

# Mobile Security: Bluetooth & IEEE-Standard 802.11

## Einleitung

Eine kürzlich veröffentlichte Studie der Gartner Group spricht davon, dass 50% aller Unternehmen planen, in Zukunft ein kabelloses Netzwerk zu unterhalten. Des Weiteren geht man bei Gartner davon aus, dass bereits 20% dieser Unternehmungen in irgend einer Art und Weise ein solches „mobiles“ Netzwerk eingerichtet haben. In einigen Fällen wurden diese Technologien aber mit der Motivation, nicht auf ausgereifte Lösungen warten zu wollen, implementiert. Dies führt dazu, dass in solchen Situationen eher von unsicheren Testinstallationen gesprochen werden kann, als von grossen nutzenbringenden und zugleich sicheren Infrastrukturen. Dieser Umstand führt zu gewissen Sicherheitsproblemen.

Das Sicherheitsbewusstsein im Bereich der mobilen Netzwerke ist zumal auf Entwickler- und Anbieterseite vorhanden, im Vergleich dazu fehlt es jedoch auf Anwenderseite zum Teil gänzlich. Die Zugangs-Sicherheit von verkabelten Netzwerken wird zum einen durch die physische Lokation des Kabels innerhalb eines Gebäudes definiert und zum anderen durch den logischen Schutz, welcher durch entsprechende Systeme, wie Netzwerkkomponenten und Firewalls sichergestellt wird. Der physische Schutz verhindert in den meisten Fällen, dass nicht autorisierte Dritte Zugang zum entsprechenden Netzwerk erhalten. Als physischer Angriffspunkt bietet sich oftmals nur die Zulieferleitung, welche den lokalen Netzwerkbetreiber mit Drittnetzen verbindet, so zum Beispiel dem Internet. Der Aufwand, die Ausrüstung sowie das notwendige Fachwissen verhindern es, dass solche Leitungen in grossem Masse angezapft werden. Einen solchen Angriff zu 100% ausschliessen, kann man aber trotzdem nicht.

Im Vergleich dazu ist es notwendig, beim Betrieb einer mobilen Infrastruktur (Netzwerk) die Sicherheitsüberlegungen über die eigenen vier Wände hinaus auszudehnen. Die Daten werden in einem bestimmten räumlichen Umkreis offen übertragen und sind somit für jede Person mit der entsprechenden Ausrüstung empfangbar. Die Empfangsqualität und die Reichweite solcher Funksignale wird durch Gebäudeschatten sowie Bauweisen, welche analog einem Faradaykäfig gleichkommen, beeinträchtigt. Von zusätzlicher Sicherheit kann hierbei aber bei weitem nicht gesprochen werden.

Um von einer sicheren Kommunikation ausgehen zu können, ist es wichtig, den Kommunikationskanal so auszulegen, dass dieser die notwendige Vertraulichkeit garantieren kann. Im Bereich „Wireless Networking“ zeichnet es sich ab, dass sich zwei Standards durchsetzen werden. Zum einen ist dies der IEEE-Standard 802.11 und zum anderen der Bluetooth-Standard. Beide Technologien haben zum Ziel, portable Geräte wie Mobiltelefone, PDA's (Personal Digital Assistants) sowie Laptops miteinander zu verbinden, so dass eine unkomplizierte und insbesondere drahtlose Kommunikation ermöglicht wird. Dieser Aspekt unterstützt unter anderem den einfachen Aufbau von sogenannten „Adhoc-Netzwerken“.

### Bluetooth

Die Bluetooth-Technologie ist eher darauf ausgelegt mobile Geräte miteinander zu verbinden, bei welchen keine grossen Bandbreiten zur Datenübertragung notwendig sind, da sich die Datenmengen in Grenzen halten. Im Vergleich dazu unterstützt der Standard 802.11 vielmehr den Austausch grosser Datenmengen und ist somit eine vertretbare Alternative zum bekannten Netzwerk bestehend aus Kabeln.

Die Sicherheitsbedürfnisse sind in beiden Fällen sehr ähnlich. Die Bluetooth-Technologie beinhaltet bereits Authentisierungs- und Chiffriermöglichkeiten. Zur Chiffrierung der Kommunikation müssen zwei Bluetoothgeräte beim ersten Kontakt einen gemeinsamen Schlüssel vereinbaren. Hierbei gibt es einige Sicherheitsüberlegungen, welche nicht ausser acht gelassen werden können. Zur Chiffrierung sind zwei Schlüssel notwendig, zum einen der „InitKey“ und zum anderen der „LinkKey“. Der „InitKey“ wird von beiden Bluetoothgeräten mittels der folgenden Funktion ermittelt:

$$\text{InitKey} := f(\text{PIN}, \text{Bluetoothadresse}_{\text{Empfänger}}, \text{Zufallszahl})$$

Die PIN wird vom Benutzer eingegeben und kann bis 128 Bit gross gewählt werden. Wichtig hierbei ist anzumerken, falls keine PIN verwendet wird, ist dieser Wert gleich Null. Da der Sender und der Empfänger den „InitKey“ mit der gleichen Funktion berechnen, muss die Zufallszahl unchiffriert übertragen werden, dabei wird auch die Bluetoothadresse bekannt gegeben. Die ganze Sicherheit hängt somit am „dünnen Faden“ der PIN, was eher bedenklich ist. Anschliessend wird der „LinkKey“ generiert, welcher für die Chiffrierung der Datenkommunikation sowie für die Authentisierung verwendet wird. Wird eine qualitativ schlechte (kurze) PIN verwendet, so kann der „Linkkey“ durch eine „brute force“-Attacke geknackt werden.

Die Authentisierung basiert auf dem „LinkKey“, da dieser permanent gespeichert wird und jederzeit zur späteren Authentisierung wieder einsetzbar ist. Dieser Umstand wird wichtig, wenn davon ausgegangen wird, dass Bluetoothgeräte hauptsächlich in „Adhoc-Netzwerken“ zusammengeschlossen werden. Jede Person besitzt nun eine gewisse Anzahl Bluetoothgeräte, welche sie zusammen in einem Personal Area Network (PAN) verbindet und einen offenen Datenaustausch ermöglicht. Um den unautorisierten Zugriff auf das eigene PAN zu schützen, wird ein sogenanntes „Frequenzhopping“ durchgeführt. Dies bedeutet, dass das Übertragungssignal von einer Frequenz zur nächsten springt und dies genau 1600 mal pro Sekunde. Für einen Angreifer wird es somit schwierig vorauszusagen, nach welchem Muster gesendet wird. Mit der entsprechenden technischen Einrichtung sollte er aber in der Lage sein, die benutzten Kanäle zu überwachen, um so die Kommunikation belauschen zu können.

Bluetooth bietet auch die Möglichkeit für sogenannte „Location attacks“. Hierbei kann ein Angreifer an verschiedenen Orten Bluetoothgeräte verteilen, welche wie Sonden jeden Passanten mit einem solchen Gerät in der Tasche über seine Bluetoothadresse identifizieren könnten. Die Voraussetzung dazu wäre, dass das zu überwachende Gerät sich im sogenannten „discoverable“ Modus befinden würde. Was heutzutage bezüglich Ortung von Abonnenten nur Mobiltelefonnetzbetreibern vorbehalten wäre, würde plötzlich jedermanns Sache sein können.

### IEEE-Standard 802.11

Auch der IEEE-Standard 802.11b (die „b“-Gruppe war gegenüber der „a“-Gruppe schneller bei der Entwicklung und so hat sich dieser durchgesetzt) bietet genügend potentielle Risiken. Da es sich um eine neuere Technologie handelt, steht vielerorts nicht die Sicherheit im Vordergrund, sondern die grundlegende Problematik eine Infrastruktur einfach zu betreiben. So ist es dann auch nicht verwunderlich, wenn ein grosser Teil solcher Betreiber, von kabellosen Netzwerken, die zur Verfügung stehenden Sicherheitseigenschaften nicht eingeschaltet haben. Der IEEE-Standard 802.11 bietet zwei wesentliche sicherheitsunterstützende Funktionen an. Zum einen ist dies die Authentisierung eines mobilen Gerätes gegenüber dem Netzwerkzugangspunkt (access point) und zum anderen ist dies die Möglichkeit, den Datenverkehr zwischen diesen beiden Punkten zu chiffrieren. Der verwendete Chiffrieralgorithmus nennt sich WEP (Wired Equivalent Privacy). Dieser definiert analog seinem Namen einen für „Wireless Networks“ äquivalenten Sicherheitsstandard zu jenem verkabelter Netzwerke.

Die Autorisierung kann auf verschiedenen Daten basieren, so zum Beispiel indem die Ethernet-Adresse (MAC-Adresse) der entsprechenden Karte oder die definierte IP-Adresse verifiziert wird. Authentisieren kann sich ein mobiles Gerät mittels korrekter Chiffrierung eines vom access point definierten Authentisierungscode (challenge).

Der hier verwendete Chiffrieralgorithmus stellt eine massive Schwachstelle dar. Dieses Kryptosystem ermöglicht es einem Angreifer nach einiger Zeit die gesendeten Daten zu dechiffrieren. Der Erfolg dieser Attacke ist abhängig von der gesendeten Datenmenge sowie der verwendeten Schlüssellänge für den WEP-Algorithmus. Eine entsprechende Software kann zur Analyse des Datenverkehrs und zur anschliessenden Dechiffrierung im Internet frei heruntergeladen werden.

Oftmals ist das Dechiffrieren von Daten jedoch gar nicht nötig, da keine Authentisierung und Chiffrierung eingeschaltet ist. Infolgedessen reicht es, mit dem Auto durch die Stadt zu fahren und zu sehen, wo ein entsprechendes Signal für einen Netzwerkzugang identifizierbar ist (war driving). Anschliessend wird dem Angreifer in den meisten Fällen automatisch eine Netzwerkadresse vergeben und er ist unautorisiert Teil eines lokalen privaten Netzwerkes. Neben dem, dass er unter Umständen weitreichenden Datenzugriff erlangen kann, hat er meistens auch die Möglichkeit, über den Internetzugang der entsprechenden Unternehmung anonym sich im Internet zu betätigen. Vorstellbar hierbei sind weitergehende Angriffe (Hacking-Attacken). Sehr einfach wird es auch für Privatpersonen gratis und anonym einen Internetzugang zu erhalten, sofern der Nachbar über einen „Wireless Access Point“ verfügt. Den direkten Schaden erleiden die Internetdiensteanbieter (Internet Service Providers). Existiert ein solcher ungesicherter „Wireless Access Point“, wird es für dessen Betreiber unmöglich sein, in Rechtstreitigkeiten beweisen zu können, dass jemand Dritter über seinen Zugang illegale Aktivitäten ausgeführt hat.

Neben den Sicherheitsaspekten dieser Wireless-Technologien beeinflusst die implementierte Sicherheit des entsprechenden mobilen Gerätes die gesamte Sicherheit in grossem Masse. Ein zentraler Punkt hierzu ist die Virenproblematik. Wird der Benutzer die Möglichkeit haben, auf seinem Handy eine Firewallsoftware zu installieren, welche ihm einen Schutz vor Viren sowie „Denial of Service“-Attacken bietet? Mit solchen und anderen Fragestellungen wird sich die zukünftige Wireless-Technologie sicherlich noch vermehrt auseinandersetzen müssen. Generell lässt sich sagen, dass momentan sowohl bei Bluetooth als auch bei IEEE 802.11 die gewünschte Sicherheit durch darüber liegende Protokolle garantiert werden muss.