Bild: Siemens, Xircom Europe

Datensicherheit in Funknetzen

Von Dr. Leonhard Stiegler

Lokale Funknetze gewähren nicht unbedingt die von öffentlichen Mobilfunk-Netzen gewohnte Sicherheit. Der Benutzer von Bluetooth- oder WLAN-Umgebungen ist vielmehr gefordert, entsprechende Sicherheitsmodi zu aktivieren.

Weltweit übersteigt die Datenkommunikation bereits heute den durch Sprache erzeugten Verkehr in Nachrichtennetzen und weist zudem die wesentlichen höheren Zuwachsraten auf. Ein zunehmender Anteil entfällt dabei auf die mobile Datenkommunikation. Für Funknetze gilt prinzipiell, dass Informationen, welche über Radiowellen übertragen werden, von jedem Empfänger im Abdeckungsbereich, der die erforderlichen Voraussetzungen der Funkschnittstelle erfüllt, empfangen werden können. Die in Festnetzen üblichen Standards der Netz-Zugangskontrolle und Datensicherheit werden somit vor allem in mobilen Netzen unabdingbar. Das bedeutet, kein Unbefugter darf Zugang zum Netz und damit zu dessen Ressourcen erhalten und die Kommunikation darf nicht abgehört werden. Die übermittelten Informationen dürfen nicht unbefugt unterdrückt, gelöscht, verändert oder ergänzt werden.

Dr. Leonhard Stiegler ist Leiter des Steinbeis-Transferzentrums TZ-Expertcom, das Teil der Steinbeis-Stiftung in Stuttgart ist.
TZ-Expertcom bietet qualifizierte Schulung und Beratung im Bereich der Telekommunikations- und Informationstechnik an. Weitere Schwerpunkte liegen in der Anfertigung von Gutachten und Studien.

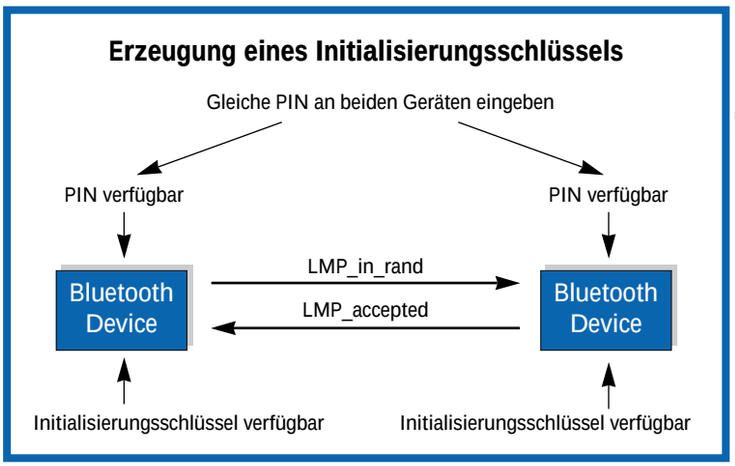
Öffentliche Mobilfunk-Netze

Zu den modernen mobilen Datennetzen (Public Land Mobile Network PLMN) gehören die aus dem GSM-Mobilfunk entstandene GPRS-Technik, sowie deren zukünftiger Nachfolger UMTS. Beide Techniken fußen auf dem ausgeklügelten Sicherheitssystem der GSM-Mobilfunk-Technik. Diese geht davon aus, dass jeder Teilnehmer durch eine weltweit eindeutige Identifizierungsnummer, die IMSI (International Mobile Subscriber Id) gekennzeichnet ist. Im Rahmen einer festgelegten Netz-Zugangsprozedur werden neben der IMSI auch so genannte Authentisierungs-Parameter zwischen dem mobilen Endgerät und dem Kommunikationsnetz ausgetauscht, um die Rechtmäßigkeit des Zugriffs und die Sicherheit der Datenübertragung zu gewährleisten. Wichtig ist darüber hinaus die durch detaillierte internationale Protokolle festgelegte Verwaltung der verwendeten Verschlüsselung zwischen dem Netzbetreiber und dem mobilen Endgerät. Man kann daher heute davon ausgehen, dass ein Internetzugang über ein öffentliches GPRS- oder UMTS-Datennetz den hohen Sicherheitsanforderungen der Festnetztechnik, zum Beispiel in einem lokalen Firmen-Netz (LAN), entsprechen.

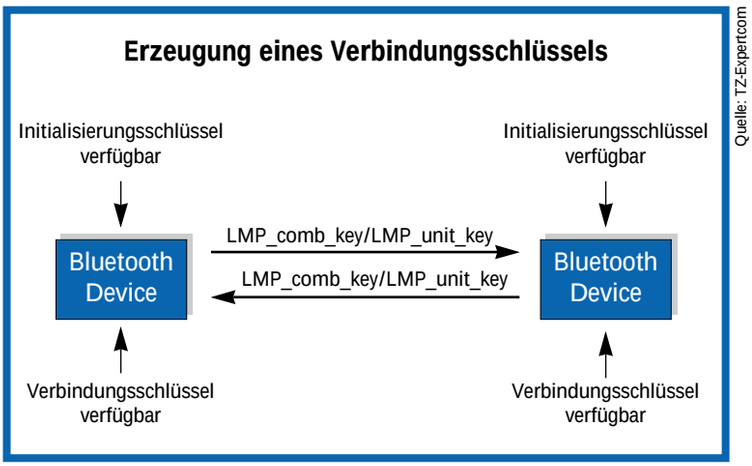
Nahbereichs-Datennetze

Neben den öffentlichen Mobilfunk-Netzen gewinnen Nahbereichs-Funktechniken eine zunehmende Bedeutung beim Transport von vielerlei Telekommunikationsdiensten über die „Luftschnittstelle“. Die wichtigsten Techniken, die sich auf international anerkannte Standards stützen, sind Bluetooth und Wireless LAN (WLAN). Bluetooth-Endgeräte sind auf dem Markt bereits erhältlich, wie zum Beispiel Mobilfunkgeräte mit Bluetooth-Schnittstelle zu Laptop, Notebook oder Palmtops. WLAN-Netzelemente werden für die effiziente Erweiterung von Firmennetzen wie auch für diverse Heimanwendungen angeboten. WLAN-Dienste an „Hotspots“ wie Flughäfen, Bahnhöfen, Sportstätten, Messehallen, Hotels und Restaurants sollen zukünftig den mobilen Internetzugang über öffentliche Netze verbessern und vereinfachen. Diese umfassenden Anwendungen rücken die Frage nach der Sicherheit von Bluetooth und Wireless LAN in den Vordergrund.

Im Bereich der Zugangskontrolle und der Datensicherheit bieten die unterschiedlichen Techniken verschiedene Methoden an. Bluetooth definiert drei Sicherheitsmodi. Im Sicherheitsmodus 1 gibt es keine Authentifizierung oder Verschlüsselung. Im Sicherheitsmodus 2 sind die Authentifizierung und die Verschlüsselung abhängig von der Anwendung das heißt, wenn die Anwendung das benötigt, wird es für diese Anwendung durchgeführt. Für die anderen Anwendungen, die auf demselben Link kommunizieren, gilt das nicht. Im Sicherheitsmodus 3 werden die Authentifizierung und die Verschlüsselung beim



Beginn der Paarungsprozedur (Pairing) zweier Bluetooth-Geräte



Geräte- beziehungsweise Kombinationsschlüssel bilden den Verbindungsschlüssel

Verbindungsaufbau durchgeführt. Dann gilt das für alle Anwendungen, die auf diesem Link kommunizieren. In den Sicherheitsmodi 2 und 3 ist die Verschlüsselung optional. Für den Sicherheitsmodus 3 bedeutet das, dass die Authentifizierung in jedem Fall beim Linkaufbau geschieht, während die Verschlüsselung auch erst von einer Anwendung aktiviert werden kann.

Im Folgenden werden die Prozeduren des Sicherheitsmodus 3 näher erläutert. Sicherheitsbarrieren gibt es in den höheren Protokollschichten. Die verwendeten Sicherheitsmethoden sind Verbindungsschlüssel, Authentisierung und Datenverschlüsselung. Eine Schwachstelle bei allen Sicherheitssystemen ist bei der ersten Kontaktaufnahme die Aushandlung einer Verschlüsselung. In dieser Prozedur sollten möglichst komplizierte „Zusatzinformationen“, die ein möglicher Lauscher nicht kennt, verwendet werden. Dadurch erhöht sich die Sicherheit der Verschlüsselung um ein vielfaches.

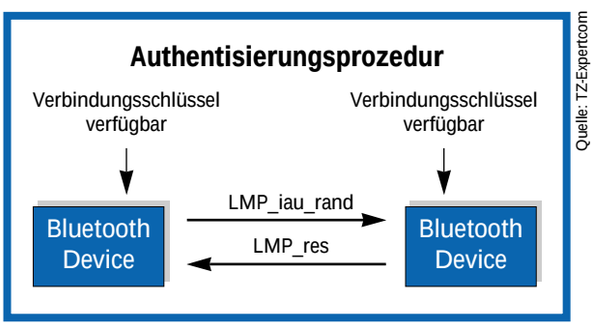
Bluetooth verwendet als gemeinsame „Zusatzinformation“ eine PIN (Personal Identification Number), welche außerhalb der Funk-Kommunikation auf beiden Bluetooth Devices bekannt sein muss. Die Paarungsprozedur (Pairing) stellt sicher, dass beide Devices dieselbe PIN verwenden. In LMP_in_rand (siehe Abbildung oben links) sendet der Initiator der Paarungsprozedur eine 128 Bit lange Zufallszahl an den Partner. Dann wird auf beiden Geräten die PIN eingegeben. Aus der PIN, der Zufallszahl und der Device-Adresse des Partners wird nun auf beiden Bluetooth Devices ein Initialisierungsschlüssel generiert.

Als Nächstes wird der Verbindungsschlüssel ausgehandelt. Manche Bluetooth-Geräte verfügen über einen eingebauten Geräteschlüssel (Unit Key). Es wird nun ausgehandelt, ob ein solcher Geräteschlüssel oder ein neuer Kombinationsschlüssel verwendet werden soll. Der Kombinationsschlüssel wird aus dem Initialisierungsschlüssel und einer neuen, in LMP_comb_key übertragenen und mit dem Initialisierungsschlüssel verschlüsselten Zufallszahl gebildet. In LMP_unit_key wird der Geräteschlüssel übertragen, zwar ist auch er mit dem Initialisierungsschlüssel verschlüsselt, dennoch bedeutet dies ein Sicherheitsrisiko. Der Geräte- beziehungsweise der Kombinationsschlüssel bildet dann schließlich den Verbindungsschlüssel. Zum Abschluss der Pairing-Prozedur geschieht die Authentisierung in beiden Richtungen um den Verbindungsschlüssel zu verifizieren. Die Abbildung oben rechts zeigt einen der beiden Abläufe.

128-Bit-Verschlüsselung

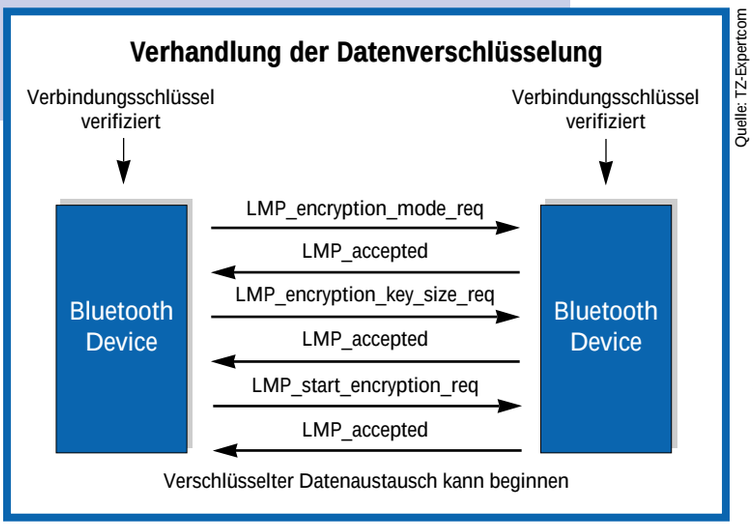
Bei künftigen Verbindungen wird die Authentisierung nur insoweit durchgeführt, wie von den Partnern gefordert. Das hängt davon ab, in welchem Sicherheitsmodus die Partner sind. Dazu wird der Verbindungsschlüssel herangezogen. Das Bluetooth Device, das die Authentisierung fordert sendet in LMP_au_rand eine 128 Bit lange Zufallszahl an den Partner. Aus dieser Zufallszahl, dem Verbindungsschlüssel und der Bluetooth-Device-Adresse des Empfängers von LMP_au_rand wird auf beiden Bluetooth-Geräten die Antwort Sres (Signed Response) berechnet. Ein weiteres Ergebnis ist der Authenticated Ciphering Offset (ACO), der später bei der Datenverschlüsselung benötigt wird. In LMP_Sres wird die Antwort zurückgeschickt und vom Empfänger geprüft. Bluetooth verwendet die safer-SK128-Verschlüsselungsmethode mit einer Schlüssellänge von maximal 128 Bit.

Ein Bluetooth Device beginnt die Verhandlung der Datenverschlüsselung mit der Nachricht LMP_encryption_mode_req. Dabei ist zu unterscheiden zwischen keiner Verschlüsselung, Punkt-zu-Punkt- (ptp) und Punkt-zu-Mehrpunkt-Verschlüsselung (pmp, Broadcast). Mode-3 Verschlüsselung (pmp) erfordert diese Festlegung natürlich mit allen an der Verbindung beteiligten Bluetooth-Geräten. Da die Länge des Datenschlüssels (maximal 128 Bit) nicht festgelegt ist, müssen sich die Bluetooth Devices gegenseitig darüber informieren. Dies geschieht mit LMP_encryption_size_req. In LMP_start_encryption_req wird eine neue 128-Bit lange Zufallszahl übertragen. Daraus, aus dem ACO (bei Punkt-zu-Punkt-Datenverschlüsselung) beziehungsweise der Bluetooth-Device-Adresse des Masters (bei Punkt-zu-Mehrpunkt-Datenverschlüsselung) und dem Verbindungsschlüssel wird der kryptografische Schlüssel berechnet.



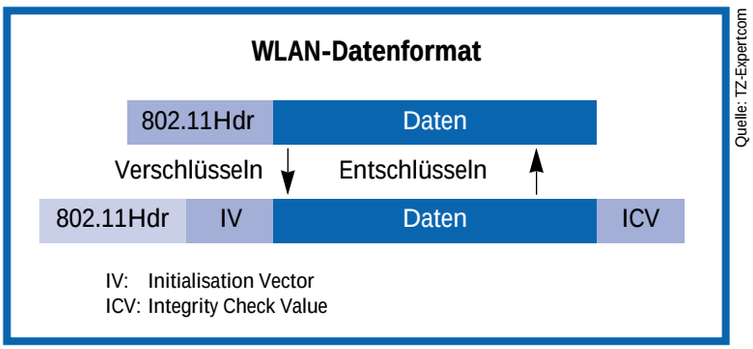
Authentisierung nach Abschluss der Pairing-Prozedur

Abhören wird durch die geringe Reichweite von Bluetooth erschwert. Der Standard sieht vor, dass die Bluetooth-Geräte untereinander die Sendeleistung aushandeln können. Wenn sich die Geräte also nahe beieinander befinden, so kann die Sendeleistung erheblich reduziert werden, sodass das Abhören aus weiterer Entfernung unmöglich wird. Die Geräte flüstern also gewissermaßen. Dieses Leistungsmerkmal wurde eigentlich entwickelt um zu verhindern, dass die Empfänger übersteuert werden. Allerdings wird es nicht von allen Bluetooth-Modulen unterstützt. Die Reichweite kann auch durch elektromagnetische Abschirmung begrenzt werden, sodass ein Funksignal einen Raum oder ein Gebäude nicht verlassen kann.



Quelle: TZ-Expertcom

Bluetooth-Geräte handeln einen maximal 128-Bit langen Schlüssel aus



Quelle: TZ-Expertcom

Verschlüsselung und Entschlüsselung bei Wired Equivalent Privacy (WEP)

Bluetooth führt ein Frequenzsprung-Verfahren aus. Die Sprungfolge ist nur den Teilnehmern eines Netzes bekannt. Ein fremder Teilnehmer kennt die Sprungfolge nicht und kann daher auch nicht mithören. Es sei denn er hört simultan alle 79 Funkkanäle ab. In der Inquiry-Prozedur werden Bluetooth Devices innnerhalb der Funkreichweite gesucht und die für einen Verbindungsaufbau notwendigen Informationen ausgetauscht. Wenn ein Bluetooth-Gerät nicht auf Inquiry antwortet, so ist es für andere Bluetooth Devices unsichtbar. Somit stellt auch das eine Form der Zugangskontrolle dar. Denn durch Verwendung eines Verbindungsfilters können Verbindungswünsche nur von registrierten Bluetooth Devices berücksichtigt werden. Dies ist ein weiteres Kriterium für die Zugangskontrolle.

Wireless LAN

Wesentliche Vertreter der Wireless-LAN-Funktechnik sind durch die Standards IEEE 802.11a und 802.11b festgelegt. Beide unterscheiden sich hauptsächlich in ihrer Funkschnittstelle und der angebotenen Datenrate. Der physikalische Zugang zu einem WLAN geschieht durch die Technik des CSMA (Carrier Sense Multiple Access), ähnlich dem drahtgebundenem LAN. Ein Unterschied besteht in der Kollisionsbehandlung. WLAN verwendet die CA- (Collision Avoidance) Methode, das bedeutet, der Zugang zum Funknetz wird „auf Anfrage“ freigegeben, erst nach dieser Freigabe darf eine Station ihre Daten versenden. Die Datenkommunikation nutzt beim Standard IEEE 802.11b das 2,4-GHz-Frequenzband.

Ein WLAN-Datenblock setzt sich aus Kopffeld (Header) und Datenfeld zusammen. Wie sind diese IEEE-802.11-Datenblöcke vor einem beabsichtigten oder unbeabsichtigten Mitlesen und Ändern geschützt? Das Ausmaß des Schutzes hängt davon ab, ob der Wireless-LAN-Benutzer seine Kommunikation mittels der in jedem Wireless-LAN angebotenen Sicherheitsbarrieren schützt, oder ob er dies unterlässt.

Zwei Methoden stehen dazu zur Verfügung: die SSID- (Service Set ID) und die WEP- (Wired Equivalent Privacy) Methode. SSID hat die Bedeutung einer Netz-Identifizierung für die einzelnen Teilnehmer. Da SSID lediglich eine Identifizierungs-Funktion ausführt und für eine sichere Datenübertragung eine untergeordnete Rolle spielt, wird in folgenden die WEP-Methode näher erläutert.

Wired Equivalent Privacy

Betrachten wir im folgenden die wichtigsten Eigenschaften der von WEP verwendeten Verschlüsselungsmethode. Die eingesetzte Vernam-Verschlüsselung oder „one-time pad“ verwendet einen gepaarten Schlüsselsatz, davon ist ein Schlüssel beim Sender und einer beim Empfänger. Die Verschlüsselung besteht nun darin, jedes Nutzdaten-Byte mit seinem entsprechenden Schlüssel-Byte zu verrechnen (bitweise XOR-Verknüpfung) und das Ergebnis zu übertragen. Beim Empfänger wiederholt sich dieser Vorgang in umgekehrter Reihenfolge zur Wiederherstellung der Nutzdaten. Bei der RC-4-Verschlüsselung wird mit jedem 802.11-Datenblock eine Schlüsselinformation (IV: 24-Bit) und eine verschlüsselte Prüfsumme für die übertragenen Daten (ICV: 32-Bit) übermittelt (siehe Abbildung rechts oben).

Die „Schwächen“ der WEP-Verschlüsselung liegen in den Feinheiten der Anwendung. Vernam-Codes müssen absolut statistisch erzeugt werden. Man verwendet daher bei hohen Sicherheitsanforderungen Hardware-Generatoren für die Erzeugung von Zufallsdaten. Vernam-Codes dürfen nur einmal verwendet werden. Die Wiederverwendung eines einmal benutzten Vernam-Codes birgt das Risiko der einfachen Decodierung durch einen Unbefugten, der die codierten Nachrichten mitgelesen und ausgewertet hat.

Authentisierung

Die Authentisierung bedeutet die Prüfung der Identität und die Feststellung der Nutzungsberechtigung eines WLAN-Benutzers. Die unter WEP definierte Authentisierung heißt „Shared Key Authentication“ und funktioniert folgendermaßen. Ein Authentisierungsschlüssel wird außerhalb einer Wireless-LAN-Verbindung zwischen dem Nutzer und dem Betreiber des WLAN-Netzes vereinbart (beispielsweise durch Kauf einer Zugangs-Lizenz). Das WLAN-Netz generiert eine Challenge-Nachricht (basierend auf einer Zufallszahl), die das Endgerät mit seinem eigenen Authentisierungs-Schlüssel codiert und als „Response“ zurück schickt. Dieses Verfahren birgt prinzipielle Schwächen, da die Challenge-Nachricht und ihre Response aufgezeichnet werden können, und da daraus der Authentisierungsschlüssel gewonnen werden kann.

Die Sicherheit in Funknetzen hängt – abgesehen von ausgeklügelten Methoden in öffentlichen PLMNs – ganz wesentlich von der Sorgfalt der Betreiber und Benutzer dieser Systeme ab. Im Gegensatz zu den öffentlichen Mobilfunk-Netzen, kann der Nutzer in lokalen Funknetzen seine Sicherheitsstufe auswählen, die niedrigste Stufe gewährt keinerlei Schutz bezüglich Netzzugang und Datensicherheit.

Die gegebenen Sicherheitsspielräume muss der Nutzer von Bluetooth und WLAN gemäß seinem Bedarf und seiner Verantwortung auswählen. Doch selbst in der höchsten Sicherheitsstufe besteht prinzipiell die Gefahr, dass ein Lauscher außerhalb des Gebäudes den Funkverkehr aufzeichnet und nach statistischen Gesichtspunkten auswertet. Die Reichweite eines WLAN lässt sich wegen der unterschiedlichen Ausbreitungsbedingungen nicht eindeutig begrenzen. *(GB)*