilt und Abhören einem Angreifer nicht hilft.
Es wird bei Bluetooth grundsätzlich einseitige Authentisierung verwendet, das heißt ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.
Die Authentisierung läuft wie folgt ab: Der Verifier sendet eine Zufallszahl an den Claimant. Dieser beweist, dass er das gemeinsame Geheimnis (den Verbindungsschlüssel) kennt, indem er unter Benutzung des Verbindungsschlüssels aus der Zufallszahl und seiner eigenen Geräteadresse eine 32 Bit lange Antwort berechnet und zum Verifier zurücksendet.

(Dabei berechnet er gleichzeitig aus diesen Daten einen 96 Bit langen sog. Authenticated Cipher Offset, der geheim gehalten wird und bei Bedarf - als ein Teil - bei der Erzeugung eines Verschlüsselungsschlüssels verwendet wird.) Der Verifier überprüft die Antwort, indem er die gleiche Berechnung durchführt. Sind die Ergebnisse identisch, ist der Claimant authentisiert.

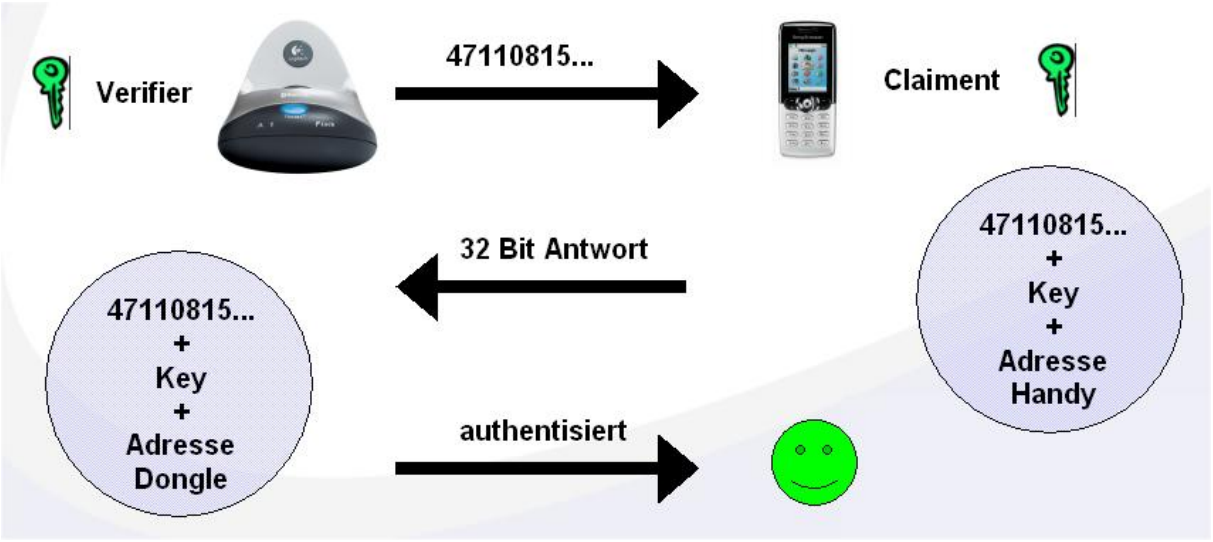


Abbildung: Die Authentisierung

3.6 Die Verschlüsselung

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem Anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master, als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat. Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels. Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl an den Slave sendet. Der Chiffrierschlüssel berechnet sich aus dem Verbindungsschlüssel, einem Cipher Offset und der Zufallszahl.
Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei Punkt-zu-Punkt-Verschlüsselung wird der Authenticated Cipher Offset des Authentisierungsprotokolls als Cipher Offset verwendet. Bei Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Masters als Cipher Offset genutzt. Außerdem muss der Verbindungsschlüssel durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird.
Zum Verschlüsseln wird eine Stromchiffre (im Standard mit E0 bezeichnet) eingesetzt. Für jedes Datenpaket wird dabei ein neuer Initialisierungsvektor ("Spruchschlüssel") aus der Geräteadresse sowie dem Zeittakt des Masters berechnet. Verschlüsselt sind die Daten nur während des Transports per Funk. Vor der Aussendung bzw. nach Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor; es handelt sich also nicht um Ende-zu-Ende-Verschlüsselung (d. h. Verschlüsselung der Daten von der Eingabe in Endgerät A bis zur Ausgabe/Bearbeitung in Endgerät B).

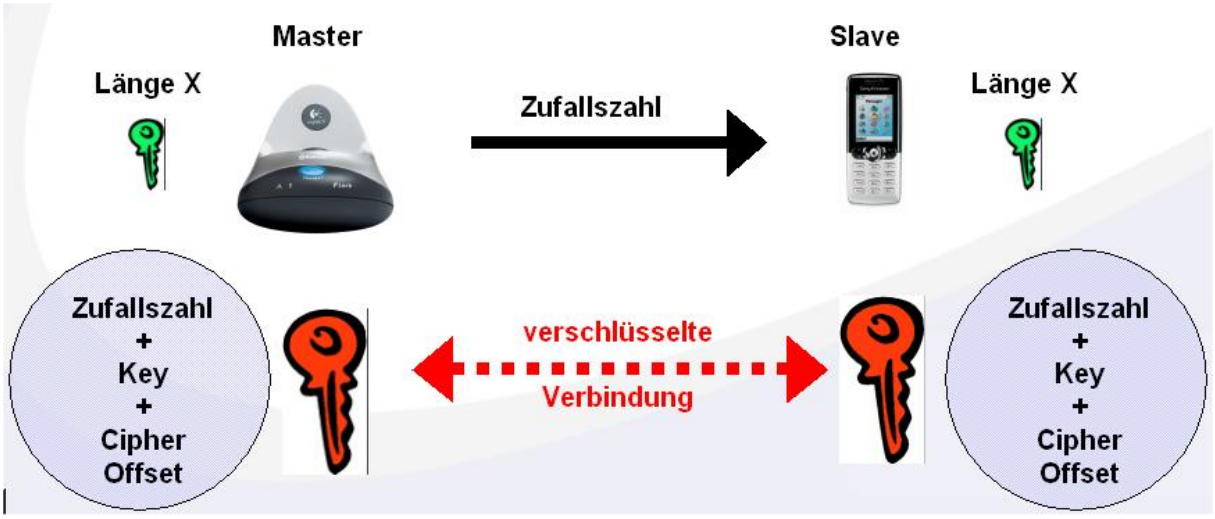


Abbildung: Die Verschlüsselung

3.7 Der Verschlüsselungsalgorithmus E0

Während bei den Blockverschlüsselungsverfahren eine Nachricht in Blöcke fester Länge unterteilt und dann verschlüsselt wird, erfolgt die Verschlüsselung mit den Stromverschlüsselungsverfahren bitweise, und zwar durch bitweise Addition der Nachricht mit einer Pseudozufallsfolge, die auch Keystream genannt wird.
Vorteile:

- → schnell
- → einfach implementierbar
- → Skalierbarkeit der Länge des geheimen Schlüssels

Das Funktionsprinzip einer Stromchiffre kann wie folgt kurz beschrieben werden: Durch einen Zufallsfolgengenerator wird eine pseudozufällige Folge Z generiert, die zur Verschlüsselung einer zu übertragenden Nachrichtenfolge X mittels einer eindeutig umkehrbaren Abbildung (z.B. der XOR-Operation) verwendet wird. Der Zufallsfolgengenerator wird dazu mit einem geheimen Schlüssel K initialisiert.
Die daraus entstandene Nachrichtenfolge Y wird über einen unsicheren Kanal zum Empfänger übertragen. Auf Empfängerseite wird der gleiche Generator zur Erzeugung der Zufallsfolge Z zur Entschlüsselung der Nachricht Y verwendet. Der Generator auf der Empfängerseite wird ebenfalls mit dem geheimen Schlüssel K initialisiert, welcher über einen sicheren Kanal vom Sender zum Empfänger übertragen wird.

Bei Bluetooth erfolgt die Implementierung wie folgt:
Eine vorangegangene erfolgreiche Authentifikation wird voraus gesetzt. Anschließend arbeitet die Stromchiffre E0 mit einem bis zu 128 Bit langen Verschlüsselungsschlüssel, der mit dem Algorithmus aus dem Link Key, dem Zufallswert und dem 96 Bit langen, bei der Authentifikation bestimmten Authenticated Ciphering Offset berechnet wird.
Die Vereinbarung des Verschlüsselungsmodes erfolgt durch das Kommando durch den Master. Dieses Kommando muss vom Slave bestätigt werden. Zur Aushandlung der Schlüssellänge sendet das Master-Device die gewünschte Schlüssellänge an den Slave. Antwortet der Slave, ist diese Schlüssellänge vereinbart.

Anderenfalls schickt der Master einen Schlüssel mit der nächst kleineren Schlüssellänge, bis die von der Anwendung festgelegte Mindestschlüssellänge erreicht ist. Akzeptiert der Slave auch diese nicht, kommt die gewünschte sichere Verbindung nicht zu Stande. Dadurch wird verhindert, dass ein Bluetooth-Device durch Angabe einer extrem klein gewählten maximalen Schlüssellänge die Etablierung einer unsicheren Verbindung bewirken kann.
Nach Vereinbarung der Schlüssellänge wird die Verschlüsselung vom Master gestartet und der Verschlüsselungsschlüssel mit dem Algorithmus aus dem Link Key und einer Zufallszahl erzeugt.

4.0 Sicherheitsaspekte

4.1 Sicherheit der Stromchiffre E0

Der Schlüsselstrom kann berechnet werden, indem man das abgehörte Chiffrat mit den Klartext-Daten XOR-verknüpft. Obwohl E0 Schlüssellängen von 8-128 Bit akzeptiert, haben Fluhrer und Lucks gezeigt, dass die erreichbare Sicherheit je nach Stärke des Angreifers 84 Bit nicht übersteigt, bei 2^{43} Bit bekanntem Schlüsselstrom schrumpft sie sogar 73 Bit. Es ist zwar unmöglich 2^{43} Bit (Terabyte) Klartext-Daten am Stück zu beschaffen, bei 132 Bit (17 Byte) sieht das allerdings anders aus, bedenkt man, wie viele TCP und IP-Header mit weitgehend bekanntem Inhalt in einem Bluetooth-basiertem IP-Netzwerk durch die Luft schwirren, ist es durchaus realistisch, diese Menge zu erraten. Die maximal effektive Schlüssellänge sinkt auf 84 Bit, selbst wenn nominal mit 128 Bit verschlüsselt wird. Das bewegt sich bereits in der Größenordnung, die nach Expertenmeinung (z. B. National Security Agency) gerade gebrochen werden kann

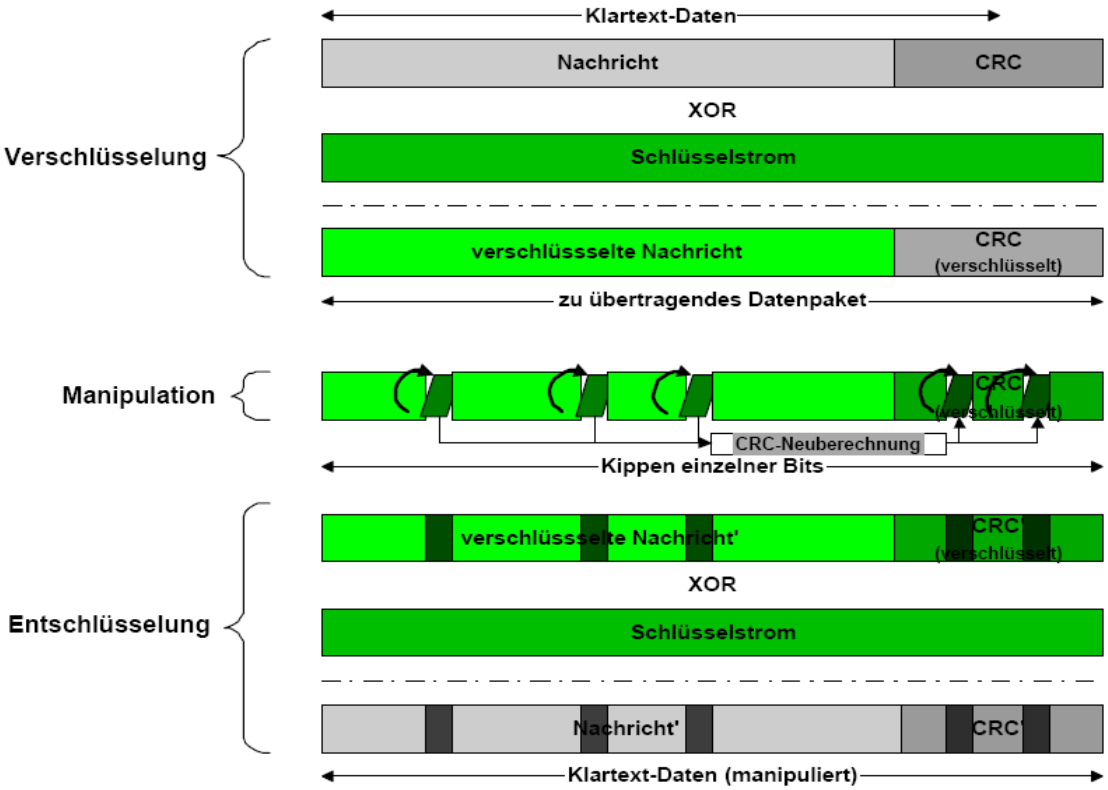


Abbildung: Angriff auf E0

4.2 Man-in-the-middle-Angriff

Selbst wenn eine starke Verschlüsselung eingesetzt wird, können übertragene Daten manipuliert werden. Bluetooth schützt jedes Datenpaket noch vor der Verschlüsselung durch Anfügen einer 16-Bit-Prüfsumme (CRC) gegen Übertragungsfehler. Danach XOR-verknüpft es das gesamte Paket inklusive CRC, aber ohne Header, mit dem Schlüsselstrom von E0. So sollte auch eine vorsätzliche Manipulation der Nutzdaten unmöglich sein. Das Zusammenspiel von

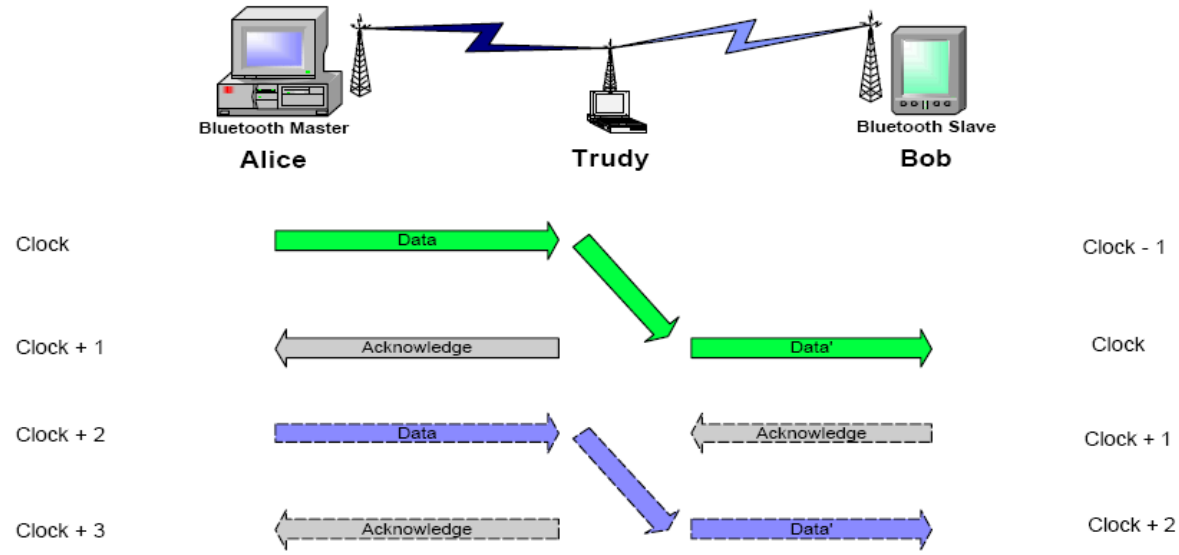
- linearer CRC angefügt
- und Verschlüsselung durch XOR-Verknüpfung mit Schlüsselstrom

ermöglichen gezielt einzelne Bits im verschlüsselten Datenpaket zu kippen und den verschlüsselten CRC und den verschlüsselten CRC derart zu beeinflussen, dass die Nutzdatenmanipulation nicht auffällt.

So trivial wie es auf den ersten Blick erscheint ist es jedoch nicht, spielt der Angreifer das manipulierte Paket einfach über das Original, so entsteht nur Datenmüll und der Sender muss das Paket erneut schicken, aber aufgrund der Eigenschaften von Stromchiffren ist es möglich, die über einen „Man-in-the-middle“-Angriff abgefangenen Daten gezielt zu verändern, wenn der verschlüsselte Klartext teilweise bekannt ist (IP-Header manipulierbar). Der Inititalisierungsvektor ändert sich bei jedem übertragenen Paket, so dass ein Angriff per einfachem Wiedereinspielen fehlschlägt.

Allerdings gibt es dennoch einige Ansätze, um das Wiedereinspielen zu ermöglichen. Das Ziel des Angreifers liegt dabei darin, eine Situation zu schaffen, in der er als „Man-In-The-Middle“ ein manipuliertes Datenpaket so absenden kann, dass es nicht durch Kollision mit dem Original verloren geht und vom Empfänger als vermeintliches Originalpaket akzeptiert wird.

- 1. Ansatz: zeitliche Entkopplung von originalem und manipuliertem Paket. Das lässt sich per Umweg über die Sendefrequenz erreichen, denn Bluetooth wechselt diese zur Störungsvermeidung zwischen den Paketen, sendet der Angreifer das manipulierte Paket auf einer anderen Fequenz aus, als auf der er es empfangen hat, bleibt die Kollision aus. Kommunizieren zwei Geräte miteinander, so synchronisieren sie zuerst ihre Clocks aufeinander, so dass sie frequenzsynchron senden und empfangen können. Ein Angreifer kann beim Verbindungsaufbau einen Periodenversatz zwischen den Kommunikationspartnern erzeugen.



Abildung: Attacke durch Periodenversatz (unidirektionale Kommunikation: Alice sendet Daten an Bob):

Der Angreifer führt einen kleinen Versatz (Größenordnung Sekunden) beim Verbindungsaufbau zwischen Sender und Empfänger ein und hat somit ausreichend Zeit, um ein Datenpaket zu manipulieren. Trudy muss sich noch darum kümmern, dass Alice für jedes abgeschickte Paket auch eine Empfangsbestätigung bekommt, das erreicht Trudy mit einem gesetzten ACK-Flag im Header des nächsten Pakets an Alice. Steht kein Paket von Bob an Alice an, generiert Trudy einfach eines mit leerem Datenteil, leider kann Trudy diese Pakete problemlos fälschen, da Bluetooth den Paket-Header nicht verschlüsselt. Die echten ACK-Pakete von Bob ignoriert Trudy einfach, Alice hört diese wegen des Frequenzversatzes nicht. Die Randbedingung: der Angreifer muss sich bereits in den Verbindungsaufbau einmischen können, um den Periodenversatz zu erzeugen.

4.3 Angriffe auf die Bluetooth-Implementierung

4.3.1 Bluebugging

Hacker verschaffen sich Zugriff auf Mobiltelefon-Befehle, ohne den Anwender des Telefons darüber in Kenntnis zu setzen.

Voraussetzungen:
BT aktiviert, Reichweite 10 m, Laptop, Software

Ein Handy mit geöffneter BT-Schnittstelle meldet diesen Status an alle in der Nähe befindlichen Geräte und ist deshalb sehr einfach ausfindig zu machen. Die Attacke erstellt eine serielle Verbindung auf dem Gerät und gibt somit vollen Zugriff auf alle AT-Kommandos. Der Angreifer kann Anrufe ausführen, SMS lesen/senden und Kontakte im Adressbuch erstellen/ändern.

4.3.2 Bluejacking

Anwender können anonym Visitenkarten verschicken, meist werden aber lustige Sprüche oder Flirt-Sprüche verschickt . Bluejacking ist kein Hacking im eigentlichen Sinn, da Daten in den Geräten nicht eingesehen, geändert oder gelöscht werden können

Voraussetzungen: BT aktiviert, Reichweite 10 m

Insgesamt lästig, aber harmlos.

4.3.3 Bluesnarfing (Snarf Attack)

Ein Hacker kann auf Daten zugreifen, die im Mobiltelefon gespeichert sind, ohne den Anwender des Telefons darüber in Kenntnis zu setzen

Voraussetzungen:
Reichweite 10 m, Laptop, Software (OS Linux)
- wenn das Telefon auf „nicht erkennbar“ eingestellt wird, ist das Aufspüren und Anzapfen des Gerätes um einiges schwieriger

Ein Zugriff auf das Adressbuch, Bilder, Kalender und IMEI wird so ermöglicht. Neben Mobiltelefonen sind auch PDAs und Laptops betroffen

4.3.5 Backdoor Attack

Ein Hacker erreicht ein Pairing mit einem Gerät, taucht aber nicht in der Liste der gepairten Geräte des Anwenders auf. Durch diese Verbindung kann er nicht nur auf die kompletten Daten im Gerät, sondern auch auf alle Modems und WAP/GPRS zugreifen.

Voraussetzungen:
Reichweite 10 m, Laptop, Software

Die Angriffe (außer Bluejacking) auf die BT-Implementierung sind nicht bei allen Mobiltelefonen ausführbar, sondern nur bei speziellen Geräten mit spezieller (nicht aktueller) Firmware. Die Möglichkeit des Hackings liegt nicht dem BT-Protokoll selbst zugrunde, sondern in der nachlässigen Implementierung der BT-Funktionen seitens der Hersteller.

Betroffen sind vor allem

Ericsson	T68
Sony Ericsson	R520m, T68i, T610, Z1010, Z600
Nokia	6310, 6310i, 7650, 8910, 8910i
Motorola	V600, V80

4.4 Schutzmaßnahmen

- Bluetooth-Geräte sollten möglichst wenig „offen“ konfiguriert werden
- Unnötige Dienste sollten deaktiviert werden
- Die Sendeleistung so niedrig wie möglich eingestellt werden
- Wenn ein Gerät Authentisierung verwendet, muss es so konfiguriert werden, dass es nach erfolgreicher Authentisierung immer auch eine starke Verschlüsselung verwendet
- Wenn ein Gerät Verschlüsselung der Kommunikation erzwingt, muss die Schlüssellänge mindestens 64 Bit betragen

4.5 Fazit

Ohne unabhängige Prüfungen erfährt der User nicht, ob in seinem Bluetooth-Gerät der Zufallszahlengenerator sorgfältig interpretiert wurde, ob die Authentifizierung tatsächlich beiderseitig stattfindet oder ob die Verschlüsselung mit einer akzeptablen Mindestschlüssellänge stattfindet. Allerdings muss man bedenken, das Bluetooth hauptsächlich dazu entwickelt wurde, damit Headsets, Drucker und dergleichen kommunizieren können. Also war und ist ein Einsatz für hochsensible Anwendungen nicht vorgesehen.

5.0 Ausblick

Neben der Verabschiedung der neuen Bluetooth-Spezifikation 2.0 + EDR veröffentlichte die Bluetooth Special Interest Group weitere, durchaus ambitionierte Ziele für die nächsten Jahre.
Der erste Teil ist die DER: Sie soll kommenden Bluetooth-Geräten bis zu dreifache Brutto-Übertragungsraten gegenüber aktuellen Geräten bescheren. Bisher funken die Geräte gemäß Bluetooth 1.1 oder 1.2 mit 1 MBit/s brutto, künftig sollen es bis zu 3 MBit/s sein.
Da wesentliche Eckwerte erhalten bleiben, kommt auch Bluetooth 2.0 + EDR mit geringem Verwaltungsaufwand aus und liefert daher auch in der Praxis bis zu dreifache Durchsatzraten. Bisher sind unter guten Bedingungen rund 80 kByte/s möglich. EDR-Geräte werden bis zu 240 kByte/s befördern und noch sparsamer mit Energie umgehen, weil deren schnelle Transceiver zwei- bis dreimal so schnell mit der Übertragung der gleichen Datenmenge fertig sind wie ihre Vorläufer.
Der schon jetzt niedrige Energieverbrauch soll noch weiter sinken, sodass man Bluetooth-Sensoren entwickeln kann, die mehrere Jahre mit einer einzigen Batterie laufen. Parallel dazu steigt die Piconetz-Kapazität von acht auf 256 Geräte, sodass ein Master nicht wie bisher nur sieben Slaves, sondern bis zu 255 Slaves steuern kann.
Die Ingenieure hoffen, dass diese beiden Schachzüge Bluetooth den Weg zur Heim- und Industrieautomation ebnen. Damit werden Handys denkbar, die die heimische Alarmanlage bedienen können, oder auch Szenarien, in denen ein PC alle Stationen einer Fertigungsstraße überwacht, indem er deren Bluetooth-Sensoren drahtlos abfragt.
Im Bereich Sicherheit wollen die Entwickler einen „stark verbesserten Non-Discoverable-Modus“ einführen. Man kann Bluetooth-Geräten ja bereits jetzt „tarnen“, indem man den Discovery Modus abschaltet. Dann antworten sie nicht auf

Discovery-Anfragen. Sie reagieren aber durchaus, wenn man sie über ihre Bluetooth-Device-Adresse anspricht (s.o.), sie sind also anfällig gegenüber Brute-Force-Attacken, in denen Angreifer ganze Adressräume stur nacheinander abklappern, in der Hoffnung früher oder später schon irgendein Ziel zu finden. Der nun geplante Non Discoverable Mode soll dann selbst solchen und noch aufwendigeren Attacken jahrelang standhalten und vor unerwünschten Entdeckern schützen.

6.0 Quellen

- Bluetooth, Die Referenz für den neuen Bluetooth-Standart von Muller, Nathan, MITP-Verlag, 2001

- www.bluetooth.org

- c't 25/04, Seite 36: Nahfunk-Verbeserungen

- c't 11/03, Seite 186ff.: Blauzahnlücken

- LOGITECH Deutschland, internes Informationsmaterial

- Bundesministerium für Sicherheit – Bluetooth, Gefährdungen und Sicherheitsmaßnahmen
  http:://www.bsi.de

- Neue Sicherheitsaspekte bei Bluetooth
  http://www.datensicherheit.nrw.de/Daten/ws051203/Vortraege/Schmidt_1.pdf

- Bluetooth - Sicherheitsarchitektur und Angriffspunkte
  www.datensicherheit.nrw.de/ Daten/ws051203/Vortraege/Loehlein.pdf

- Martin Herfurts CeBIT snarfing expedition
  http://trifinite.org/trifinite_stuff_bluebug.html

- Security Briefs
  http://www.thebunker.net/security/bluetooth.htm

- Bluejacking hits the mainstream
  http://news.zdnet.co.uk/communications/wireless/0,3948,39117662,00.htm

- heise Security - Informationen aus dem BSI
  http://www.heise.de/security/artikel/40198

- Wired 12.12: They've got your number
  http://wired.com/wired/archive/12.12/phreakers.html?pg=2&topic=phreakers

- S.R. Fluher und S. Lucks: Analysis Of the E0 Encryption System
  http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz