Bluetooth-Sicherheit – Schwachstellen und potenzielle Angriffe

Dr. Kai-Oliver Detken[1], Prof. Dr. Evren Eren[2]

[1]DECOIT GmbH, Fahrenheitstraße 1, D-28359 Bremen
detken@decoit.de

[2]FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund
eren@fh-dortmund.de

Zusammenfassung

Bei Bluetooth handelt es sich um eine Nahbereichsfunktechnik, mit welcher dem Kabelsalat ein Ende bereitet werden soll. Bluetooth wurde extra für die Kopplung von beispielsweise PC, Drucker, Scanner und den verschiedenen mobilen Endgeräten (wie z.B. Handy, PDA oder MP3-Player) entwickelt und bildet dabei eine einheitliche Schnittstelle über die alle Geräte kommunizieren können. Bluetooth wurde durch die Special Interest Group (SIG) 1998 ins Leben gerufen. Die SIG entstand durch die Interessengemeinschaft von fünf Unternehmen aus der Telekommunikations- und Computerbranche. Zu den Gründungsfirmen gehörten Nokia, Ericsson, Intel, IBM und Toshiba. Diese Arbeitsgruppe hat mittlerweile Rahmenbedingungen formuliert und einen allgemein akzeptierten Standard festgelegt, an dem über 1500 Firmen mitgearbeitet haben. Die Version 1.0 der lizenzfreien Bluetooth Spezifikation wurde im Sommer 1999 vorgestellt. Aktuell ist heute die Version 1.2. In diesem Beitrag werden die möglichen Schwachstellen von Bluetooth genau analysiert. Hierbei wird auf Design- und Implementierungsschwächen sowie Schwachstellen des OBEX-Protokolls eingegangen. Des Weiteren werden in diesem Kapitel mögliche Angriffsvarianten aufgezeigt. Der Beitrag schließt mit einer Bewertung ab.

1 Schwachstellen

Bluetooth ist nicht die erste Technologie, die eine drahtlose Datenübertragung ermöglicht und lässt sich leichter konfigurieren als beispielsweise WLAN. Außerdem benötigt sie keinen direkten Sichtkontakt wie bei Infrarot. Obwohl sie bezüglich der Anwendungssicherheit relativ gute Schutzmechanismen zur Verfügung stellt, wobei das Gerät immer eine Interaktion mit dem Benutzer erfordert, gehört sie nicht zu den sichersten Protokollen.

Da Bluetooth auf einer Funkverbindung aufbaut, ist es natürlich grundsätzlich verwundbarer als eine Verbindung über ein festes Kabel. Die Entwickler von Bluetooth haben deshalb Sicherheitsmechanismen auf verschiedenen Ebenen (Verbindungs- oder Dienstebene) entwickelt. Das Frequenzsprungverfahren (Frequency-Hopping-Verfahren) bietet grundsätzlich keinen Abhörschutz, da man sich mit der Sprungsequenz des Opfers synchronisieren und so die Verbindung belauschen kann. In Ad-hoc-Netzwerken wie Bluetooth existiert ebenfalls

keine feste Infrastruktur. Netzwerke werden spontan gebildet. Die Geräte in einem Ad-hoc-Netzwerk sind drahtlos miteinander verbunden. Manche Geräte agieren als Router, wenn sie Nachrichten an andere Geräte weiterreichen, die zu weit von dem sendenden Gerät entfernt sind, um die Nachricht direkt empfangen zu können. Die Topologie eines Ad-hoc-Netzwerkes ist nicht fest – sie ändert sich laufend. All dies macht ein Ad-hoc-Netzwerk verwundbar.

Zu all den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (vgl. Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb), 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. Die Schwachstellen lassen sich in zwei Bereiche kategorisieren:

a. Schwächen im Design des Sicherheitskonzepts
b. Schwachstellen in den Implementierungen und sowie mögliche Risiken, die sich aus dem Zusammenhang der Bluetooth-Anwendungen ergeben

1.1 Designschwächen

1.1.1 Verschlüsselungsalgorithmus

Verschlüsselung ist bei Bluetooth nicht grundsätzlich vorgeschrieben. Viele Bluetooth-Geräte werden herstellerseitig so konfiguriert, dass Verschlüsselung und Authentisierung deaktiviert sind. Wenn keine Authentisierung und Verschlüsselung aktiviert ist, ist Bluetooth nicht sicher. Beispielsweise ist während der Übertragung von TCP/IP-Paketen die Stromchiffre E0 durch Known-Plaintext-Angriffe[1] gefährdet. Für solche Angriffe trägt der Algorithmus selbst dazu bei, weil er auf einer XOR-Verknüpfung von Klartext und Schlüsselstrom aufbaut. Auf der anderen Seite kann der Angreifer recht gut Teile der Klartext-Nachricht herausfinden, weil TCP/IP-Header eine bekannte Form besitzen. Durch diese beiden Vorteile kann ein Angreifer die effektive Schlüssellänge von 128 Bit auf etwa 84 Bit reduzieren. Dadurch sinkt die Anzahl der möglichen Schlüsselkombination und ein Brute-Force-Angriff wird für einen potentiellen Angreifer erleichtert. E0 gewährleistet die Sicherstellung der Integrität mittels Anfügen einer CRC-16 (Cyclic Redundancy Check, 16 Bit) basierten Prüfsumme an den Klartext vor dessen Verschlüsselung. Durch die Linearität der CRC-Prüfsumme und lineare XOR-Struktur der Stromchiffre E0 kann man einzelne Bits gezielt manipulieren.

Bisher sind Angriffe auf den Verschlüsselungsalgorithmus nur theoretisch erklärt. Stutzke und Löhlein [LOST 2000] zählen die möglichen Angriffe auf E0 wie folgt auf:

- Inversionsattacke
- Schnelle Korrelationsattacke
- Bedingte Korrelationsattacke
- „Ultimative Divide and Conquer“-Attacke
- „Time Memory Trade-off“-Attacke

Durch diese Angriffe auf den Verschlüsselungsalgorithmus E_0 sinkt die Sicherheit von 2128 Operationen auf 266. Die Wahrscheinlichkeit für eine Brute-Force-Attacke wächst. Zwar wird die Verschlüsselung hiermit noch nicht gebrochen, aber durch diese Angriffe wird die

[1] Der Angreifer kennt in diesem Fall Teile des Klartextes der übermittelten Nachricht

Verwundbarkeit des E_0-Algorithmus klar. Die leistungsfähigsten Angriffe auf E_0 sind die Wechselbeziehungsangriffe (Correlation-Attacken) in der Kombination mit vollständiger Suche (mit einer Brute-Force-Attacke) über einen begrenzten Schlüsselraum (dieses wird manchmal auch als „schätzende Initiale“ bezeichnet).

1.1.2 Zufallszahlengenerator

Ein weiterer kritischer Punkt bei Bluetooth ist der Zufallsgenerator. In der Bluetooth-Spezifikation werden keine Anforderungen an den Zufallsgenerator gestellt und er wird unzureichend definiert. Die Hersteller entscheiden hier, auf welche Art sie die Zufallszahlen erzeugen. Aus wirtschaftlichen Gründen werden teilweise schlechte Zufallszahlengeneratoren eingesetzt, die mit vorhersagbaren Ergebnissen die Sicherheit erheblich gefährden.

1.1.3 Unit Key (Geräteschlüssel)

Im Bluetooth-Standard liegt keine Beschreibung vor, wie der Unit Key im Gerät gespeichert werden soll. Hier besteht die Möglichkeit, dass ein Angreifer den Schlüssel unerlaubt ausliest. Auch hier liegt es nahe, dass manche Hersteller die Sicherheit aus Kostengründen vernachlässigen. Der Unit Key ist mehrfach verwendbar, wird jedoch im Allgemeinen nur ein Mal verwendet. Er wird in allen Endgeräten gespeichert, die mit dem Besitzer des Unit Keys eine Kommunikation aufbauen wollen. Dadurch kann sich jedes Gerät als Master ausgeben. Man müsste lediglich die BD_ADDR nachahmen („Sniffing“-Attacke). Ein Angreifer kann Informationen einer zuvor aufgebauten Verbindung nutzen, da der Link Key aus der BD_ADDR, PIN und einem RAND erzeugt wird, sind diese Informationen jedem Verbindungspartner bekannt. Somit könnten auch diese Daten dem Angreifer bekannt sein. Mit ihnen kann er versuchen, einen Link Key einer aktiven Verbindung zu erraten. Damit wäre er in der Lage, die Verbindung abzuhören. Aus diesem Grund wird ab Version 1.2 der Gebrauch von Unit Keys nicht mehr empfohlen, auch wenn sie noch in der Spezifikation enthalten sind.

1.1.4 Schlüsselstärke

Problematisch am Sitzungsschlüssel (Encryption Key) ist seine variable Länge, die weniger als 128 Bit betragen kann. Die spezifizierte Mindestlänge von 8 Bit reicht für eine tragbare Verschlüsselung nicht aus. Da nicht in allen Ländern Verschlüsselung mit 128 Bit erlaubt ist, konnte eine Mindestschlüssellänge auf 128 Bit nicht festgeschrieben werden. Benutzer haben damit keinerlei Einfluss auf die Schlüsselstärke des E_0-Algorithmus. Die Schlüssellänge ist in der Hardware implementiert.

Ein Angreifer kann natürlich versuchen, die Schlüssellänge, die im Klartext gesendet wird, zu erraten, um später die Kommunikation abzuhören. Die Gefahr wäre nicht so eklatant, wenn beide Nutzer über die Länge des verwendeten Schlüssels informiert würden, sodass ein rechtzeitiger Abbruch möglich wäre.

1.1.5 PIN-Code

Die PIN spielt zunächst bei der Authentisierung der Geräte eine Rolle und muss somit beim ersten Kontakt zweier Geräte angegeben werden. Sie dient der Berechnung des Link Keys und geht auch indirekt, durch die Erzeugung des Sitzungsschlüssels aus dem Link Key, mit in den Sitzungsschlüssel ein.

Bei einer 128-Bit-Verschlüsselung ist immer noch keine hinreichende Sicherheit gewährleistet, wenn eine vierstellige PIN zum Einsatz kommt. Schwache PINs, die für die Generierung

der Verbindungs- und Verschlüsselungsschlüssel benutzt werden, können leicht geschätzt werden. Im Allgemeinen erhöht eine längere PIN die Sicherheit. Manche PINs sind beim Auslieferungszustand standardmäßig auf „0000“ eingestellt. Wenn beim Pairing eine schwache PIN verwendet wird, kann ein Angreifer diese ermitteln und anschließend den Link Key erraten. Er könnte während des Pairing-Prozesses die Authentisierung aufzeichnen. Mit Hilfe der abgehörten Daten ist er dann in der Lage zu prüfen, ob er die PIN richtig ermittelt hat. Er kann die Kommunikation ungestört belauschen. Die Einbeziehung der PIN in die Berechnungen der unterschiedlichen Schlüssel ist äußerst bedenklich und stellt die größte Schwachstelle im Sicherheitskonzept von Bluetooth dar.

Weil die PINs als einzige geheime Parameter bei der Generierung des Link Keys verwendet werden, stellen sie einen großen Risikofaktor dar. Wenn von einem Endgerät der Unit Key als Link Key gebraucht wird, wird für jede andere weitere Verbindung mit diesem Gerät immer derselbe Schlüssel verwendet. Wenn der Angreifer eine Verbindung zu diesem Gerät aufbauen kann, kann er sich selbst als dieses Gerät ausgeben bzw. identifizieren lassen und die Kommunikation abhören. Der Cyclic Redundancy Check (CRC) dient zwar zur Integritätssicherung. Allerdings wird mit diesem immer noch kein ausreichender Schutz für die absichtliche Datenmanipulation zugesichert.

Eine elegante Weise zur Erzeugung und Verteilung von PINs existiert nicht. Die Erzeugung von PINs in großen Bluetooth-Netzen mit einer hohen Zahl von Benutzern kann schwierig sein.

1.1.6 Frequenzsprungverfahren

Das Frequenzsprungverfahren (Frequency Hopping) wird oft mit der Abhörsicherheit in Zusammenhang gebracht. Dieses Verfahren wurde entwickelt, um die Übertragung gegen Störquellen widerstandsfähiger zu machen. Es ist jedoch kein Mechanismus zur Sicherstellung der Datenkommunikation. Durch einen schnellen Wechsel zwischen 79 Frequenzen wird der technische Aufwand für Angriffe erschwert.

Jedoch stellt das Frequenzsprungverfahren keinen endgültigen Schutzwall gegen Angriffe dar, denn ein Angreifer kann mit einem Breitbandscanner alle 79 Kanäle gleichzeitig von Bluetooth benutzten und Frequenzen innerhalb eines Zeitintervalls abhören. Anschließend ist er dann problemlos in der Lage, die Datenübertragung zu rekonstruieren und die von ihm gesammelten Datenpakete in der richtigen Reihenfolge zusammenzusetzen.

1.1.7 Sicherheitsmodi

Da alle Sicherheitsdienste in der Datenübertragungsschicht (Layer-2) angesiedelt sind, ist bei Bluetooth keine Ende-zu-Ende-Sicherheit möglich. Zwar wird die Verbindung geschützt, jedoch fehlt eine nahtlose und durchgehende Datenverschlüsselung zwischen Endgeräten. Nur einzelne Verbindungen werden verschlüsselt und authentisiert. Die Daten werden an den Zwischenpunkten wieder entschlüsselt. Diese Schwächen werden in den Sicherheitsmodi folgendermaßen aufgelistet:

- **Modus 1:** Verschlüsselung wird nicht aktiviert.
- **Modus 2:** Verschlüsselung, die von der Applikationsebene aus aktiviert wird.
- **Modus 3:** Verschlüsselung, die unabhängig von der Applikationsebene aktiviert wird.

In den Sicherheitsmodi 1 und 2 ist Verschlüsselung optional und kann aus diesem Grund umgangen werden.

1.1.8 Entfernen aus dem Empfangsbereich

In der Bluetooth-Spezifikation ist das Verhalten des Geräts für den Fall, dass es sich aus der Sendereichweite eines gepairten Endgeräts wegbewegt, nicht definiert. Die Auswirkungen dieser Schwachstelle sind von der Anwendung und von der benutzten Hardware abhängig. Geräte können im eingeschalteten Modus stets kommunizieren, auch wenn sie sich in einer völlig neuen Umgebung befinden sollten. Wiederum können andere Geräte dieses Merkmal benutzen, um daraus Bewegungsprofile zu erstellen. Somit kann eine Vielzahl von Geräten in der Umgebung ausfindig gemacht werden. Als Lösung bietet Bluetooth hierzu den Non-Discoverable-Mode an. Ein in diesem Modus befindliches Gerät reagiert nicht auf etwaige Suchanfragen anderer Bluetooth-Geräte. In Tabelle 1 werden die vorgestellten Schwachstellen zusammengefasst.

1.1.9 Implementierungsschwächen

Die am meisten genannten Bedrohungen beziehen sich auf die Bluetooth-Schnittstelle. Angriffe nutzen dabei die Sicherheitslücken in instabilen Implementierungen des Bluetooth-Protokollstacks. Wenn ein Angreifer mit einer Antennen[2]-Verstärkung ausgestattet ist, kann er somit noch Signale wesentlich kleiner -85 dBm[3] empfangen. Dabei kann er von einem weit entfernten Platz aus operieren (außerhalb der Private-Bubble der Klasse-3-Geräte).

Das erste Sicherheitsloch, das im November 2003 von Adam Laurie[4] entdeckt wurde, basiert auf der Authentisierung bei Geräten, wobei die eigentliche Lücke nur in bestimmten Geräten mit Implementierungsfehler vorkommt. Diese Geräte löschen alte Pairings nicht sauber und ermöglichen trotz der Löschung der Pairings immer noch Verbindungen zu den zuvor aufgebauten Geräten. Es könnte dadurch eine Verbindung ohne Benachrichtigung des Benutzers aufgebaut werden. Dieses Sicherheitsloch wird beim Bluesnarf-Angriff verwendet.

Bezüglich dieser Sicherheitslücken, die auch in den Angriffen Bluebug und BT-Chaos ausgenutzt werden, ist nichts Genaues bekannt. Man weiß jedoch, dass es sich bei den ausgenutzten Sicherheitslücken nicht um Fehler in der Bluetooth-Spezifikation handelt. Sie entstanden vielmehr durch schlechte Implementierungen seitens der Hersteller.

Die Topologie ist bei Ad-hoc-Netzen mit mobilen Endgeräten nicht fest vorgegeben. So sind die sicherheitstechnischen Konsequenzen für den Fall nicht festgelegt, dass sich ein oder mehrere Bluetooth-Geräte aus dem Empfangsbereich der anderen Geräte entfernen. Ein weiterer unbeschriebener Risikofaktor ist die Möglichkeit, Verbindungen auf höheren Schichten auch über große Entfernungen und zahlreiche Piconets hinweg aufzubauen.

Bei Betrachtung der Sicherheitsmodi, speziell Modus 2, stellt man weiterhin fest, dass die Zugangskontrolle beim Verbindungsaufbau nur von einem Gerät durchgeführt werden könnte. Diese Zugangskontrolle ist jedoch bidirektional erforderlich, da auch jede Verbindung bidi-

---

[2] Antennen mit hohem Gewinn und zusätzlichen Elektronikkomponenten

[3] Die meisten neuen Bluetooth-Implementierungen haben eine Empfindlichkeit von -85 dBm statt der mindestens geforderten -70 dBm.

[4] Adam Laurie (A.L. Digital Ltd): http://www.thebunker.net/security/bluetooth.htm

rektional ist. Weiterhin ist zu diesem Zeitpunkt lediglich das Gerät, nicht jedoch dessen Benutzer authentisiert worden, was nur auf Applikationsebene durchgeführt werden kann.

Eine weitere Schwäche ist die eindeutige BD_ADDR, die dazu missbraucht werden kann, das Gerät respektive dessen Benutzer zu observieren, und so ein Bewegungsprofil zu erstellen. Die BD_ADDR wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket vorhanden [KOES 2002].

Tab. 1: Designschwächen

Angriffe	Vertraulichkeit	Integrität	Verfügbarkeit	Verbindlichkeit	Authentizität	Verlässlichkeit
E_0	x	x		x	x	
Generator	x	x		x	x	
Schlüsselstärke	x	x		x	x	
PIN-Code	x	x		x	x	
Unit Key	x	x		x	x	
FH-Verfahren	x			x	x	
Sicherheitsmodi	x	x		x	x	
Empfangsbereich			x			x

1.1.10 OBEX-Schwächen

Das OBEX-Protokoll wird für unterschiedliche Aufgaben in mehreren Profilen eingesetzt. Als die bedeutsamsten Profile gelten das OBEX Object-Push-Profil und das Synchronisationsprofil, das auf der IrMC-Spezifikation aufsetzt. Im Falle, dass ein mobiles Gerät beide Profile unterstützt, werden diese mit höchster Wahrscheinlichkeit auf den gleichen OBEX-Stack zurückgreifen. Eine Implementierung vom OBEX-Protokoll findet man in dem Open-Source-Projekt „OpenOBEX[5]“, die das OBEX-Protokoll unabhängig vom Transport-Medium implementiert. Durch die Kombination (Object Push, Synchronisation, IrDA, Bluetooth und OBEX) werden Sicherheitslücken offen gelegt. Anhand des folgenden Beispiels soll dies erläutert werden.

Das OBEX-Object-Push-Profil und das Synchronisationsprofil spezifizieren genaue Anwendungsfälle, wobei das OBEX-Protokoll und das Generic-Object-Exchange-Profil (GOEP) nur das Framework für OBEX und Bluetooth beschreiben.

OBEX definiert, wie bei HTTP, den Zugriff auf das Dateisystem. Das bedeutet, dass man Dateien von einem OBEX-Server herunter- und hochladen kann. Meistens ist das OBEX-Dateisystem allerdings virtuell, denn jede Dateioperation wird in systemspezifische Funktionen umgewandelt und ausgeführt. Bei der Versendung einer Visitenkarte wird sie in die Inbox des Gerätes geschrieben („OBEX PUT“-Operation ohne Pfadangabe). Das Zielgerät wird durch das OBEX-Dateisystem benachrichtigt und die Visitenkarte zur Anzeige gebracht. Das OBEX-Object-Push-Profil definiert hier nur den Austausch von PIM-Daten, also OBEX-Operationen für die INBOX. Das Synchronisationsprofil, das aus dem IrDA-Bereich kommt, wird nun in der Bluetooth-Spezifikation verwendet. IrMC benutzt ebenfalls die Standard OBEX-Operation „GET und PUT“. Außerdem definiert es spezielle Pfade, mit

[5] OpenOBEX: http://openobex.sf.net

denen man Funktionen ansteuern kann. So erhält man beispielsweise mit dem Befehl „GET telecom/pb.vcf“ das komplette Telefonbuch eines Mobiltelefons. Die gegenteilige PUT-Operation würde das Telefonbuch überschreiben. Mit Hilfe des Pfades „telecom/cal.vcs“ kann der Kalender ausgelesen und verändert werden. Neben diesen beiden Pfaden existieren noch weitere Pfade, mit denen man auf Einzeleinträge bzw. Spezialinformationen zugreifen kann, die dann eine Datensynchronisierung erlauben.

Ein Vergleich der beiden Profile führt dazu, dass ein Zugriff auf das Synchronisationsprofil unbedingt gesichert werden muss, um die persönlichen PIM-Daten zu schützen. Da über das Object-Push-Profil nur Visitenkarten ausgetauscht werden, ist hier ein spezieller Schutz nicht notwendig. Es ist davon abzuraten, die Bluetooth-Sicherheitsmechanismen auf das Object-Push-Profil anzuwenden, da sie zu einem unerwünschten Vertraulichkeitsstatus mit einem fremden Gerät führen können.

Man kann eine OBEX-Verbindung über RFCOMM-Channel X aufbauen, wenn das Antriggern der Bluetooth-Sicherheitsmechanismen aufgrund der RFCOMM Channel Number erfolgt. Wird eine Verbindung über RFCOMM 3 aufgebaut, wird kein Link Key angefordert. Daher handelt es sich hier um eine unsichere Verbindung. Wird im Gegensatz eine Verbindung über RFCOMM 4 etabliert, ist ein Link Key zwingend erforderlich. Man kann beispielsweise den Zugriff auf „telecom/pb.cf“ auch über das OBEX Object-Push-Profil durchführen, wenn beide Profile den gleichen OBEX-Stack und wahrscheinlich auch das gleiche virtuelle Dateisystem verwenden. Somit ist auch ein unautorisierter Zugriff auf das Telefonbuch möglich. Bluetooth-Geräte, die sich im Visible-Modus befinden, können möglicherweise somit ihre PIM-Daten unbeabsichtigt offen legen.

Wird der OBEX-Stack nicht vom Hersteller sondern von einem Zulieferer hergestellt, so ist es möglich, dass diese Implementation ggf. von mehreren Herstellern verwendet wird. Falls Hersteller A kein Synchronisationsprofil realisiert hat, ist es sehr wahrscheinlich, dass man beispielsweise mit dem Zugriff „telecom/pb.vcf“ das gewünschte Resultat erzielt, da derselbe OBEX-Stack bei Hersteller B auch das Synchronisationsprofil bedienen muss. Ein Angreifer kann mittels des offiziellen „Linux Bluetooth Stacks“ BlueZ[6] und der OpenOBEX-Implementierung diese Sicherheitslücke leicht ausnutzen.

1.2 Angriffe

1.2.1 Lokalisierung

Dieser Angriff ermöglicht es, den Standort des Zielgerätes ausfindig zu machen. Voraussetzung hierfür ist, dass sich das jeweilige Gerät im Discoverable-Modus befindet. Das heißt, dass das Gerät regelmäßig nach Inquiry-Nachrichten abhört und darauf eine Antwort zurückliefert. Die Angriffsgeräte senden nun dauernd Inquiry-Nachrichten aus, sodass die Zielgeräte in dem oben genannten Modus reagieren. Deren Antwort enthält auch die BD_ADDR.

Der Angreifer wird seine Angriffsgeräte (meist reicht ein Laptop und die entsprechende Software aus) an strategisch gut überlegten Plätzen wie z.B. in großen Wartehallen an Flughäfen oder Internetcafes aufstellen. Für den Angreifer ergibt sich ein kaum erwähnenswerter finanzieller Aufwand und die Wahrscheinlichkeit einen erfolgreichen Angriff durchzuführen,

[6] BlueZ: http://www.bluez.org

ist aufgrund der hohen Gerätedichte an den genannten Orten, sehr hoch. Wenn eine Beziehung zwischen der BD_ADDR und der Zielperson beispielsweise beim Kauf des Gerätes via Kreditkarte hergestellt werden kann, kann die Lokalisierung der Zielperson bei ausreichender Überdeckung wichtiger Punkte grob determiniert werden. Dabei kann es also festgehalten werden, welche Personen sich wann und wo treffen. Wenn sich das Gerät nicht im Discoverable-Modus befinden sollte, kann der Angriff so umgelenkt werden, dass aktive Kommunikation belauscht werden und dadurch auch der Channel-Access-Code in Erfahrung gebracht werden kann. Diesen Angriff kann man zwar nicht eindeutig einem Gerät zuordnen, aber die Kollisionswahrscheinlichkeit ist hinreichend klein, um das Zielgerät anzugreifen. Für diesen Angriffszweck braucht man ein Gerät, welches auf allen 79 Hops parallel abhört und jegliche CACs aufzeichnet.

1.2.2 Bluesnarf

Ursprünglich kommt das Wort „Snarf“ aus dem Hackerjargon. Bei einer „Snarf-Attacke“ wird ein Dokument oder eine Datei ohne Einverständnis des jeweiligen Eigentümers eingesehen. Im Frühling 2004 wurden die ersten Meldungen über Bluesnarf- bzw. Snarf-Attacken veröffentlicht. Diese Angriffe nutzen das von Adam Laurie (A.L. Digital Ltd.) gefundene Sicherheitsloch schlecht programmierter Firmware von Bluetooth-Handys aus. Mit Bluesnarf-Attacken hat man als Angreifer die Möglichkeit, Daten aus dem Adressverzeichnis oder Kalender einzusehen, ohne dass der Besitzer dies wahrnehmen kann. Diese Attacke kann man nur dann durchführen, wenn sich das Zielgerät im Invisible-Modus befindet. Normalerweise kann man sich diesen Angriff im Umkreis von rund 10 Metern vornehmen. Die neulich von Adam Laurie abgeschlossenen Tests zeigen aber als Ergebnis, dass solche Attacken auch im Umkreis von 1 km auch Erfolg haben könnten, obwohl der Bluetooth-Standard eine maximale Übertragungsdistanz von 100 Metern vorsieht. Das Wichtigste hierbei ist, dass für die Datenübertragung keine Kopplung der Geräte (Pairing) erfolgt. Auf dem Handy ist nicht zu sehen, dass Daten ausgelesen werden.

1.2.3 BTChaos

Bei dem BTChaos-Angriff geht es darum, dass eine vom Sicherheitsunternehmen Integralis entdeckte Sicherheitslücke in Bluetooth-Handys ausgenutzt wird. Diese Sicherheitslücke ist durch eine Bluetooth-Implementierung der Mobiltelefon-Hersteller entstanden. Laut Aussagen der Firma Integralis baut das Tool auf das Backup-Programm btxml.c auf und diese Chaos Attacke ist somit eine erweiterte Bluesnarf-Attacke. Dieses Tool liest die Daten mit AT-Befehlen, wie Bluebug aus den Mobiltelefonen aus und schreibt noch zusätzlich Daten. Wie alle anderen Bluetooth-Attacken funktioniert auch der BTChaos-Angriff nur, wenn sich das Zielgerät im Umkreis von rund 10 Metern zum Angreifer befindet. Zum Ausführen der Attacke wird ein spezielles C-Programm sowie diverse, frei erhältliche Software benötigt. Diese Attacke basiert auf einer fehlerhaften Implementierung der Authentisierung und läuft über OBEX ab. Ähnlich wie bei der Bluebug-Attacke können mit der Chaos-Attacke folgende Aktionen durchgeführt werden: Telefonanrufe umleiten, Telefonverbindungen aufbauen und bestehende Verbindungen beenden, SMS lesen und versenden und Auslesen des Telefonbuchs, gespeicherter SMS und ISM Nummer aus dem Handy.

Folgende Standard-Mobiltelefone mit Bluetooth sind laut Angabe des Entwicklers von solchem Angriff betroffen: Sony Ericsson: T68i, T610 und Nokia: 6310i, 6650. Auf der Webseite von Integralis kann eine detaillierte Liste mit den Testergebnissen eingesehen werden.

1.2.4 Bluebug

Die Funktionsweise der Bluebug-Attacke ist ähnlich wie die der BTChaos-Attacke. Der Unterschied zwischen beiden Attacken ist, dass über die Bluebug-Attacke die AT-Befehle an das Zielgerät über RFCOMM gesendet werden können, wobei diese bei der BTChaos-Attacke über OBEX durchgeführt wird. Anhand dieser AT-Befehle ist es möglich ein SMS zu versenden, welche für das Opfer nicht sichtbar ist und auch nicht im Postausgang als gesendete SMS abgelegt wird. Die Standard-SMS-Einstellungen fordern nur selten einen Bericht über die gesendete Nachricht, wobei aber bei dieser Art von Attacke das Opfer einen Bericht der SMS, welche er nicht selber gesendet hat, erhält. Bei PDU (Protocol Data Unit)-verschlüsselten Nachrichten kann durch das Setzen eines Flags überprüft werden, ob ein solcher Bericht gesendet wird oder nicht. Außerdem kann mit der Bluebug-Attacke die Telefonnummer des Zielgerätes ermittelt werden. Bei allen anderen Bluetooth-Attacken ist nur die spezifische BD_ADDR des Zielgerätes erkennbar. Laut Angaben von Martin Herfurt, dem Entwickler der Bluebug-Attacke, baut der SMS-Bereich seines Angrifftools auf das öffentlich erhältliche PDUSpy auf.

Mit dem AT-Befehlssatz können folgende Aktionen durchgeführt werden:

- **Telefongespräche:** Ein Angreifer kann Telefongespräche einleiten und mit dem Telefon des Opfers sein eigenes Telefon (mit anonymer Calling-Card) anrufen. Dadurch ist er imstande, alles festzuhalten, was in der Nähe des Opfers gesprochen wird. Der Anruf dauert so lange, bis der Angreifer oder das Opfer das Gespräch beendet. Er ist auch in der Lage, seinem Opfer durch teure Servicenummern einen finanziellen Schaden hinzuzufügen.
- **SMS:** Durch das Versenden einer SMS vom Handy des Opfers kann der Angreifer folgenden Schaden anrichten:
  - Der Angreifer schickt die SMS-Kurznachricht an sich selbst und kann somit die Telefonnummer des Opfers ermitteln.
  - Der Angreifer kann an teure Servicerufnummern SMS-Kurznachrichten verschicken und z.B. Klingeltöne, Logos, Games etc. bestellen.
  - Einige Netzbetreiber bieten ihren Kunden Location Based Services (LBS) an. Um diese freizuschalten, muss an den Netzbetreiber eine entsprechende SMS-Kurznachricht geschickt werden. Der Angreifer könnte diese Nachricht nun schicken, um den LBS-Dienst freizuschalten. Danach wäre es ihm möglich, die Position seines Opfers zu verfolgen.
  - SMS können mittels PDUSpy auch ausgelesen werden, um an private Informationen (im SIM gespeicherten Kurznachrichten) des Opfers zu gelangen.
- **Telefonbuch:** Viele Informationen, z.B. über den letzten Anrufer, lassen sich auch aus dem Telefonbuch eines Handys gewinnen. Dieses kann auch gefälscht werden, indem falsche Telefonnummern unter einem Eintrag hinterlegt werden wie z.B. teure Service-/ Mehrwertnummern. Ebenso kann die Anrufliste überschrieben bzw. gelöscht werden, um eben diese Anrufe zu verschleiern.

- **Anrufweiterleitung:** Es ist möglich, für das Opfer unbemerkt Anrufe auf andere Handys umzuleiten.
- **Internetverbindung:** Der Angreifer kann eine Internetverbindung aufbauen, über welche er dann anonym bzw. mit der Identität des Opfers weiteren Schaden anrichten kann (z.B. Malcode in Umlauf bringen). Das Gerät kann außerdem so manipuliert werden, dass es die Anrufe immer über einen bestimmten Service-Provider ausführt (ähnlich wie ein PC-Dialer).

Folgende Modelle sind nach Angaben des Entwicklers durch die Bluebug-Attacke betroffen: Sony Ericsson: T610, Nokia: 6310i sowie Motorola: V80 und V600. Eine detaillierte Liste dieser Geräte kann man bei A.L. Digital einsehen. Laut Martin Herfurt sollen die Details dieses Angriffs nur an Gerätehersteller weitergeleitet worden sein, da durch diese Bluebug-Attacken erheblicher Schaden verursacht werden kann.

1.2.5 PIN

Angriffsziel ist der PIN-Code, der zum Generieren des Link Keys benutzt wird. Auch der Link Key selbst ist ein Angriffsziel. Die PIN-Attacke besteht darin, den PIN im Rahmen aktiver Kommunikation mit dem Zielgerät zu eruieren. Wieder ist hierzu das Durchsuchen des Schlüsselraumes notwendig. Der PIN-Code kann bei Gegebenheit online bestimmt werden. Da in manchen Geräten der PIN-Code fest eingegeben ist, lässt sich dieser Sicherheitsmechanismus auf sehr einfache Weise umgehen. Es reicht, nach jedem gescheiterten Anmeldeversuch und der Eingabe eines falschen PIN-Codes die BD_ADDR des Bluetooth-Gerätes zu ändern. Bei Mobiltelefonen oder PDAs ist dies nicht so einfach, doch ein Notebook mit einer Bluetooth-Karte bietet schon uneingeschränkte Möglichkeit, in den Bluetooth-Stack einzudringen.

Eine andere Alternative zu der PIN-Attacke wäre, diese offline durchzuführen. Kann ein Angreifer die beim Erzeugen des Link Keys ausgetauschten Nachrichten abhören, so ist er in der Lage, im Nachhinein offline eine erschöpfende Suche nach der verwendeten PIN durchzuführen. Wichtig ist, dass die Zufallszahl RAND und die Nachrichten im Überprüfungsprotokoll des Init Keys abgehört werden. Somit kann der Angreifer einfach alle PINs des angenommenen PIN-Raumes durchprobieren und immer überprüfen, ob die richtige PIN gewählt wurde. Wesentlich bei dieser Attacke ist, dass der Gegner nur passiv ist. Mit dem Init Key kann ein Angreifer, falls er die Nachrichten beim Generieren des Link-Schlüssels abhört, diesen einfach berechnen.

1.2.6 Spoofing

Bei Spoofing wird der Geräteschlüssel als Angriffsmedium verwendet. Spoofing ist als ein Oberbegriff für Angriffstechniken zu verstehen. Bei dieser Angriffstechnik versucht der Angreifer durch Vortäuschen einer falschen Identität, sich Zugriff zu einem fremden System zu verschaffen. Wie Spoofing funktioniert, wird an folgendem Beispiel erklärt:

Die Geräte A und Geräte B benutzen für ihre Kommunikation als Link-Key den Schlüssel des Gerätes A. Danach kommunizieren die Geräte A und C (Dritt-Gerät) mit dem gleichen Link-Key, der zuvor für die Verbindung zwischen den Geräten A und B verwendet wurde. In diesem Fall kennt das Gerät B den Schlüssel des Gerätes A und kann ohne Probleme diesen einsetzen, um eine mögliche Datenübertragung zwischen A und C abzuhören oder gegebenenfalls das Gerät C vorzutäuschen.

In der Praxis braucht man für so eine Angriffstechnik ein Notebook mit Bluetooth-Karte bzw. Adapter. Im Falle einer Verbindung wird die Kommunikation der beiden Geräte über den Link Key aufgebaut. Durch Modifizierung des Protokoll-Stacks kann erreicht werden, dass das angreifende Gerät (in diesem Fall das Notebook) jedes Mal die Verwendung des Schlüssels des anzugreifenden Gerätes anfordert. Dadurch erkennt der Angreifer (Gerät B) den Schlüssel des anzugreifenden Gerätes (Gerät A). Nach Verbindungsende wird die Geräteadresse A im Gerät B abgespeichert, weil er durch frühere Verbindungen diese schon in Erfahrung bringen konnte. Das Gerät B geht dann anschließend durch, ob der Link Key des Gerätes A zur Kommunikation gebraucht wird. Nun kann er die Kommunikation belauschen.

1.2.7 Bluejacking

Eine weitere Angriffstechnik bei Bluetooth ist Bluejacking und diese leitet sich aus den Begriffen „Bluetooth“ und „Hijacking“ ab. Der Angriff besteht darin, einem anderen Bluetooth-Nutzer durch den Missbrauch der Visitenkartenfunktion im Bluetooth-Handy oder PDA unerwünschte Nachrichten zu versenden. Weil beim Bluejacking aufgrund der erforderlichen Nähe meist Sichtkontakt besteht, kann das Opfer personenbezogene Mitteilungen oder über seinen Aufenthaltsort bekommen.

Technisch gesehen verändert der Angreifer die Datenpakete während der „Hanshake“-Protokollphase so, dass er bereits in diesem Stadium anonyme Nachrichten versenden kann. Dies ist möglich, da bereits in der Initialisierungsphase bzw. beim Pairing-Prozess der Name des angreifenden Bluetooth-Gerätes im Display des Zielgerätes angezeigt wird. Da für dieses Feld 248 Zeichen erlaubt sind, kann der Angreifer diesen Datenblock bereits für seine Attacke bzw. für die Nachrichtenanhänge nutzen.

Ob neben dem schreibenden Zugriff (o.g. Mitteilungen) auch ein lesender Zugriff auf die Ressourcen des Opfers während der Authentisierungsphase möglich ist, ist noch nicht geklärt. Ebenso ist unklar, ob ein „Hijacking“ von gerade geführten Gesprächen möglich ist. Aufgrund der „Pairing-Bereitschaft“ des Bluetooth-Protokolls ist dies technisch durchaus vorstellbar und wird weiter untersucht.

1.2.8 Bluesniping

Bluetooth-Geräte können bis zu einem Kilometer Entfernung mit einer gewehrartigen Antenne attackiert werden. Bisher war die Voraussetzungen bei den Angriffen die physische Nähe zum Opfer, da die Funktechnik nur auf kurze Distanzen (10 Meter) funktioniert. Von dem US-Unternehmen Flexis[7] haben die Mitarbeiter ein «Gewehr» konstruiert, mit dem sie aktive Bluetooth-Schnittstellen in Bürohäusern aus mehr als einem Kilometer Entfernung ausfindig machen können.

Die aktiven Bluetooth-Geräte in Bürohäusern sind durch diese Angriffstechnik namens „Bluesniping“ gefährdet und so kann der Angreifer vom Opfer die Agenden, Adressbüchern, Aufgabenlisten oder den mobil abgewickelten Mailverkehr ausspionieren. Laut Testergebnis des US-Unternehmens Flexis stellte sich heraus, dass nach kürzester Zeit mit dem „Bluespinner“[8] im örtlichen Geschäftsviertel mehrere Dutzend offene Bluetooth-Geräte entdeckt worden sind. Seine Besonderheit ist die Richtantenne, die für das Wardriving entwickelt wurde.

---

[7] Flexis: Ein US Unternehmen, spezialisiert in dem Bereich der mobilen Sicherheit

[8] BlueSniper: http://www.tomsnetworking.com

Für ein besseres Ziel wird diese auf einen Gewehrkolben montiert. Zusätzlich wird ein Kleinstcomputer im Patronenmagazin angeschlossen. Die Sicherheitsabteilung der Bluetooth Special Interest Group (BSIG)[9] reagierte auf die neue Angriffswaffe relativ ratlos. Außer ein paar grundlegenden Verhaltensregeln fiel dem Verantwortlichen gegenüber Flexilis nichts Konkretes zur veränderten Bedrohungslage ein [MEIE 2005].

1.2.9 Bluetooth Wardriving

Da jedes Bluetooth-Gerät eigenständig seine eindeutige 48-Bit Adresse überträgt, ist es möglich, die Benutzerbewegungen zu verfolgen. Um ein Gerät vor Locationtracking (Standortverfolgung) zu schützen wird ein anonymer Modus benötigt. Geräte, die im anonymen Modus betrieben werden, aktualisieren regelmäßig ihre Bluetooth-Device-Adresse indem sie zufällig eine neue auswählen. Verschiedene Arten des Location-Tracking-Angriffs sind möglich:

- **Subsection-Inquiry-Attack:** Bei diesem Angriff werden Lokalisierung von Bluetooth-Benutzern eines oder mehrerer Bluetooth-Geräte in der gesamten Region verteilt. Wenn das potenzielle Opfer eines solchen Angriffs sein Gerät im feststellbaren (Discoverable) Modus lässt, kann das angreifende Gerät einfach den Bereich, in dem es häufige Anfragemeldungen für Geräte nutzt, ausfragen und ein Protokoll mit allen Geräteadressen, die entdeckt worden sind, anfertigen.
- **Subsubsection-Traffic-Monitoring-Attack:** Dieser Angriff ist möglich, wenn sich das Bluetooth-Gerät des Opfers nicht im feststellbaren (discoverable) Modus befindet. Der Angreifer überwacht einfach die Kommunikation zwischen zwei vertrauten Bluetooth-Geräten, die dem Opfer gehören. Diese Geräte kommunizieren, in dem sie einen spezifischen Channel Access Code (CAC) anwenden. Dieses CAC berechnet sich aus der BD_ADDR des Master-Geräts im Piconet. Darüber hinaus, wird die gesamte BD_ADDR in den FHS-Paketen der Geräte versendet, die es dem Angreifer ermöglichen, eindeutig die Identität eines Bluetooth-Geräts zu bestimmen. Jedoch werden die FHS-Pakete nur verwendet, wenn die Verbindung bereits hergestellt ist.
- **Subsubsection-Pagin-Attack:** Dieser Angriff ermöglicht dem Angreifer zu bestimmen, ob ein vorgegebenes Bluetooth-Gerät mit einer bekannten BD_ADDR oder Device Access Code (DAC) innerhalb der Reichweite vorhanden ist. Der Angriff fordert, dass das Opfergerät angeschlossen ist. Das angreifende Gerät spricht das Zielgerät an und wartet darauf, dass das ID-Paket zurückgesendet wird, antwortet jedoch dann nicht. Wenn eine ID zurückgesendet wird, weiß der Angreifer, dass das Opfergerät existiert. Das Zielgerät, das auf eine Antwort wartet, wird sofort deaktiviert, und der Vorfall wird nicht zur Anwendungsebene geschickt, d.h., es erfolgt kein Bericht.
- **Subsubsection-Frequency-Hopping-Attack:** Das Frequenzsprungverfahren wird von einer wiederholenden springenden Reihenfolge bestimmt. Es wird von verschiedenen Eingabeparametern bestimmt wie z.B. die Adresse und den Master Clock. Im Status der Verbindung werden Lower Address Part (LAP)10 und vier Bits in der Upper Address Part (UAP)11 des Master-Geräts verwendet. Im Status „Page“ wird die LAP/UAP der paginierten Einheit verwendet. Somit ist es (zumindest theoretisch) möglich, Informa-

[9] BSIG: https://www.bluetooth.org/foundry/sitecontent/document/About_the_SIG

[10] LAP: Bits von 0 bis 23 der einmaligen 48 Bit langen BD_ADDR

[11] UAP: Bits von 24 bis 31 der einmaligen 48 Bit langen BD_ADDR

tionen der LAP und vier Bits in der UAP zu erhalten, die auf dem beobachteten Sprungverfahren basieren.

- **Subsubsection-User-Friendly-Name-Attack:** Ein Bluetooth-Gerät kann jederzeit den benutzerfreundlichen Namen nach einem erfolgreichen Baseband-Paging-Verfahren anfordern. Der Anforderungsbefehl des Namens kann genutzt werden, um eine „Location Tracking"-Attacke vorzubereiten.

1.2.10 Location-Tracking

Beim Location Tracking decken mehrere Hotspots ein bestimmtes Gebiet flächendeckend ab. Sobald ein mobiles Gerät in Reichweite eines Hotspots kommt, wird es registriert und so lange verfolgt, bis es nicht mehr in Reichweite der Hotspots liegt. Das Location Tracking ist eine erweiterte Form des BlueJackings, denn es bietet sich an, den mobilen Geräten Nachrichten zu schicken sobald sie in Reichweite eines Hotspots gelangen. Die Firma „PanGo Networks" bietet eine Software an, mit der sich sog. Proximity-Platforms realisieren lassen. Diese finden Einsatz in Einkaufszentren wo den Besuchern gezielt Werbung und Schnäppchenangebote für das Geschäft, in dem sie sich gerade befinden, auf ihr mobiles Gerät geschickt werden soll. [LEUL 2004]

1.2.11 Denial-of-Service

Ein weiterer Angriff ist die so genannte Denial-of-Service-Attacke (DOS). Bei einem solchen Angriff werden ständig Kommunikationsanfragen vom bluetooth-fähigen Computer eines Hackers[12] an ein anderes Bluetooth-Gerät gesendet. Somit wird der Akku des Bluetooth-Geräts während der Empfangszeit temporär ausgesetzt. Der Hacker kann den Bluetooth-Service des Geräts zeitweise aus dem Verkehr nehmen, wobei parallel die Bluetooth-Verbindung mit den unnötigen bzw. ungültigen Kommunikationsanfragen überfordert ist. Unter dem DOS-Angriff versteht man lediglich die temporäre Störung. Bei so einer temporären Störung bekommen Hacker keine Zugriffsmöglichkeiten auf die Daten oder den Service des betroffenen Geräts. Der Hacker verhindert nur den normalen Gebrauch oder das Management von Kommunikationsmöglichkeiten. Die Informationen auf diesem betroffenen Gerät bleiben jedoch dem erhalten. Wenn der Hacker ein vertrautes Gerät während dieser DOS simuliert und lässt das System vertrautes Gerät sinken. Die Gefahr eines DOS-Angriffs ist wegen der Anforderungen und der kurzen Erreichbarkeit der Bluetooth-Wireless-Technologie gering. Und solche Angriffe wurden nur im Labortest nachgewiesen.

1.2.12 Man-in-the-Middle

Bei dieser Attacke geht es darum, Pakete zweier Kommunikationspartner abzufangen und sie anschließend zu manipulieren. Damit eine Man-in-the-Middle-Attacke durchgeführt werden kann, muss der Angreifer sicherstellen, dass das manipulierte Paket nicht mit dem Originalpaket kollidiert und somit nicht verloren geht. Um dies zu verwirklichen, muss der Angreifer das manipulierte Paket auf einer anderen Frequenz sendet. Der Frequenzsprung wird aber vom Master festgelegt und die beteiligten Geräte können im Piconet miteinander kommunizieren. Wenn sie miteinander synchronisieren, muss der Angreifer den Eindruck der Synchronisation verschaffen. Wenn die Verbindung verschlüsselt ist, lässt sich die Man-in-the-Middle-Attacke nicht so leicht realisieren, weil bei jedem Frequenzsprung ein neuer Initiali-

[12] unter Verwendung bestimmter Software gegebenenfalls ein Tool, der für DOS-Angriff gedacht ist.

sierungsvektor (IV) der Stromchiffre erzeugt wird. Durch eine Schwachstelle im Design wiederholt sich der Initialisierungsvektor innerhalb eines halben Zyklus. So kann theoretisch auch eine Man-in-the-Middle-Attacke realisiert werden. Wobei es in der Praxis bei dieser Attacke nicht nur mit dem Einsatz eines Bluetooth USB-Sticks und einem herkömmlichen PC getan ist, braucht man hier leistungsfähige Hardware.

1.2.13 Re-Pairing

Sobald Bluetooth-Geräte einen gemeinsamen Link Key besitzen, können die ersten Schritte des Pairing-Prozesses übersprungen werden, und es kann direkt mit der gegenseitigen Authentisierung begonnen werden. Ein Angreifer muss in der Lage sein, die beiden Geräte erneut zu einem Pairing-Prozess zu bewegen. Gemäß der Spezifikation darf ein Gerät einen Verbindungsschlüssel „vergessen“. Wenn dies eintritt, wird (statt der gegenseitigen Authentisierung) die Initialisierungsphase gestartet. Der Angreifer muss seine eigene BD_ADDR manipulieren, damit er dem jeweiligen Gerät den richtigen Kommunikationspartner vortäuschen kann.

1.2.14 Backdoor

Bei der Backdoor-Attacke muss ein Angreifer zunächst einen physikalischen Zugriff auf das Gerät realisieren. Mit dieser Methode kann er auf dem Opfergerät sein gepairtes Angriffsgerät manuell auf „Invisible (unsichtbar)“ setzen. Danach kann er eine für das Opfer nicht erkennbare Bluetooth-Verbindung ohne Pairing-Aufforderung herstellen und dann sämtliche Hilfsmittel benutzen, um eine vertraute Verbindung zum Opfergerät herzustellen. Ohne Einwilligung des eigentlichen Besitzers können Dienste in Anspruch genommen werden.

1.2.15 Brute-Force

Geräteklassen wie Bluetooth-Headsets unterstützen nur eine vierstellige PIN, was einen Angriff leichter macht und beschleunigt. Aus der PIN (bestehend aus 16 Bytes) leitet sich der Link Key ab, den die Geräte bei erfolgreichem Pairing-Prozess zur Verschlüsselung und Authentisierung speichern. Falls der Angreifer in der Lage ist, den gesamten Pairing-Prozess zu protokollieren, könnte er die PIN mittels einer „Brute-Force“-Attacke herausfinden. Aus dieser PIN kann er wiederum den Link Key ermitteln. Praktisch gesehen geht noch keine Gefahr hervor, da der Pairing-Prozess zwischen Bluetooth-Geräten selten stattfindet. Deswegen muss der Angreifer zur rechten Zeit am rechten Ort sein, um eine „Brute-Force“-Attacke durchführen zu können. Diese Attacke hat die Funktion, verschlüsselte Passwortlisten zu knacken, die in der Regel aus Hash-Werten bestehen. Man benötigt dafür Tools wie BtScanner und RedFang.

1.2.16 Vergleich der Angriffe

Tab. 2: Zusammenfassung der Angriffe

Angriffe	Vertrau-lichkeit	Integrität	Verfüg-barkeit	Verbind-lichkeit	Authenti-zität	Verläss-lichkeit
Lokalisierung	x			x		
Bluesnarf	x					
BTChaos	x					
Bluebug	x	x	x	x	x	x
PIN		x		x	x	
Location Tra-cking	x					
Spoofing	x					
Bluejacking			x			x
Bluesniping	x					
Wardriving	x	x	x	x	x	x
DOS			x			x
Man-in-the-Middle	x			x	x	
Re-Pairing	x					
Backdoor	x					
Brute-Force	x					

2 Bewertung

Dem Anwender sollte eine Reihe von Problemen bewusst sein, die durch diese technischen Defizite hervorgerufen werden. Dieses Kapitel geht auf mögliche resultierende Risiken ein. Im normalen Fall hat der Benutzer von Bluetooth-Geräten keine Informationen über die korrekte Implementierung vorhandener Sicherheitstechniken. Der Benutzer kann sich nicht sicher sein, ob die Authentisierung beiderseits erfolgt bzw. welche Schlüssellänge der Sitzungsschlüssel (Encryption Key) minimal besitzen muss. Bevor der Benutzer die Sicherheitsparameter für die Übertragung seiner sensiblen Daten über die Bluetooth-Schnittstelle einsetzt, sollte er sich erst ausführlich informieren, welche Parameter sein Gerät zur Verfügung stellt.

So manchem Angreifer gelang es durch die Implementierungsschwächen der Bluetooth-Schnittstelle bei einigen Mobiltelefonen, das betroffene Gerät zu kontrollieren. Anschließend wurde das betroffene Gerät beispielsweise zur Anmeldung an kommerziellen WLAN-Hotspots verwendet. Um dies zu ermöglichen, müsste der Angreifer eine SMS an den Betreiber des Hotspots senden. Der Angreifer kann sich mit den rückermittelten Daten völlig legal auf Kosten des Handy-Besitzers am Hotspot anmelden. Die Hersteller der betroffenen Geräte kümmern sich momentan um Nachbesserungen.

Ein weiteres Problem besteht darin, Bewegungsprofile zu erstellen. Es ist möglich, mittels eines dichten Netzes von Bluetooth-Geräten, regelmäßig die Umgebung nach neuen unbekannten Geräten durchzusuchen. Die gefundenen Geräte antworten meistens mit ihrer eindeutigen BD_ADDR auf Anfragen in Abhängigkeit von ihrem derzeitigen Modus. Durch diese Information ist man in der Lage, die Bewegung eines bestimmten Bluetooth-Gerät nachzuvollzie-

hen. Für Supermarkketten oder Einkaufspassagen wären solche Profile potentiell interessant. Durch die erstellten Profile könnten diese ihr Marketing optimieren, um so das Angebot besser an Kunden zu orientieren. Bei Bluetooth sind die spezifizierten Sicherheitsmechanismen nur optional, wie in vielen Kommunikationsstandards.

Es wäre generell zu empfehlen, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und gegebenenfalls anzupassen:

- Es dürfen keine Unit-Keys (Geräteschlüssel) während der Verschlüsselungsphase bei den Geräten verwendet werden. Außerdem müssen diese in geeigneter Form abgespeichert werden.
- Wenn Geräte mindestens einen sicherheitsrelevanten Dienst bereitstellen, sollte Verschlüsselung mit Combination-Keys unterstützt werden.
- Bei der Gerätekonfiguration sollten die Eigenschaften Connectability, Discoverability und Pairability eingeschränkt werden.
- Die variable Sendeleistung sollte so niedrig wie möglich und nur so hoch wie für die Funktionalität erforderlich eingerichtet werden.
- Statt der Default-PIN sollte eine möglichst lange und zufällig gewählte PIN benutzt werden.
- Falls bei einem Gerät eine Authentisierung stattfindet, muss dieses Gerät so eingestellt werden, dass es nach erfolgreicher Authentisierung stets auch eine starke Verschlüsselung benutzt.
- Falls ein Gerät Kommunikationsverschlüsselung voraussetzt, muss die Schlüssellänge mindestens 64 Bit betragen. Als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung mit größtmöglicher Schlüssellänge erfolgen.
- Da stationäre Geräte in der Regel mit denselben Peripheriegeräten kommunizieren, ist eine Absicherung dieser nicht besonders wichtig. Allerdings sollten diese in abhörgefährdeten Umgebungen authentisiert verschlüsselt betrieben werden. Auch die Länge des PIN-Codes sollte über die minimal empfohlene PIN-Länge hinausgehen.

Mobile Geräte, die sich mit fremden Geräten beziehungsweise mit Geräten unterschiedlicher Benutzer verbinden, müssen besonders abgesichert werden:

- Die bei dem Pairing-Prozess benutzte PIN muss ausreichend lang sein.
- Jedes Gerät, das mehrere Dienste mit verschiedenen Sicherheitsniveaus zur Verfügung stellt, sollte im Sicherheitsmodus 2 betrieben werden. Hierbei ist darauf zu achten, dass die Sicherheits-Policies sorgfältig erstellt werden.
- Geräte, die nur einen Dienst oder mehrere Dienste mit gleichem Sicherheitsniveau anbieten, sind im Sicherheitsmodus 3 zu betreiben.
- In den Geräten sollte außerdem die PIN nach der Initialisierung gelöscht werden. Somit wird sie im Gerät nicht gespeichert und muss nach jedem Einschalten des Gerätes erneut angegeben werden.
- Bei Verlust beziehungsweise Diebstahl eines Geräts sollen alle zugehörigen Link-Keys (Verbindungsschlüssel) in den verbliebenen Geräten gelöscht werden.
- Eine bessere Maßnahme zur Unterbindung oder Abschwächung möglicher Attacken wäre, beim Kauf des Gerätes darauf zu achten, dass keine Verbindung zwischen der Basisadresse und der Identität des Käufers hergestellt werden kann.

Für Unternehmen sollten insbesondere Softwarelösungen zur Identifikation von Bluetooth-Geräten Einsatz finden. Diese richten sich vor allem an jene Unternehmen, welche die Verwendung von Bluetooth aus Sicherheitsgründen verbieten. Einige dieser Softwarelösungen sind für PDAs bestimmt, womit auf dem Firmengelände Bluetooth-fähige Geräte wie Laptops, PDAs, Tastaturen, Headsets und Telefone erkannt und Dienste auf diesen Geräten erkannt werden können. Es lassen sich nicht nur Geräte mit falscher bzw. mangelhafter Konfiguration identifizieren, sondern auch herauszufinden, welche Geräte (und Art) in Betrieb sind und mit welchen anderen Geräten sie kommunizieren. Beim Monitoring von Bluetooth-Aktivitäten können Administratoren spezifische Gefahren erkennen und potenzielle Einbrüche abwehren. Typische Funktionen solcher Programme sind:

- Identifikation unterschiedlicher Klassen von Bluetooth-Geräten (PDAs, Keyboards, Headsets, Laptops, Mobiltelefone etc.)
- Ausgabe von zusätzlichen Informationen über das gefundene Gerät (u.a. Hersteller, Signalstärke des Gerätes etc.)
- Informationen über Verbindungen zwischen Geräten
- Identifikation verfügbarer Dienste auf Geräten

Literatur

[DEER06] Detken, Eren: Mobile Security – Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. 672 Seiten; hanser Verlag; ISBN 3-446-40458-9; München 2006

[KOES02] Kösling, A.: Sicherheitsanalyse in drahtlosen Netzen. Universität Oldenburg; Oldenburg 2002

[LOST00] Löhlein, Stutzke: Sicherheit aktuell verwendeter Stromchiffren. Fern-Universität Hagen; Hagen 2000

[LEUL04] Leidecker, Ultsch: Bluetooth Sicherheitsanalyse. FH Stuttgart; Stuttgart 2004

[MEIE05] Meierhans, D.: Nach Wardriving BlueSniping. InfoWeek 21.3.2005