

Bluetooth Attacken



Diplomarbeit 2004

Telekommunikation und Informatik

Hochschule für Technik und Wirtschaft Chur

Diplomanden:
Partnerfirma:
Testgeräte
Dozent:
Ausgabedatum:
Abgabedatum:

Claudio Beltrametti, Reto Calonder
Astalavista IT Engineering, Chur
Swisscom Mobile AG, Chur
Rolf Herheuser
23. August 2004
4. Oktober 2004

Zusammenfassung

Dieser Bericht besteht aus zwei Dokumenten, im ersten mit dem Titel Malware on Mobile Devices werden die zurzeit bekannten Viren, Würmer und Trojaner für PDA's und Mobiltelefone beschrieben. Dieser zweite Teil befasst sich mit Bluetooth-Attacken auf mobile Endgeräte.

Wenn von Bedrohungen für mobile Endgeräte gesprochen wird, dann gehören Angriffe über die Bluetooth-Schnittstelle zu den meistgenannten. Dieser Bericht beschreibt alle bisher bekannten Angriffe via Bluetooth auf mobile Endgeräte. Um das ganze Thema besser zu verstehen werden zu Beginn des Berichtes einige Grundlagen der Bluetooth-Technologie beschrieben. Dabei wird neben dem Protokollstack auch auf die wichtigsten Funktionen von Bluetooth eingegangen.

Bluetooth-Attacken nutzen Sicherheitslücken aus, die auf unsaubere Implementierungen des Bluetooth-Protokollstacks in den Endgeräten zurückzuführen sind. Die verschiedenen Bluetooth-Tools haben unterschiedliche Funktionen und können beispielsweise persönliche Daten wie Telefonbucheinträge, Kurznachrichten oder Anruflisten auslesen, ohne dass der Benutzer etwas davon bemerkt.

Wie kann man sich vor solchen Angriffen schützen? Der letzte Teil des Berichtes zeigt, dass es nicht nur Schutzmechanismen technischer Natur gibt. Das Benutzerverhalten, und der bewusste Umgang mit der angewandten Technologie ist ebenfalls ein wesentlicher Bestandteil der Sicherheit mobiler Endgeräte.

Inhaltsverzeichnis

Einführung	1
Bluetooth Grundlagen.....	1
Technologie.....	1
Bluetooth Protokolle	2
Verbindungsmanagement	3
Gemeinsame Parameter	3
Bluetooth Attacken.....	4
Angriffstools	4
„Basis“ Bluetooth-Tools.....	6
Umgehungsmöglichkeiten Pairing.....	7
Bluescan.....	7
Tests mit Bluescan.....	8
Auswertungstabelle.....	8
Schutzmechanismen.....	11
Benutzerverhalten	11
Technische Schutzmechanismen.....	12

Einführung

Wenn in der näheren Vergangenheit von Viren oder Malware auf mobilen Endgeräten gesprochen worden ist, dann betrifft ein Teil sicherlich auch Angriffe über die Bluetooth-Luftschnittstelle. Diese Schnittstelle ermöglicht es mit relativ einfachen Mitteln Daten aus Geräten auszulesen, die sich in der Umgebung befinden. Als Beispiel von Daten können Telefonadressen, gespeicherte Termine oder die IMEI des Gerätes genannt werden. In ähnlichen Angriffen können sogar Textnachrichten, Bilder und Profile ausgelesen werden. Eine weitere Möglichkeit benutzt sogenannte AT-Befehle. Mit diesen kann die volle Kontrolle über das Endgerät erlangt werden. Das bedeutet, dass man über das angegriffene Gerät Nachrichten versenden, Telefonanrufe tätigen oder sonstige Daten einsehen kann. All diese Tätigkeiten gehen natürlich auf Kosten des Geräteinhabers. Für das Verständnis dieses Berichts ist es vor allem für Interessierte mit wenig IT-Kenntnissen nötig, dass im ersten Teil die Grundlagen von Bluetooth erklärt werden.

Nach Schätzungen des Marktforschungsunternehmens Frost & Sullivan¹ sind voriges Jahr 70 Millionen Bluetooth-Geräte verkauft worden. Die Marktforscher von Forrester Research² gehen davon aus, dass dieses Jahr sogar jedes fünfte verkaufte Handy bluetoothfähig ist.

Im Mobiltelefon-Bereich wird Bluetooth hauptsächlich für die Verwendung von drahtlosen Headphones und zur Synchronisierung der Daten mit dem PC benötigt. Bluetooth ermöglicht es verschiedene Endgeräte schnell und unkompliziert miteinander zu verbinden. Aus diesem Grund werden von den Herstellern je länger je mehr bluetoothfähige Geräte hergestellt und die Verbreitung dieser Technologie in den Endgeräten wird deshalb weiterhin rasant ansteigen.

Bluetooth Grundlagen

Bluetooth ist nicht die erste Technologie, die eine drahtlose Datenübertragung ermöglicht, doch sie ist sicherlich eine der Interessantesten. Sie stellt einen offenen Standard zur drahtlosen Kommunikation zwischen verschiedensten Endgeräten dar. Im Vergleich zu Infrarot benötigt Bluetooth keinen direkten Sichtkontakt. Zudem ist ein Bluetooth-Anschluss viel einfacher zu konfigurieren als zum Beispiel eine WLAN-Verbindung.

Technologie

Bluetooth wird im frei verfügbaren ISM-Frequenzband (2,4 GHz) betrieben. Das hat den grossen Vorteil, dass Bluetooth-Geräte überall auf der Welt betrieben und mit anderen Geräten vernetzt werden können. Die maximale Übertragungsrates liegt bei 1Mbit/s, welche sich alle im Piconetz befindlichen Geräte teilen müssen. Es können symmetrische Verbindungen von 434 kBit/s und asymmetrische mit 721/58 kBit/s aufgebaut werden. Es gibt in der Bluetooth-Spezifikation zwei unterschiedliche Verbindungsarten:

SCO: SCO (Synchronous Connection Oriented) Leitungsvermittelte Punkt-Punkt Verbindungen zwischen einem Master und den Slaves in einem Piconetz. Piconetze sind Ad Hoc-Netze mit maximal 8 Teilnehmern, wobei es einen Master und höchstens 7 Slaves gibt. SCO hat keine Fehlerkorrekturmöglichkeiten.

ACL: ACL (Asynchron Connectionless) ist paketvermittelt und dient als Vermittlung zwischen Master und allen aktiven Slaves, die am Piconetz teilnehmen. Punkt-Punkt oder Punkt-Mehrpunkt Konfiguration sind möglich. ACL bietet zudem Fehlerkorrekturmechanismen.

Der Bluetooth Standard schreibt 3 verschiedene Abstrahlleistungsklassen vor:

- Klasse 1: 100mW Sendeleistung, max. Distanz 100m im Freien
- Klasse 2: 2.5mW Sendeleistung, max. Distanz 10m im Freien
- Klasse 3: 1mW Sendeleistung, max. Distanz 2-3m im Freien

In den meisten Handygeräten wird Bluetooth mit der Abstrahlklasse 2 von 10 Metern implementiert.

¹ <http://www.frost.com/prod/servlet/press-de-press.pag>

² <http://www.forrester.com>

Bluetooth Protokolle

Hier werden nur die für diesen Bericht wichtigen Protokolle des Bluetooth Protokollstacks erläutert.

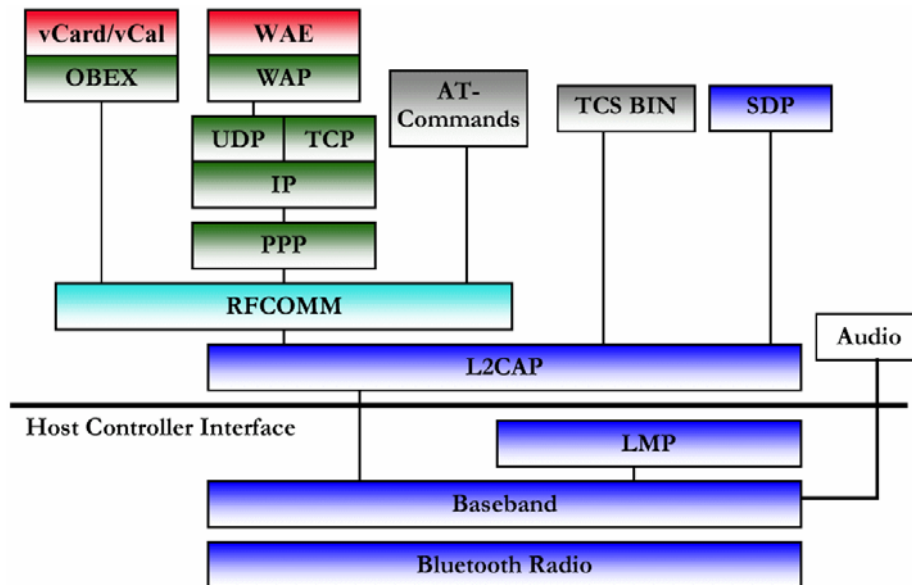


Abbildung 1: Bluetooth Protokollstack ¹

Der Bluetooth Protokollstack kann in vier grobe Schichten aufgeteilt werden, jede Schicht beinhaltet die folgenden Protokolle:

Layer	Protokolle
Bluetooth Kernprotokolle Kabelersatzprotokolle Telefonieprotokolle Adaptierte Protokolle	<i>Baseband, LMP, L2CAP, SDP</i> <i>RFCOMM</i> <i>TCS Binary, AT-commands</i> <i>PPP, IP, UDP/TCP, OBEX, WAP</i>

BT Radio	Die unterste Schicht im Stack spezifiziert die physikalischen Übertragungseinrichtungen des 2.4GHz ISM Frequenzbandes.
Baseband	Das Basisband (Schicht 1 Protokoll) ermöglicht die physikalische Funkverbindung zwischen Bluetooth-Geräten im Pico-Netz. Die Pakete für SCO und ACL werden zusammengesetzt, CRC gesichert und verschlüsselt.
LMP	Der Verbindungsauf- und abbau und die Kontrolle zwischen den Endgeräten gehört zu den Hauptaufgaben des LMP (Link Manager Protocol). Der ganze Sicherheitsmechanismus (Authentication, Encrypting-Decrypting) läuft ebenfalls über LMP. Zudem kontrolliert das Protokoll den Verbindungsstatus der Endgeräte und deren Energiemodi.
L2CAP	Das Logical Link Control and Adaptation Protocol ist für die Paketsegmentierung und Neuzusammensetzung zuständig, es unterstützt zudem das Multiplexieren der höheren Ebenen. Es unterstützt verbindungslose und verbindungsorientierte Services.
RFCOMM	Das Cable Replacement Protocol basiert auf dem ETSI Standard 7.10, es ist ein Serial Line Emulation Protokoll, das die serielle Schnittstelle RS-232 emuliert und somit eine Unterstützung für die höheren Protokollschichten wie zum Beispiel OBEX bietet.

¹ http://www-user.tu-chemnitz.de/~kirst/prosem/docs/b_prot2.htm

- SDP Das Service Discovery Protocol erlaubt eine Diensterkennung innerhalb des Bluetooth Systems. Damit können Geräteinformationen, Dienste und Leistungsmerkmale aller verfügbaren Dienste abgefragt werden.

- OBEX Obex ist ein Protokoll der Anwendungsschicht im Bluetooth Protokollstack. Es wird für den Austausch von Objekten benötigt. OBEX kann mit dem HTTP-Protokoll aus dem TCP/IP-Protokollstack verglichen werden. Es beinhaltet dieselben grundlegenden Funktionalitäten.

- AT-Befehle Der AT-Befehlssatz der Firma Hayes wurde ursprünglich zur Modemkommunikation entwickelt. Heute gilt er als anerkannter Industriestandard. AT-Befehle können auch über Bluetooth angewendet werden, um Steuerfunktionen auf einem entfernten Endgerät zu übernehmen.

Verbindungsmanagement

Der Link Manager, der in jedem Bluetooth Gerät eingebaut ist, regelt die Erkennung der Geräte. Die Nachrichten werden dabei mittels LMP versandt, die höher liegenden Schichten verwalten den Leitungsaufbau und die Kommunikation. Bei einer Bluetooth Verbindung gibt es immer einen Master und einen oder mehrere Slaves. Das den Verbindungsaufbau initialisierende Gerät ist dabei der Master, dieser steuert und beendet die Verbindungen.

Jedes Bluetooth Gerät enthält eine 48 bit lange Geräteadresse, die meist BD_ADDR genannt wird, sie ist weltweit eindeutig, und analog zur MAC-Adresse im PC-Bereich aufgebaut.

Gemeinsame Parameter

Gewisse Parameter werden für die Kommunikation zwischen zwei Geräten zwingend benötigt und müssen daher von allen Geräten unterstützt werden:

- Gerätename:** Der Gerätename kann nach Standard bis zu 248 Byte umfassen, normalerweise werden aber nur Gerätenamen bis max. 40 Byte unterstützt, da viele Displays der mobilen Geräte schlichtweg zu klein sind, um solch lange Namen vernünftig anzuzeigen.

- Pairing:** Zwei Geräte die erstmals miteinander kommunizieren, benötigen ein Initialisierungsverfahren. Dieses erzeugt einen gemeinsamen Verbindungscode, der für die nachfolgende Authentifizierung verwendet wird. Bei der erstmaligen Verbindung muss der Teilnehmer beim Pairing einen PIN eingeben, der dann vom Partnergerät bestätigt werden muss. Die folgende Grafik veranschaulicht den Pairing-Mechanismus.

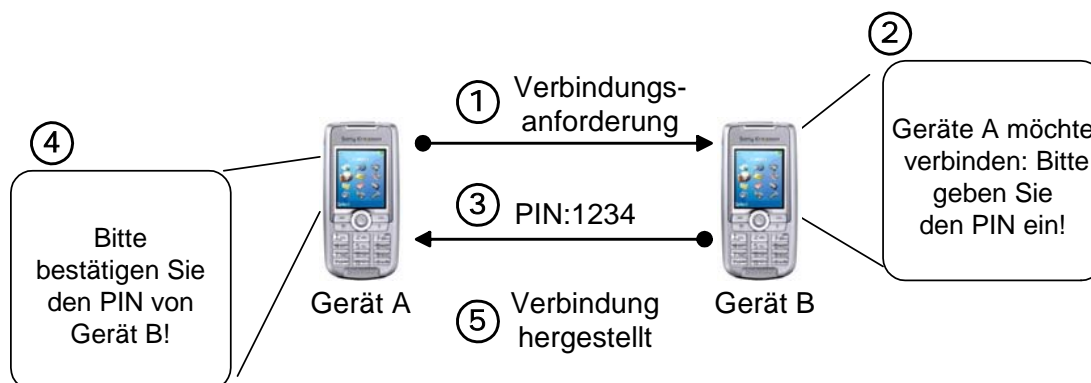


Abbildung 2: Pairing von zwei Geräten

- Sicherheitsmodi:** Für Bluetooth Endgeräte sind 3 Sicherheitsmodi möglich.
Sicherheitsmodus 1 leitet nie Sicherheitsprozeduren ein, er wird nur verwendet wenn keine sicherheitskritischen Anwendungen zum Einsatz kommen.
Sicherheitsmodus 2 leitet erst Sicherheitsprozeduren ein, wenn die Aufforderung zur Einrichtung eines Kanals empfangen wird, oder das Gerät selbst einen Kanal einrichten will.
 Im *Sicherheitsmodus 3* werden die Sicherheitsprozeduren eingeleitet bevor die Nachricht zur Bestätigung der Verbindungseinrichtung versendet wird
- Erkennungsmodi:** Die Bluetooth Geräte befinden sich entweder im „visible“ Modus, in dem sie von andern Geräten erkannt werden können, oder im „invisible“ Modus. In diesem sind sie für andere Geräte grundsätzlich nicht sichtbar.

Bluetooth Attacken

Die ersten Sicherheitslücken im Bereich von Bluetooth wurden von Adam Laurie und Martin Herfurt entdeckt. Adam Laurie von der A.L.Digital Ltd. bemerkte im November 2003 das erste Sicherheitsloch. Es betrifft die Authentication und den Datenübertragungsmechanismus bei Bluetooth Geräten. Die eigentliche Lücke besteht nur bei bestimmten Endgeräten. Sie löschen alte Paarung nicht sauber und ermöglichen trotz der Löschung der Paarung immer noch Verbindungen zu den zuvor gepaarten Geräten. Dadurch können Verbindungen ohne Benachrichtigung des Benutzers aufgebaut werden. Das Sicherheitsloch wird bei der Bluesnarf Attacke ausgenutzt. Über die Sicherheitslücke, die von Martin Herfurt in der Bluebug Attacke angewandt wird, ist nichts genaueres bekannt. Dasselbe gilt für die Sicherheitslücke, die bei der BTChaos Attacke angewandt wird. Wie diese Sicherheitslücken aussehen und wie sie ausgenutzt werden können, wurde bisher nicht veröffentlicht

Bekannt ist jedoch, dass es sich bei den ausgenützten Sicherheitslücken nicht um Fehler in der Bluetooth Spezifikation handelt. Sie entstanden vielmehr durch eine unsorgfältige Implementierung der Gerätehersteller. Im Folgenden werden einige mögliche Attacken genauer beschrieben.

Angriffstools

Nr.	Name	Entwickler	Verfügbarkeit
1	Bluesnarf	A.L.Digital, Adam Laurie	nicht veröffentlicht und nicht online verfügbar
2	BTChaos	Integralis, Michael Müller	nicht veröffentlicht und nicht online verfügbar
3	Bluebug	Austria Research, Martin Herfurt	nicht veröffentlicht und nicht online verfügbar

1. Bluesnarf Attacke

Das Wort Snarf stammt aus dem Hackerjargon. Es bedeutet ein Dokument oder eine Datei ohne Bewilligung des Eigentümers einzusehen. Im Frühling 2004 wurden die ersten Meldungen über Bluesnarf- bzw. Snarf Attacken veröffentlicht. Diese Angriffe nutzen das von Adam Laurie gefundene Sicherheitsloch aus. Bluesnarf ermöglicht es einem Angreifer, Daten aus dem Adressverzeichnis oder Kalender einzusehen, ohne dass der Eigentümer des Gerätes dies bemerkt. Mit den geeigneten Werkzeugen ist die Attacke bei Geräten im „invisible“ Mode möglich.

Gewöhnlich ist die Bluesnarf Attacke nur im Umkreis von rund 10 Metern zum Opfer möglich. Adam Laurie hat kürzlich aber Tests abgeschlossen, bei denen eine Bluesnarf Attacke über knapp 1 km erfolgreich verlief¹. Erstaunlich erscheint dies insbesondere, da der Bluetooth Standard eine maximale Übertragungsdistanz von 100 Metern vorsieht.

Angreifbare Geräte

Gemäss Angaben des Entwicklers wurden folgende Mobiltelefone erfolgreich mit Bluesnarf angegriffen.

Sony Ericsson: T68, T68i, R520m, T610, Z600, Z1010
Nokia: 6310, 6310i, 6750, 8910, 8910i

Eine detaillierte Liste mit getesteten Geräten ist auf der Webseite von A.L.Digital² auffindbar.

¹ <http://wireless.weblogsinc.com/entry/2983435022266434/>

² <http://www.thebunker.net/release-bluestumbler.htm>

2. BTChaos

Bei der Chaos Attacke wird eine vom Sicherheitsunternehmen Integralis ¹ entdeckte Sicherheitslücke in Bluetooth Handys ausgenutzt. Diese stammt nicht vom eigentlichen Bluetooth Standard, sondern entstand ebenfalls durch unsaubere Arbeit bei der Bluetooth Implementierung der Mobiltelefonhersteller. Gemäss Aussagen der Firma Integralis baut das Tool auf das Backup-Programm btxml.c auf und liest die Daten wie auch Bluebug mit AT-Befehlen aus den Mobiltelefonen aus.

Wie alle anderen Bluetooth Attacken funktioniert auch die Chaos Attacke nur wenn sich das Opfer im Umkreis von rund 10 Metern zum Angreifer befindet. Zum Ausführen der Attacke wird ein spezielles C-Programm sowie diverse frei erhältliche Software benötigt.

```

[root@cornholio btchaos-v0.41# ./btchaos
Searching...please stand by...
----- New Device Found -----
Class:      Cell Phone
BTADDR:    00:60:57:
BT-Name:   Dr.Schmidt
-----
Choose Option:
-----
1 = Read Phone Ident
2 = Read Phonebook
3 = Read SMS
4 = Read ALL
5 = Disrupt Phonecall
6 = Dial Number
7 = Send SMS
8 = DoS
9 = quit
6
Number to dial?:
090012341234
Thank you! Placing Voice Call to Number: 090012341234
    
```

Abbildung 3: C-Programm zur Ausführung einer Chaos Attacke ²

Ähnlich wie bei der Bluebug Attacke können mit der Chaos Attacke folgende Aktionen durchgeführt werden:

- Telefonanrufe umleiten
- SMS lesen und versenden

Angreifbare Geräte

Gemäss Angaben des Entwicklers konnten bei folgenden Mobiltelefonen erfolgreiche Angriffe mit BTChaos ausgeführt werden:

Sony Ericsson: T68i, T610
Nokia: 6310i, 6650

Eine detaillierte Liste mit getesteten Geräten kann auf der Webseite von Integralis ³ eingesehen werden.

3. Bluebug Attacke

Die Bluebug Attacke funktioniert ähnlich wie Bluesnarf. Das Besondere von Bluebug ist, dass sogenannte AT-Commands an das Opfergerät gesendet werden können. Mit diesen AT-Befehlen ist es beispielsweise möglich ein SMS zu versenden. Für den Gerätebesitzer ist das Senden einer solchen SMS nicht sichtbar und es wird auch nicht im Postausgang gespeichert. In seltenen Fällen fordern die SMS-Einstellungen einen Bericht über versandte Nachrichten. Dieser wird auf dem Empfängergerät generiert. In diesem Fall würde das Opfer einen Bericht einer SMS bekommen, die er nicht selbst geschrieben hat. Bei PDU-codierten Nachrichten kann durch das Setzen eines Flags kontrolliert werden, ob ein solcher Bericht gesendet wird oder nicht. Zudem kann mit der Bluebug Attacke dank der Möglichkeit Kurzmitteilungen zu versenden, die Telefonnummer des Opfergerätes

¹ http://www.integralis.de/media/press_releases/2004/250304.html

² http://www.xonio.com/features/feature_unterseite_11876679.html

³ http://www.integralis.de/media/press_releases/2004/120504OM.html

ausfindig gemacht werden. Bei allen anderen Bluetooth Attacken wird nur die spezifische BD_ADDR des Opfergerätes erkennbar. Laut Angaben von Martin Herfurt, dem Entwickler des Bluebug Angriffs, baut der SMS-Bereich seines Bluebug Angriffstools auf das öffentlich erhältliche PDUSpy¹ auf.

Mit dem AT-Befehlssatz können folgende Aktionen durchgeführt werden:

- Telefonanrufe tätigen (z.B. auf kostenpflichtige Nummern)
- SMS lesen oder versenden
- Telefonbucheinträge lesen, bearbeiten, löschen oder hinzufügen
- Verbindung ins Internet herstellen
- Das Gerät so manipulieren, dass es die Anrufe immer über einen bestimmten Service Provider ausführt (ähnlich wie PC-Dialer)

Angreifbare Geräte

Gemäss Angaben des Entwicklers konnten bei folgenden Mobiltelefonen erfolgreiche Angriffe mit Bluebug ausgeführt werden:

Sony Ericsson: T610
Nokia: 6310i
Motorola: V80, V600

Eine detaillierte Liste mit getesteten Geräten kann auf der Webseite von A.L.Digital² eingesehen werden.

„Basis“ Bluetooth-Tools

Nr.	Name	Entwickler	Verfügbarkeit
1	Redfang	@stake	Online verfügbar
2	BtScanner	Pentest Security Assurance	Online verfügbar
3	Btxml	Andreas Oberritter	Online verfügbar
4	Bluestumbler	A.L.Digital, Adam Laurie	nicht veröffentlicht und nicht online verfügbar

Beschreibung der Tools:

- 1) **Redfang:** Ermöglicht es mit einer Brute-force Attacke Geräte zu erkennen die Bluetooth auf „invisible“ geschaltet haben und eigentlich unsichtbar wären.³
- 2) **BtScanner:** Erkennt alle sichtbaren Geräte in der Umgebung und listet alle Details dieser auf, die ohne Pairing ausfindig gemacht werden können.⁴
- 3) **Btxml:** Kreiert ein Backup von persönlichen Daten, die sich auf dem Mobiltelefon befinden. Die Ausgabe erfolgt im XML-Format auf der Konsole des Rechners. Verbindung erfolgt via RFCOMM. Zusätzlich ermöglicht Btxml bei gewissen Endgeräten die Umgehung des Pairings.⁵
- 4) **Bluestumbler:** Erkennt alle sichtbaren Geräte und gibt den Namen, die Bluetooth-Adresse, die Signalstärke etc. aus. (ähnlich wie BtScanner)⁶

¹ <http://www.nobbi.com>

² <http://www.thebunker.net/release-bluestumbler.htm>

³ http://www.atstake.com/research/tools/info_gathering/

⁴ http://www.pentest.co.uk/cgi-bin/viewcat.cgi?cat=downloads§ion=01_bluetooth

⁵ <http://www.saftware.de/bluetooth/btxml.c>

⁶ <http://www.thebunker.net/release-bluestumbler.htm>

Umgehungsmöglichkeiten Pairing

Nr.	Name	Kurzbeschreibung
1	Bluejacking	Benutzer zur PIN-Bestätigung auffordern
2	Backdoor	Pairing unsichtbar schalten

1. Bluejacking

Bluejacking wird ein neuer, relativ ungefährlicher Trend genannt, der seit einiger Zeit an stark frequentierten Stellen wie Bahnhöfen, Flughäfen oder Messen verwendet wird. Bei einer Bluetooth-Verbindungsanforderung erscheint normalerweise die „Kennung“ oder der Name des Gerätes, das versucht eine Verbindung aufzubauen, auf dem Display des zweiten Gerätes. Bluejacker definieren nun die Kennung ihres Gerätes mit einem speziellen Namen, der mittels einer Verbindungsanforderung aufs Display des Opfergerätes gepusht wird. Diese Kennung kann bis zu 248 Zeichen lang sein, bei herkömmlichen Mobiltelefonen wird sie aber oft auf 40 Zeichen beschränkt. Hier ein kleines Beispiel:

Herzliche Gratulation, sie haben in unserem Swisscom-Wettbewerb 100 Gratisgesprächsminuten gewonnen! Geben Sie zur Aktivierung den PIN 1234 ein!

Zugegeben, es werden vielleicht nur wenig Benutzer auf so einen Trick einsteigen, aber die Möglichkeit besteht sicherlich!¹

2. Backdoor

Die Backdoor Attacke hat den Nachteil, dass zuerst ein physikalischer Zugriff aufs Gerät stattfinden muss. Bei diesem kann der Angreifer sein gepaartes Angriffsgerät auf dem Opfergerät manuell „unsichtbar“ schalten. Danach kann der Angreifer eine Bluetooth-Verbindung ohne Paarungsanforderung und somit für das Opfer nicht erkennbar aufbauen.

Bluescan

Auf der Grundlage des Basistools btxml.c entstand Bluescan. Die Grundfunktionen von btxml.c wurden übernommen. Der grösste Unterschied zu btxml.c betrifft die Ausgabe der Daten. Sie erfolgt nicht mehr im XML-Format, sondern in einer für die Konsole optimierten Darstellung. Dadurch können die ausgelesenen Daten einfacher aufgefunden und bearbeitet werden.

Das Auslesen der Daten funktioniert mit dem Nokia 6310i und dem Sony Ericsson T610 vollumfänglich. Bei diesen Telefonen können das Telefonbuch, die Versionsnummer, die IMEI und alle Kurznachrichten ausgelesen werden. Das Sony Ericsson T68i erlaubt zwar keine Ausgabe der Kurznachrichten. Alle anderen Daten können aber auch mit diesem Telefon ausgelesen werden. Auf eine zusätzliche Auflistung der Testresultate wird hier verzichtet, sie können aus der Auswertungstabelle des Bluescan-Tests entnommen werden.

Bluescan wurde für die folgenden Testreihen auf einem Slackware Linux² der Version 9.1 mit BlueZ Protokollstack³ installiert. BlueZ ist der meistverbreitetste Protokollstack für Linux-Betriebssysteme und wird benötigt um eine Bluetooth Verbindung herzustellen. Zudem wird ein Bluetooth Dongle benötigt. Hierfür wurde das Lowcost Bluetooth-Dongle Modell MSI Bluetooth PC2PC verwendet.

Folgende Pakete werden für den BlueZ Protokollstack benötigt:

bluez-libs 2.10	http://www.bluez.org/download.html
bluez-utils 2.10	http://www.bluez.org/download.html
bluez-sdp 1.5	http://bluez.sourceforge.net/download/
bluez-pin 0.24	http://www.bluez.org/download.html

¹ <http://www.bluejackq.com/>

² <http://www.slackware.com>

³ <http://www.bluez.org/>

Tests mit Bluescan

Bluescan wurde auf verschiedenen Geräten auf seine Funktion getestet. Es folgt eine kurze Erklärung der jeweiligen Punkte, die auf den verschiedenen Telefonen getestet wurden und die in der weiter unten folgenden Auswertungstabelle aufgeführt sind.

Beschreibung

Unter diesem Punkt können spezifische Angaben des Mobiltelefons ausgelesen werden. Dazu gehören: Angabe des Herstellers, die genaue Modellbezeichnung, die Version und die IMEI des Gerätes.

Adressspeicher

Es können alle Adressbucheinträge, die sich im Telefon- als auch im SIM-Speicher befinden, ausgelesen werden.

Anruflisten

Die gesamte Anrufliste mit erhaltenen, getätigten und verpassten Anrufen kann ausgelesen werden.

SMS auslesen

Es können sowohl im Telefon- als auch im SIM-Speicher enthaltene Kurzmitteilungen ausgelesen werden.

Version

Enthält die Firmware Version der getesteten Geräte. Die Version kann bei Sony Ericsson Geräten mit der Tastenfolge -> * <- <- * <- * angezeigt werden. <- und -> stehen dabei für Joystickbewegungen nach links bzw. rechts (beim P900 stehen die Pfeile nach links für Rotationen des Jog Dials (oben rechts) nach unten bzw. rechts nach oben). In den nun angezeigten Menüs wird die Version unter *Service Information/SW Informationen* angezeigt. Bei Nokia Modellen kann die Software Version durch tippen von *#0000# angezeigt werden.

Auswertungstabelle

Bezeichnung	Beschreibung	Adressspeicher	Anruflisten	SMS auslesen	Version
Sony Ericsson P900					R3c006 ^I
Sony Ericsson K700i					R2A041
Sony Ericsson T610	x ^{II}	x	x	x	R1A081 ^{III}
Sony Ericsson T68i	x ^{II}	x			R6A012 ^{IV}
Nokia 6650					V 04.02
Nokia 6310 ^V	x	x	x	x	V 5.10

^I Bluetooth Version: CXC12529 R5D

^{II} In der Beschreibung fehlt die Ausgabe der IMEI Nummer

^{III} Ebenfalls getestete Version, die keine Auslesung ermöglichten: R6C005,

^{IV} Ebenfalls getestete und funktionierende Version: R2E006

^V Nach 10 Sekunden wird die Bluetooth Verbindung zum Nokia 6310 getrennt

Die Resultate zeigen klar auf, dass nicht alle Modelle mit Bluescan angegriffen werden können. Insbesondere die Versionsnummern der getesteten Sony Ericsson T610 ermöglichen den Schluss, dass nur Mobiltelefone mit älteren Software Versionen angreifbar sind. Die Implementierung des Bluetooth Protokollstacks scheint also von den Herstellern verbessert worden zu sein. Für gewisse Nokia Endgeräte sind die seit dem Frühjahr versprochenen Firmware Updates seit Ende September erhältlich. Genauere Informationen hierzu können direkt der Nokia Sicherheitsupdate Webseite¹ entnommen werden.

¹ <http://www.nokia.com/nokia/0,1522,,00.html?orig=/bluetoothsecurity>

Der folgende Printscreen der Anwendung zeigt einen Ausschnitt der Ausgabe und gibt somit einen Einblick in das Tool Bluescan:

```

root@slackware:/opt/bluescan# ./bluescan.out

*****
*****
*****          BLUESCAN  V 1.0          *****
*****
*****          developed by Claudio Beltrametti & Reto Calonder          *****
*****          thesis diploma autumn 2004          *****
*****          *****
*****          *****
*****          *****

...Beginn des Scanvorgangs...

GERÄTE-ADRESSE:  00:60:57:04:83:A5      NAME:    A6310i
HERSTELLER      Nokia                 MODELL:  Nokia 6310i
VERSION:        V 5.10  11-09-02 NPL-1 (c) NMP.
IMEI:           350984209924357

-----
EINTRÄGE IM TELEFONSPEICHER           Grösse="500"

      NAME          NUMMER
-----
      Claudio B     0796985157
      Reto Calonder  0793536343
      Bahnhof Disentis +41819475132
      Concordia Notdienst +41446551126
      Claudio        0794652136

-----
GEWÄHLTE RUFNUMMERN                   Grösse="20"

      NAME          NUMMER
-----
      Reto Calonder  0793536343

-----
VERPASSTE ANRUFEN                       Grösse="10"

      NAME          NUMMER
-----
      Claudio B     0796985157

-----

```

```

-----
ANGENOMMENE ANRUFE                               Grösse="10"
      NAME                NUMMER
-----
      Reto Calonder       +41793536343
-----

EINTRÄGE AUF SIM-KARTE                           Grösse="150"
      NAME                NUMMER
-----
      Hotline CH         +41800556464

SMS IM TELEFONSPEICHER:

NACHRICHT: "REC READ","30927",,"04/09/02,13:56:44+08" Ihr Konfigurationscode ist: 6319

SMS IM SIM SPEICHER:

NACHRICHT: "REC READ","+41796985157",,"04/09/15,15:16:43-00" test cb www.sunrise.ch
NACHRICHT: "REC READ","+41796985157",,"04/09/15,16:33:55-00" test nokia 6230
NACHRICHT: "REC READ","+41796985157",,"04/09/20,14:10:53+00" test sms Hallo

...Vorgang abgeschlossen... Auslesen des Gerätes beendet!...
  
```

Zu Beginn der Ausgabe werden allgemeine Daten über das Endgerät aufgelistet. Danach erfolgt die Ausgabe aller sich im Speicher befindlichen Daten. Die Auslesung dieser Daten erfolgt dabei über AT-Befehle. Bei Bluescan wird der AT-Befehl CPBR benutzt.. Die genaue Verwendung dieses Befehls wird in der Source des Programms ersichtlich. Alle Befehle sind dabei nach folgendem Grundschema aufgebaut:

AT+CPBR [=index]

In den Klammern mit index wird ein zusätzlicher Wert eingefügt, der genauer spezifiziert, was aus dem Telefonspeicher ausgelesen werden soll. Mit dem Befehl AT+CPBR=ME werden beispielsweise nur Telefonbucheinträge, die sich auf dem Telefonspeicher befinden ausgelesen. Es folgt eine komplette Auflistung der im Bluescan Programm verwendeten CPBR-Zusätze zur Auslesung des Telefonspeichers:

ME	Mobile Equipment Telefonbucheinträge des Gerätespeichers
SM	SIM Memory Telefonbucheinträge des SIM-Speichers
DC	Dialed Calls Anrufliste mit den gewählten Rufnummern
MC	Missed Calls Anrufliste mit den verpassten Anrufen
RC	Received Calls Anrufliste mit den angenommenen Anrufen
MV	Voice activated dialing list Telefonnummern, die über Sprachbefehle angewählt werden können
LD	Last dialed Numbers Wahlwiederholungsspeicher

FD SIM fixed dialing memory
Nummern die Fest auf der SIM gespeichert sind, z.B. die Hotline-Nummer des Mobilfunkbetreibers

Die Kurzmitteilungen können analog zum Telefonspeicher mit folgendem AT-Befehl ausgelesen werden:

AT+CMGR [=index]

Für index existieren dabei folgende Zusätze:

ME Mobile Equipment
Kurznachrichtenspeicher auf dem Gerät

SM SIM Memory
Kurznachrichtenspeicher auf der SIM-Karte

Schutzmechanismen

Neben den Bluetooth Attacken sind auch die ersten Malwareprogramme im Umlauf und es ist nur noch eine Frage der Zeit, bis es zu grösseren Ausbreitungen solcher Programme kommt. Deshalb sind geeignete Schutzmassnahmen zu treffen, damit die Benutzer solche Attacken unbeschadet überstehen.

Um sein eigenes Gerät zu schützen sind nicht nur technische Massnahmen wichtig, es geht vielmehr auch darum, sein eigenes Verhalten der Situation anzupassen. Dies kann genauso viel bewirken wie teure technische Hilfsmittel. Die Schutzmechanismen werden deshalb in zwei Hauptkategorien eingeteilt. Zum einen kann das eigene Verhalten dazu beitragen, einen gewissen Schutz aufrecht zu erhalten und zum anderen kann der Schutz mittels technischer Hilfsmittel wie Antivirenprogrammen erhöht werden.

Benutzerverhalten

Vielen Benutzern sind die verschiedenen Angriffspunkte eines mobilen Endgerätes gar nicht bekannt, da sie nur wenige Funktionen ihres Gerätes wirklich brauchen. Bei Handys ist die Hauptfunktion beispielsweise das Telefonieren und andere Funktionen wie etwa Bluetooth kennen viele Benutzer überhaupt nicht. Zudem werden verschiedene Technologien von den Herstellern so vorkonfiguriert, dass sie eine möglichst einfache Bedienung der jeweiligen Funktion erlauben. So wird beispielsweise die Bluetooth Schnittstelle von den Herstellern standardmässig auf „visible“ (sichtbar) vorkonfiguriert. Der Benutzer weiss meist nicht was das bedeutet, da er diese Technologie kaum benötigt und er kennt meist auch die Gefahren nicht, die damit verbunden sind. Es ist deshalb wichtig, die gängigsten Funktionen des Gerätes kennen zu lernen.

Es folgen ein paar Regeln, die die Sicherheit des Gerätes durch einfaches Verhalten um einiges erhöhen können:

- Nicht benötigte Funktionen wie Bluetooth immer ausschalten und nur bei Gebrauch einschalten. (Schont zudem den Akku!)
- Die Sichtbarkeit des Gerätes für Bluetooth auf „invisible“ stellen
- Gepaarte Geräte nach Gebrauch wieder entpaaren
- Unbekannte Verbindungsaufforderungen immer ablehnen
- Nie unbekannte Programme auf dem Endgeräten ausführen
- Nur E-Mail-Anhänge von bekannten Personen öffnen.
- Bluetooth-Pairing PIN und andere PIN wenn möglich mit 6 oder 8 Zeichen wählen
- Endgeräte nicht unbeaufsichtigt liegen lassen
- Besonders vorsichtiger Gebrauch von Bluetooth in öffentlichen Räumen mit vielen Personen.
- Ungeschützte PDA's nicht mit dem Firmennetz verbinden.

Sofern die Bluetooth-Funktion ganz ausgeschaltet ist, können keinerlei Angriffe über die Bluetooth Schnittstelle auf das Gerät durchgeführt werden. Dasselbe gilt auch für andere Funktionen. Um eine Bluetooth Verbindung aufzubauen, wird ein sogenanntes Pairing durchgeführt. Der dabei verwendete

Pincode ist ein sehr entscheidender Faktor für die Sicherheit einer Bluetooth Verbindung. Wenn dieser Code wie vielfach üblich nur vier Zeichen enthält, kann er in weniger als einer Sekunde geknackt werden, bei sechs Zeichen dauert es schon ca. zehn Sekunden, für einen 16-stelligen Pincode sind ungefähr 2700 Jahre notwendig. Beinahe alle Hersteller von mobilen Endgeräten ermöglichen aber nur die Eingabe von vierstelligen PIN's, obwohl seit längerem Tools frei erhältlich sind, die diesen PIN mittels Brute-force-Angriffe knacken können (Redfang).

Technische Schutzmechanismen

Für Bluetooth-Angriffe sind technische Schutzmechanismen weniger von Bedeutung. Anders sieht dies jedoch bei Malware aus. Diese gibt es trotz anderer Berichte bereits für PDA's und normale Mobiltelefone. Deshalb wird es zunehmend wichtig für diese Geräte auch funktionierende Sicherheitslösungen zu installieren. Dazu gehört natürlich eine Antivirus-Software, wie sie bereits den meisten Leuten vom PC-Bereich her bekannt ist. Diese muss regelmässig aktualisiert werden, damit sie auch etwas nützt. Eine Firewall wird bei zunehmender Bedrohung auch für mobile Geräte bald ein Muss. Des Weiteren ist auf eine sichere Verschlüsselung der versendeten Daten zu achten.

Den hundertprozentigen Schutz gibt es nicht, aber mit einem relativ kleinen Aufwand lässt sich in Sachen Sicherheit schon sehr viel machen.