Bundesamt
für Sicherheit in der
Informationstechnik

Bluetooth

Gefährdungen und Sicherheitsmaßnahmen

Diese BSI-Broschüre richtet sich an Sicherheitsbeauftragte und an Endbenutzer von Bluetooth-Geräten. Es werden mögliche Gefährdungen bei der Nutzung von Bluetooth beschrieben und geeignete Schutzmaßnahmen aufgezeigt.

Bundesamt für Sicherheit in der Informationstechnik

Projektgruppe "Local Wireless Communication"

Postfach 20 03 63

53133 Bonn

Tel.: +49 (0) 1888 9582-0

E-Mail: bluetooth.lwc@bsi.bund.de

Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Grundlagen der Bluetooth-Spezifikation

Bluetooth ist ein offener Industriestandard (vgl. IEEE 802.15.1-2002 [1]) für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking).

Die Entwicklung von Bluetooth geht auf eine Initiative der so genannten Bluetooth Special Interest Group (SIG) [2] im Jahre 1998 zurück, der heute über 2.500 Hersteller angehören. Die derzeit aktuelle Version der Spezifikation ist V1.1 [3]; es sind aber auch noch zahlreiche Geräte im Einsatz, die auf der Vorgängerversion 1.0b basieren.

1.1 Technische Grundlagen

Bluetooth arbeitet 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.

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 10 Metern bei Klasse3-Geräten (bis 1mW Sendeleistung) bis zu ca. 100 Metern bei Klasse1-Geräten mit bis zu 100 mW Sendeleistung. Zur Senkung des Stromverbrauchs sind Spar-Modi (Sniff-, Park- und Hold-Mode) und Sendeleistungsregelung (Power Control) spezifiziert.

1.2 Protokollarchitektur

Neben den hardwarenahen Protokollen (Funktechnik und Basisband) definiert die Spezifikation [3] für das Verbindungsmanagement eine Link-Schicht, die neben Fehlerkorrekturverfahren auch kryptographische Sicherheitsmechanismen bereitstellt. Zusätzlich verfügt sie über eine Host-Controller-Schnittstelle sowie diverse weitere Protokolle für unterschiedliche Applikationen. Eine ausführliche Beschreibung des Bluetooth Protokollstacks findet man in der Literatur (z. B. in [4]). Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, hat die SIG so genannte Anwendungs-Profile definiert. Neben grundlegenden Profilen wie zum Beispiel dem Generic Access Profile, dem Serial Port Profile oder dem Generic Object Exchange Profile gibt es beispielsweise ein Headset Profile, ein LAN Access Profile, ein PAN (Personal Area Networking) Profile usw.

1.3 Verbindungsaufbau und Netztopologien

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.

Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten unterstützt Bluetooth auch Punkt-zu-Mehrpunkt-Verbindungen. Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem so genannten Piconet als Slaves im Park-Mode mit einem Master vernetzt sein. Zusätzlich können bis zu 7 Slaves gleichzeitig aktiv mit dem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel-Hopping-Sequence und dem Zeittakt des Masters. Prinzipiell sieht Bluetooth sogar die Möglichkeit einer Vernetzung von bis zu zehn Piconets zu einem so genannten Scatternet vor. In der Praxis kommen solche komplexen Netztopologien aber zurzeit noch selten vor.

1.4 Kryptographische Sicherheitsmechanismen

Da Bluetooth ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass "unberechtigte" bluetooth-fähige Geräte die Bluetooth-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Die in der Bluetooth-Spezifikation vorgesehenen kryptographischen Sicherheitsmechanismen haben die Ausschaltung dieser zwei Bedrohungen zum Ziel. Neben nicht-kryptographischen (Korrektur-)Verfahren zum Schutz gegen Übertragungsfehler sieht die Spezifikation kryptographische Authentisierungs- und Verschlüsselungs-Algorithmen vor. Diese sind bereits auf Chip-Ebene implementiert und stehen auf der Link-Schicht einheitlich zur Verfügung.

Basis aller eingesetzten kryptographischen Verfahren sind Verbindungsschlüssel (Link Keys), die jeweils zwischen zwei Bluetooth-Geräten während der so genannten Paarung vereinbart werden.

Paarung (Pairing) und Verbindungsschlüssel

Wenn zwei Bluetooth-Geräte kryptographische Sicherheitsmechanismen nutzen wollen, müssen sie zuvor miteinander "gepaart" werden. In der Regel wird dabei ein nur für die Verbindung 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 eine feste PIN, so muss diese in das andere Gerät eingegeben werden. Zwei Geräte mit fest voreingestellter PIN können nicht gepaart werden.

Neben den Kombinationsschlüsseln erlaubt der Standard weitere Möglichkeiten für Verbindungsschlüssel:

- Geräteschlüssel (Unit Keys) können als Verbindungsschlüssel genutzt werden. Der Geräteschlüssel wird bei der erstmaligen Verwendung eines Bluetooth-Gerätes erzeugt und normalerweise nicht mehr geändert. Geräteschlüssel werden beispielsweise verwendet, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt oder ein Gerät einer großen Gruppe von Nutzern zugänglich sein soll.
- Master-Schlüssel (Master Keys) können für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, wenn ein Master mehrere Geräte unter Verwendung desselben Chiffrierschlüssels erreichen will. Master-Schlüssel werden nur bei Punkt-zu-Mehrpunkt Verbindungen eingesetzt und über die aktuellen Verbindungsschlüssel gesichert vom Master an die Slaves übertragen.

Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird 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.

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).

1.5 Sicherheitsbetriebsarten

Die Spezifikation beschreibt im Generic Access Profile 3 Sicherheitsmodi:

- **Sicherheitsmodus 1**: Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheitsmechanismen, 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.

Zusätzlich sind für die Erkennbarkeit von Bluetooth-Geräten beim Inquiry die Modi "non-discoverable" (Gerät antwortet nicht auf Inquiry) bzw. "limited discoverable" und "general discoverable" spezifiziert. Weiterhin gibt es die Betriebsmodi "non-connectable" (keine Reaktion auf Paging-Anforderungen) bzw. "connectable" sowie "non-pairable" (keine Paarung möglich) und "pairable".

2 Gefährdungen bei der Nutzung von Bluetooth

Zu all den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (vgl. [5]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

2.1 Schwächen im Sicherheitskonzept

Verschlüsselung ist nicht grundsätzlich vorgeschrieben

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der übertragenen Daten optional und muss von den Anwendungen explizit beantragt werden.

Unsichere Voreinstellungen sind nicht grundsätzlich ausgeschlossen

Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert: Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind häufig abgeschaltet und PINs auf "0000" eingestellt. Wenn Geräte keine Eingabemöglichkeit besitzen (z. B. Headsets), ist eine Änderung der voreingestellten Werte gar nicht oder nur schwer möglich.

Schwache PINs können erraten werden

Wird bei der Gerätepaarung eine schwache PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss der Angreifer nur die Paarung und die folgende Authentisierung abhören. Anhand der Aufzeichnungen der abgehörten Protokolle kann der Angreifer überprüfen, ob die PIN von ihm korrekt geraten wurde. Auf diese Weise ist es möglich, kurze oder triviale (z. B. "1234567890") PINs zu ermitteln.

Als sicherheitskritisch anzusehen ist, dass PINs als einzige geheime Parameter bei der Verbindungsschlüsselerzeugung eingehen. Erfahrungsgemäß lassen sich hier schwache - weit verbreitete - Nutzergewohnheiten nur schwer durchbrechen.

Geräteschlüssel sind unsicher

Werden Geräteschlüssel von einem Gerät als Verbindungsschlüssel verwendet, so wird für jede Verbindung mit diesem Gerät immer der gleiche Schlüssel benutzt. Gelingt es dem

Angreifer eine Verbindung mit diesem Gerät aufzubauen, ist er anschließend in der Lage, sich für dieses Gerät auszugeben oder jede Kommunikation mit diesem Gerät abzuhören.

Schwache Integritätssicherung

Zur Integritätssicherung wird ein Cyclic Redundancy Check (CRC, codierungstheoretisches Verfahren zur Erkennung von Übertragungsfehlern) verwendet. Dadurch werden zwar zufällige Störungen bei der Übertragung von Datenpaketen mit hoher Wahrscheinlichkeit erkannt, aber gegen eine absichtliche Manipulation von Datenpaketen bieten CRC-Verfahren keinen ausreichenden Schutz.

Qualität des Zufallsgenerators

Zur Zufallserzeugung sind im Bluetooth-Standard keine Mechanismen festgelegt worden. Erfahrungsgemäß ist damit zu rechnen, dass die Güte der Zufallsgeneratoren hersteller- und implementierungsabhängig stark variiert.

2.2 Man-in-the-Middle-Angriffe

Ein weiteres Sicherheitsproblem von Bluetooth besteht darin, dass in bestimmten Konfigurationen so genannte "Man-in-the-Middle"-Angriffe möglich sind [6].

Dabei schiebt sich ein Angreifer, der (unberechtigt) Zugriff auf ein Bluetooth-Gerät erhalten will, "mitten zwischen" zwei berechtigte Geräte. Anschließend kommunizieren die beiden Geräte über den Angreifer miteinander, der die Datenpakete abfängt und manipulieren kann. Folgende Szenarien sind denkbar:

- Der Angreifer baut aktiv eine Verbindung zu beiden Geräten auf.

  Der Angreifer verbindet sich mit beiden Geräten und gibt dabei vor, jeweils das andere Gerät zu sein. Sofern sich das Gerät des Angreifers gegenüber einem Gerät authentisieren muss, reicht es die Authentisierungsanfrage an das andere Gerät weiter und sendet die Antwort zurück. Anschließend kann der Angreifer mit dem Gerät beliebig interagieren. Als Voraussetzung für die erfolgreiche Durchführung dieses Angriffs müssen beide Geräte "connectable" sein (vgl. 1.5).

- Der Angreifer schaltet sich ein, während die Geräte eine Verbindung aufbauen.

  Während des Verbindungsaufbaus müssen sich die Geräte auf die Sprungsequenz synchronisieren. Der Angreifer kann diese Synchronisation verhindern, so dass beide Geräte zwar die gleiche Sequenz, aber verschiedene Offsets in der Sequenz verwenden.

2.3 Probleme bei der Verschlüsselung

Die von Bluetooth optional verwendete Verschlüsselung hat einige Schwächen:

- Sicherheit der Stromchiffre E0

  Obwohl E0 Schlüssellängen von 1-16 Bytes (8-128 Bit) akzeptiert, haben Fluhrer und Lucks gezeigt, dass die erreichbare Sicherheit je nach Stärke des Angreifers 73 bzw. 84 Bit nicht übersteigt [7].

- Der Initialisierungsvektor ist nicht vom vollständigen Zeittakt abhängig.

  Jedes übertragene Datenpaket wird unter Verwendung eines neuen Initialisierungsvektors verschlüsselt. Dieser errechnet sich unter anderem aus dem Zeittakt des Masters. Es wird allerdings das höchstwertige Bit des Zeittaktes "vergessen"; so sind selbst bei eingesetzter Verschlüsselung Man-in-the-Middle-Angriffe (vgl. 2.2) möglich.

- Verschlüsselte Daten können manipuliert werden.

  Selbst wenn eine starke Verschlüsselung eingesetzt wird, können übertragene Daten manipuliert werden. Aufgrund der Eigenschaften von Stromchiffren ist es möglich, die über einen "Man-in-the-Middle"-Angriff (vgl. 2.2) abgefangenen Daten gezielt zu verändern, wenn der verschlüsselte Klartext teilweise bekannt ist. So ist es beispielsweise möglich, IP-Header gezielt zu manipulieren.

2.4 Unkontrollierte Ausbreitung der Funkwellen

Der Funkverkehr von Bluetooth-Verbindungen kann mit Hilfe von Bluetooth-Protokollanalysatoren passiv mitempfangen und aufgezeichnet werden. Die Synchronisation auf die Frequency-Hopping-Sequenz gelingt bei Kenntnis der Geräteadressen auch dann, wenn sich die Geräte im "Non-discoverable"-Modus befinden. Alle Schichten des Bluetooth-Protokoll-Stacks können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten (Payload) ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen Bluetooth-Signals kann ein solcher "Lauschangriff" auch noch in einer gegenüber der Funktionalitätsreichweite größeren Entfernung durchgeführt werden. Eine Sendeleistungsregelung ist optional und wird nicht von jedem Bluetooth-Gerät unterstützt.

In der Literatur zum Thema findet man gelegentlich die Behauptung, dass allein die Verwendung des Frequenzsprungverfahrens eine unberechtigte Teilnahme bzw. den Empfang und das Abhören von Bluetooth-Verbindungen wesentlich erschwere - für einen ausreichend informierten Angreifer stellt dies allein jedoch kein ernsthaftes Hindernis dar. Der Grund für die Verwendung eines Frequenzsprungverfahrens liegt darin, Übertragungsfehler aufgrund von Störungen durch den Betrieb anderer Geräte (z. B. drahtlose LANs), die dasselbe Frequenzband nutzen, klein zu halten und somit eine gute Verfügbarkeit sicherstellen zu können.

2.5 Bewegungsprofile

Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

2.6 Verfügbarkeitsprobleme

Die Verfügbarkeit kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- Störungen durch andere Nutz-Anwendungen im gleichen ISM-Band
- Störung durch gezielt eingesetzte Störsender
- Denial-of-Service (Denkbar sind zum Beispiel Angriffe auf die Energiereserven einzelner Geräte durch Abhalten vom Ruhe-Modus.)

2.7 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu bedenken:

- Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.
- Authentisieren muss sich bei Bluetooth nur das Gerät, in der Regel aber nicht der Benutzer gegenüber dem Gerät. Bei Abhandenkommen mobiler, gepaarter Geräte sind diese also in der Regel ohne weiteres durch unbefugte Dritte im Herkunftsbereich nutzbar.
- Bluetooth-Geräteadressen sind mit geeignetem Equipment manipulierbar (Flash-Memory).
- Auch in Ad-hoc-Netzwerken existiert die Gefahr der Verbreitung von Computer-Viren und trojanischen Pferden.
- Das Abhören bzw. Aufzeichnen von Raumgesprächen unter Verwendung von handelsüblichen oder speziell manipulierten Bluetooth-Geräten (z. B. Headset mit 100 mW Sendeleistung) ist grundsätzlich nicht auszuschließen (vgl. hierzu auch [8]).

3 Schutzmaßnahmen

Bluetooth-Geräte, die mindestens einen sicherheitsrelevanten Dienst anbieten, sollten Verschlüsselung mit Kombinationsschlüsseln unterstützen; die Geräte dürfen keine Geräteschlüssel verwenden. Außerdem müssen sie in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen ergriffen werden können und welche Rest-Risiken bestehen.

3.1 Absicherung von Bluetooth-Geräten

Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und wenn möglich zu ändern:

- Die Bluetooth-Geräten beiliegende Installations-Software versucht häufig, möglichst viele Dienste zu aktivieren, damit alle Möglichkeiten der Kommunikation mit anderen Geräten genutzt werden können. Nicht benötigte Dienste sollte der Anwender stets deaktivieren.
- Bluetooth-Geräte sollten möglichst wenig "offen" konfiguriert werden, das heißt es ist empfehlenswert, Connectability, Discoverability und Pairability so weit wie möglich einzuschränken.
- Falls die Sendeleistung variabel ist, sollte sie so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich eingestellt werden.
- Als Default-PIN sollte eine möglichst lange und zufällig gewählte PIN verwendet werden (siehe 3.2).
- 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, und als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung akzeptiert werden. Die Schlüssellänge sollte so groß wie möglich gewählt werden.

Stationäre Geräte

Die Absicherung von stationären Geräten, bei denen Bluetooth als Kabelersatz - zum Beispiel zur Verbindung mit immer den gleichen Peripheriegeräten - verwendet wird, ist nicht besonders kritisch. In abhörgefährdeten Einsatzumgebungen sollten die Geräte mit Authentisierung und aktivierter Verschlüsselung betrieben werden. Die Länge der verwendeten PIN sollte über die minimal empfohlene PIN-Länge (siehe 3.2) hinausgehen.

Mobile Geräte

Bluetooth-Geräte, die mobil verwendet werden und mit fremden Geräten (d. h. Geräten unterschiedlicher Besitzer) kommunizieren, müssen besonders gesichert werden:

- Die Paarung zweier fremder Geräte sollte immer in abhörsicherer Umgebung durchgeführt werden. Die bei der Paarung verwendete PIN muss ausreichend lang sein (siehe 3.2).
- Jedes Gerät, das mehrere Dienste mit unterschiedlichen Sicherheitsniveaus anbietet, sollte in Sicherheitsmodus 2 betrieben werden. In diesem Fall ist darauf zu achten, dass die Sicherheitspolicies sorgfältig erstellt werden.
- Geräte, die nur einen Dienst oder mehrere Dienste mit gleichem Sicherheitsniveau anbieten, sollten im Sicherheitsmodus 3 betrieben werden.
- Die Geräte sollten - falls möglich - so konfiguriert werden, dass die PIN nach der Initialisierung gelöscht wird. Auf diese Weise ist die PIN nicht im Gerät gespeichert und muss nach jedem Einschalten des Gerätes neu eingegeben werden.
- Die Geräte sollten ausgeschaltet werden, wenn sie nicht benutzt werden.
- Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Gerätes sollten alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden.

3.2 Hinweise zur Wahl von PINs

PINs sollten eine möglichst zufällige Folge aus den verwendbaren Zeichen sein, triviale PINs wie "0000" oder "1234" sind unbedingt zu vermeiden (vgl. [5]). Für eine ausreichende Sicherheit bei der Paarung zweier Bluetooth-Geräte ist eine ausreichend lange PIN notwendig. Eine sichere PIN sollte zumindest eine Länge von circa 64 Bit aufweisen. PINs mit bis zu 40 Bit Länge können beispielsweise auf einem handelsüblichen, modernen PC gebrochen werden. Da es bei Bluetooth-Geräten nur möglich ist, PINs in Form von Ziffern bzw. alphanumerischen Zeichen einzugeben, gibt Tabelle 1 Empfehlungen für die Anzahl der zu verwendenden Zeichen.

Verwendete Zeichen	Min. empfohlene PIN-Länge	Minimale PIN Länge
0-9 (10 Zeichen)	19 Stellen (= 63 Bit)	12 Stellen (= 40 Bit)
0-9, A-Z (36 Zeichen)	12 Stellen (= 62 Bit)	8 Stellen (= 41 Bit)
0-9, A-Z, a-z (62 Zeichen)	11 Stellen (= 65 Bit)	7 Stellen (= 42 Bit)
(druckbares) ASCII (95 Zeichen)	10 Stellen (= 66 Bit)	6 Stellen (= 39 Bit)

Tabelle 1: Wahl von PINs

Beispiel: Akzeptiert das Gerät nur Ziffern und Großbuchstaben als PIN, sollte in jedem Fall eine PIN von mehr als 8 Stellen verwendet werden; empfohlen werden jedoch PINs mit mindestens 12 Stellen.

Anmerkung: Unter Umständen gibt es Geräte, bei denen 19-stellige PINs nicht eingegeben werden können. Im Falle, dass nur Ziffern eingegeben werden können, sind dann aber zum Beispiel 16 Stellen für eine ausreichende Sicherheit nicht genug.

3.3 Weitere Schutzmaßnahmen

Über die in 3.1 genannten Maßnahmen hinaus sollten auf Bluetooth-Geräten - falls dies technisch möglich ist - weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

usw.

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [5].

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen (vgl. auch [8]).

3.4 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von Bluetooth-Geräten immer folgende Rest-Risiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (vgl. 2.5) kann nicht verhindert werden.
- Die Gefährdung der Verfügbarkeit (vgl. 2.6) ist ebenfalls nicht vermeidbar.
- Man-in-the-Middle-Angriffe (vgl. 2.2) sind auch bei optimal konfigurierten Geräten theoretisch möglich. Abhilfe ist nur durch die Verwendung zusätzlicher Sicherheitsmaßnahmen möglich, zum Beispiel durch die Verwendung von Sicherheitsdiensten in transportorientierten Schichten des ISO-Referenzmodells (z. B. IPSec oder SSL) oder direkt auf Anwendungsebene (Ende-zu-Ende-Sicherheit).

4 Ausblick

Für 2003 ist die Veröffentlichung der Bluetooth-Spezifikation Version 1.2 geplant.

Zukünftige Versionen des Bluetooth-Standards werden die Verwendung des Geräteschlüssels als Verbindungsschlüssel nicht mehr erlauben. Zusätzlich wird das Konzept der Gruppenschlüssel eingeführt. Gruppenschlüssel sollen Roaming ermöglichen, so dass ein Gruppenschlüssel nicht verbindungsindividuell zwischen zwei Geräten ausgehandelt wird, sondern dienstindividuell.

Es ist ebenfalls davon auszugehen, dass die Erstellung eines Kombinationsschlüssels nicht mehr ausschließlich durch die Eingabe einer PIN gesichert wird. Anstelle dessen wird der Kombinationsschlüssel über das Diffie-Hellmann-Verfahren vereinbart. Bei diesem Protokoll wird der Schlüssel über ein asymmetrisches kryptographisches Verfahren berechnet. Die PIN dient nur noch zur Kontrolle, ob die Berechnung nicht manipuliert wurde.

Das Erstellen von Bewegungsprofilen soll durch den neuen Standard erschwert werden, indem die feste Geräteadresse durch temporäre Adressen ersetzt wird. Die feste Geräteadresse wird dann nur noch zum Verbindungsaufbau verwendet.

5 Literatur und Links

Ausführliche Informationen zur Bluetooth-Spezifikation in deutscher Sprache kann man unter anderem den Büchern [4] und [9] entnehmen. Eine genauere Beschreibung der Bluetooth-Sicherheitsarchitektur ist zum Beispiel in [10] enthalten. Aktuelle Informationen zu Bluetooth findet man unter [11] und [12].

Eine ausführliche Beschreibung verschiedener Schwächen im Sicherheitskonzept von Bluetooth findet sich in [13]. Ferner sei an dieser Stelle auf eine umfangreiche Publikation vom amerikanischen National Institute of Standards and Technology [14] hingewiesen, die unter anderem ebenfalls Informationen zum Thema dieser Broschüre enthält.

Es gibt inzwischen zahlreiche Bücher und Publikationen zum Thema Bluetooth. Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[1] http://www.ieee802.org/15/pub/TG1.html

[2] http://www.bluetooth.org

[3] Specification of the Bluetooth System, Version 1.1, erhältlich unter http://www.bluetooth.org/specifications.htm

[4] J. F. Wollert: Das Bluetooth-Handbuch. Poing: Franzis Verlag 2002

[5] Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb

[6] D. Kügler, "Man in the Middle" Attacks on Bluetooth, Financial Cryptography '03, Lecture Notes in Computer Science, Springer-Verlag (noch nicht erschienen)

[7] S. R. Fluhrer und S. Lucks: Analysis of the E_0 Encryption System, Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Seiten 38-48, Springer-Verlag, 2001, http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz

[8] GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen, BSI 2002, http://www.bsi.bund.de/literat/doc/mobiltel/mobiltel.pdf

[9] N. J. Muller: Bluetooth. Bonn: MITP-Verlag 2001

[10] D. Fox: Bluetooth Security, Secorvo White Paper 2002, http://www.secorvo.de/whitepapers/secorvo_wp05.pdf

[11] http://www.bluetooth.com

[12] http://www.palowireless.com

[13] M. Jakobsson und S. Wetzel: Security Weaknesses in Bluetooth. Progress in Cryptography - CT-RSA 2001, Lecture Notes in Computer Science 2020, Seiten 176-191, Springer-Verlag, 2001, http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf

[14] T. Karygiannis und L. Owens: Wireless Network Security, National Institute of Standards and Technology (NIST) Nov. 2002, http://www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

6 Abkürzungen

ACL	Asynchronous connection-less
ASCII	American Standard Code for Information Interchange
BSI	Bundesamt für Sicherheit in der Informationstechnik
CRC	Cyclic Redundancy Check
CVSD	Continous Variable Slope Delta (-Modulation)
E0	Stromchiffre zur Verschlüsselung
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Industrial, Scientific, Medical (2,4 GHz-Band)
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
PAN	Personal Area Network
PCM	Puls Code Modulation
PIN	Personal Identification Number
SCO	Synchronous connection-oriented
SIG	(Bluetooth) Special Interest Group
SSL	Secure Sockets Layer
TDD	Time Division Duplex