D·A·CH Mobility 2006

Bluetooth-Sicherheit

Schwachstellen und potenzielle Angriffe

Dr.-Ing. Kai-Oliver Detken
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Prof. Dr.-Ing. Evren Eren
URL: http://www.inf.fh-dortmund.de/eren
E-Mail: eren@fh-dortmund.de

Consultancy & Internet Technologies

Inhalt

- Technologie-Randbedingungen
- Schwachstellen
  - Designschwächen
  - Angriffe
- Bewertung
  - Anpassung der Konfiguration
  - Sicherheitsempfehlungen
  - Auffinden von Bluetooth-Geräten
- Fazit

Technologie-Randbedingungen (1)

- Bluetooth-Geräte senden als Short Range Devices im lizenzfreien ISM-Band zwischen 2,402 GHz und 2,480 GHz
- Störungen können z.B. durch WLAN-Netze, schnurlose (drahtlose) Telefone, Garagentoröffner oder Mikrowellenherde verursacht werden, die im gleichen Frequenzband arbeiten
- Um Robustheit gegenüber Störungen zu erreichen, wird ein Frequenzsprungverfahren (Frequency Hopping) eingesetzt, bei dem das Frequenzband in 79 Frequenzstufen im 1-MHz-Abstand eingeteilt wird, die bis zu 1600 Mal in der Sekunde gewechselt werden
- Am unteren und oberen Ende gibt es jeweils ein Frequenzband als Sicherheitsband (Guard Band) zu benachbarten Frequenzbereichen

Technologie-Randbedingungen (2)

- Theoretisch kann eine Datenübertragungsrate von 1 MBit/s beim Download bei gleichzeitigen 57,6 kBit/s beim Upload erreicht werden
- Seit der Version 2.0 können Daten durch EDR (Enhanced Data Rate) maximal etwa dreimal so schnell übertragen werden, also mit rund 2,1 MBit/s
- Bereits seit Version 1.1 kann ein Bluetooth-Gerät gleichzeitig bis zu sieben Verbindungen aufrechterhalten, wobei sich die beteiligten Geräte die verfügbare Bandbreite teilen müssen (shared medium)
- Bluetooth unterstützt die Übertragung von Sprache und Daten
- Eine Verschlüsselung der transportierten Daten ist ebenfalls möglich

Schwachstellen

- Die Schwachstellen lassen sich in zwei Bereiche kategorisieren:
  - Schwächen im Design des Sicherheitskonzepts
  - Schwachstellen in den Implementierungen und sowie mögliche Risiken, die sich aus dem Zusammenhang der Bluetooth-Anwendungen ergeben

Designschwächen

- Verschlüsselung ist bei Bluetooth nicht grundsätzlich vorgeschrieben
- In der Bluetooth-Spezifikation werden keine Anforderungen an den Zufallsgenerator gestellt und er wird unzureichend definiert
- Im Bluetooth-Standard liegt keine Beschreibung vor, wie der Unit Key im Gerät gespeichert werden soll
- Die Länge des Sitzungsschlüssels (Encryption Key) ist variabel und kann weniger als 128 Bit betragen
- PIN-Codes, die eine zu geringe Länge aufweisen (4stellig), können während des Pairing-Prozesses abgehört werden
- In der Bluetooth-Spezifikation ist das Verhalten des Geräts für den Fall, dass es sich aus der Sendereichweite eines gepairten Endgeräts wegbewegt, nicht definiert (Bewegungsprofile)

Sicherheitsmodi

- Da alle Sicherheitsdienste in der Datenübertragungsschicht (Layer 2) angesiedelt sind, ist bei Bluetooth keine Ende-zu-Ende-Sicherheit möglich
- Nur einzelne Verbindungen werden verschlüsselt und authentisiert
- 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

Zusammenfassen der Designschwächen

Angriffe	Vertrau-lichkeit	Integrität	Verfüg-barkeit	Verbind-lichkeit	Authenti-zität	Verläss-lichkeit
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

Angriffe

- **Lokalisierung:** Standort des Zielgeräts herausfinden
- **Bluesnarf:** Firmware-Bugs werden genutzt, um Adressverzeichnisse einzusehen
- **BTChaos:** Es werden Daten mit AT-Befehlen ausgelesen; Daten können geschrieben werden
- **Bluebug:** mittels AT-Befehle können SMS gesendet werden
- **PIN:** Attacke auf den PIN Code
- **Spoofing:** Geräteschlüssel wird als Angriffsmedium verwendet
- **Bluejacking:** es werden unerwünschte Nachrichten versendet
- **Bluesniping:** Attackieren aus großer Entfernung
- **Bluetooth Wardriving:** Verfolgung von Benutzerbewegungen
- **Location-Tracking:** Lokalisierung innerhalb von Hotspots
- **Denial-of-Service:** ständige Kommunikationsabfragen, um das Bluetooth-Gerät zu belasten
- **Man-in-the-Middle:** Pakete abfangen und manipulieren
- **Re-Pairing:** Pairing-Prozess wird erzwungen, um Attacke zu fahren
- **Backdoor:** Zugriff über Invisible-Mode ohne Kenntnisnahme des Benutzers
- **Brute-Force:** 4stelliger PIN kann abgeleitet werden, um daraus den Link Key zu ermitteln

Zusammenfassung der Angriffe (1)

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 Tracking	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					

Zusammenfassung der Angriffe (2)

- Die am meisten genannten Bedrohungen beziehen sich auf die Bluetooth-Schnittstelle. Angriffe nutzen dabei die Sicherheitslücken in instabilen Implementierungen des Bluetooth-Protokollstacks
- Viele Sicherheitseinstellungen sind nur optional nutzbar, so dass durch die Nichtnutzung oder durch schlechte Implementierungen Sicherheitslöcher entstehen
- Eine weitere Schwäche ist die eindeutige Geräteadresse, die nicht nur zum Verbindungsaufbau verwendet wird. Es lassen sich daher Bewegungsprofile erstellen.
- Durch Kombinationen (Object Push, Synchronisation, IrDA, Bluetooth und OBEX) werden Sicherheitslücken offen gelegt

Bewertung

- Der Benutzer von Bluetooth-Geräten hat keine Informationen über die korrekte Implementierung vorhandener Sicherheitstechniken (z.B. Authentifizierung)
- Es können Bewegungsprofile erstellt werden. Es ist dadurch möglich, mittels eines dichten Netzes von Bluetooth-Geräten, regelmäßig die Umgebung nach neuen unbekannten Geräten durchzusuchen
- Es wäre generell zu empfehlen, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und gegebenenfalls anzupassen
- Mobile Geräte, die sich mit fremden Geräten beziehungsweise mit Geräten unterschiedlicher Benutzer verbinden, müssen besonders abgesichert werden

Anpassung der Konfiguration (1)

- 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

Anpassung der Konfiguration (2)

- 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 notwendig. Allerdings sollten diese in abhörgefährdeten Umgebungen authentisiert verschlüsselt betrieben werden. Auch die Länge des PIN-Codes sollte über die minimal empfohlene PIN-Länge hinausgehen

Sicherheitsempfehlungen

- 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 Security Policys 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 sollten 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

Auffinden von Bluetooth-Geräten

- Für Unternehmen sollten insbesondere Softwarelösungen zur Identifikation von Bluetooth-Geräten Einsatz finden
- 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

Zusammenfassung

- Für eine gewisse Basissicherheit sollte eine einmal erkannte Gegenstellen dauerhaft in den jeweiligen Authentifzierungslisten gespeichert und eine Re-Authentifizierung per PIN deaktiviert werden
- Außerdem sollten Benutzer PINs mit deutlich mehr als vier Zeichen Länge verwenden, falls die verwendete Software dies gestattet. Das Bluetooth-Protokoll sieht bis zu 16 beliebige Zeichen (128 Bit) vor!
- Darüber hinaus sollte eine unerwartete Aufforderung zur erneuten Authentifizierung hellhörig machen und zur Vorsicht mahnen

Danke für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 1
D-28359 Bremen
Germany
Phone: +49-421-2208-185
Fax: +49-421-2208-150
E-Mail: detken@decoit.de

Consultancy & Internet Technologies