Sicherheitsaspekte drahtloser Datenübertragungsverfahren
Ein Update

Dipl.-Ing. Erich H. Franke, DK6II
D-75203 Königsbach-Stein
email: erich.franke@afusoft.de

Beitrag zur 49. Weinheimer UKW-Tagung 2004 in Bensheim

Die neuen digitalen übertragungssysteme, die im privaten und öffentlichen Bereich nicht mehr wegzudenken sind, bringen interessante Probleme mit sich: Abhören, Stören, Verfälschen von drahtlos übertragenen Nachrichten um nur einige zu nennen. Wir wollen im folgenden Beitrag die Risiken und Nebenwirkungen näher betrachten.

Königsbach-Stein, im Juli 2004

Übersicht

Wenn wir von drahtlosen Übertragungsverfahren sprechen, haben wir es bei neu eingeführten Systemen mit nur wenigen Ausnahmen mit digitalen Verfahren zu tun.

Diese betreffen zum großen Teil bestehende Systeme und Dienste auf analoger Basis mit großer Verbreitung, deren Umstellung aufgrund eben dieser Verbreitung sehr hohe Kosten erfordern würde, beispielsweise der analoge Rundfunk und Fernsehen im Vergleich zu *Digital Audio/Video Broadcasting* (DAB, DVB) deren Verbreitung momentan von Industrie und Politik gleichermaßen vorangetrieben werden.

Als Treiber zeugt sich hier zum Einen das Satellitenfernsehen, wo die Preise digitaler Empfänger im Verlauf des vergangenen Jahres das Niveau der analogen erreicht haben.

Man denke aber auch an die Sprachübertragung im Flugfunk, weite Teile der Kommunikation von ‚*Behörden und Organisationen mit Sicherheitsaufgaben*' (BOS) in Deutschland und last-not-least auch die Sprachübertragung im Amateurfunk mit den Cousins LPD (*Low Power Devices*) und CB (*Citizen Band*), also der ‚klassischen' Funk-Domäne.

Interessant zu beobachten hier ist die Entwicklung auf dem Sektor „Digitaler Behördenfunk", d.h. BOS, bei dem politische und Kostenüberlegungen zu neuen Entwicklungen geführt haben.

Bei neu eingeführten Systemen erfolgt die Übertragung in den meisten Fällen digital, wobei der Unterschied zwischen analoger und digitaler Übertragung der breiten Öffentlichkeit oft gar nicht bewusst ist. In privaten Haushalten ist man beispielsweise für die Sprachübertragung, abgesehen von Spielzeugen auf Basis LPD oder CB, lange an digitale Mobiltelefone gewöhnt und kaum jemand muss sich heute noch an die alten ‚analogen' Mobiltelefonnetze A und B erinnern und in der PC-Vernetzung sind Sprach- Bild- und Datenübertragung sowieso bereits zusammen gewachsen.

Dabei treiben im Wesentlichen drei Hauptaspekte die Digitalisierung voran:

Für den Privatanwender ist ein Argument die ‚gleich bleibend gute Übertragungsqualität', ein Aspekt der im stationären Betrieb meistens gilt. Die Sprachqualität von ISDN wird gegenüber der beim analogem Telefon als ‚besser' empfunden, obgleich ISDN keine Fehlerkorrektur enthält.

Bei Bildübertragung – beispielsweise im Satellitenfernsehen müssen Daten wegen der begrenzten Kanalkapazität komprimiert werden. Da sich Fehler in den komprimierten Daten meist auf ganze Bereiche (Blöcke) auswirken würden, werden Fehlerkorrekturverfahren angewandt.

Das führt dazu, daß ein derartiges System eine bestimmte Fehlerlast kompensieren kann. Die übertragenen Daten erscheinen fehlerfrei, so lange nicht eine kritische Schwelle überswchritten wird. Wird nämlich das Fehlerkorrekturverfahren durch eine höhere Fehlerrate überlastet, so tritt schlagartig eine große Zahl von Störungen auf - die Verbindung reißt plötzlich komplett ab.

Anwender von Mobiltelefonen können das ggf. selbst beobachten. Fährt der Mobilteilnehmer in ein ‚Funkloch' so reißt die Verbindung meist schlagartig ab, obgleich noch kurz zuvor die Verbindung einwandfrei

und ‚unverrauscht' war. Im analogen Funk wäre man indessen gewohnt, dass das Signal mehr oder minder starke Rauscheinbrüche aufzeigt.

Erfahrungsgemäß werten professionelle oder behördliche Anwender diesen digitalen Aspekt eher als Nach- denn als Vorteil. Das ‚analoge', gutmütige Verhalten, bei der die Sprachqualität im Gebiet der Grenzreichweite allmählich abnimmt (*graceful degradation*) sicher gerade in Krisensituationen die Kommunikationsfähigkeit.

Zum zweiten ist die Möglichkeit, neben klassischer Sprache über das gleiche Medium Daten und Bilder zu übertragen für alle Anwendungsbereiche interessant – gerade auch für Behörden und Organisationen mit Sicherheitsaufgaben.

Hierzu bieten alle ernstzunehmenden Mobilfunk-Aspiranten die Möglichkeit, Internet-Protokolle zu übertragen.

Der dritte und wahrscheinlich wichtigste Aspekt ist die Möglichkeit, die Übertragung durch kryptologische Verfahren sichern zu können. Gute Schutzverfahren sind bei digitaler Datenübertragung technisch ungleich einfacher zu implementieren als bei klassischen analogen Verfahren, bei denen in vielen Fällen eine einfache Verschleierung genügen musste.

Neben dem für den privaten Anwender unzweifelhaft erstrebenswerten Schutz der Privatsphäre und für den kommerziellen und behördlichen Nutzer wichtigen Geheimschutz sprechen harte wirtschaftliche Faktoren für die Einführung von Verschlüsselungs- und Authentisierungsverfahren. Für den Kommunikationsanbieter liegt hier die Möglichkeit der kommerziellen Abrechenbarkeit seiner Dienstleistungen – ein Aspekt, der nicht nur im Mobilfunk sondern auch im Bereich der Unterhaltungsmedien (*Digital Rights Management*, DRM) eine wachsende Rolle spielt.

Wir wollen im folgenden ohne inhaltliche Wertung die technischen Aspekte von Schutzmaßnahmen und deren Überwindbarkeit betrachten – interessant vor allem um bei Auslegung neuer Systeme bereits bekannte Fallstricke zu umgehen.

Szenarien und Lösungen

Wenn wir Schutzmaßnahmen bei drahtlosen Übertragungsverfahren diskutieren müssen wir zunächst die Bedrohungsszenarien betrachten. Für den privaten Nutzer stellt sich die ‚Bedrohung' oft anders dar als für einen kommerziellen Anwender oder für eine Behörde. Die Grundsätze sind jedoch ähnlich.

Der offensichtlichste Fall stellt das unbefugte Abhören einer Verbindung mit anschließender ‚Inhaltsauswertung' dar. Diesem Szenario wird durch Verschlüsselung der Daten begegnet. Hierunter versteht man die umkehrbare Veränderung der schützenswürdigen Nutzdaten durch mathematische Verfahren.

Die schützenswürdigen Nutzdaten werden gerne auch als ‚rot' bzw. als ‚Klartext' bezeichnet. Nach der Verschlüsselung wird hieraus ‚schwarze' bzw. Kryptoinformation. Für das Verschlüsselungsverfahren den ‚Algorithmus' gibt es verschiedene Verfahren. Das einfachste ist die Verknüpfung mit einer so genannten Pseudozufallsfolge, beispielsweise Bit für Bit mit einer Exklusiv-Oder-Verknüpfung. Dies ist bei Weitem nicht das beste denkbare Verfahren, aber es ist einfach zu implementieren und wird deshalb häufig eingesetzt.

Die benutzte Zufallsfolge muss dabei auf der Sende- wie auf der Empfangsseite identisch erzeugbar sein, also statistisch zufällig ‚aussehen' jedoch deterministisch zu erzeugen sein - deshalb die Bezeichnung Pseudo-Zufallsfolge.

Die Zufallsfolge soll möglichst ‚lang' sein, sich also erst in möglichst großen Zeitabständen wiederholen. Sie wird auf Sende- und Empfangsseite von Informationen wie dem ‚Schlüssel', der sog. ‚Variablen' abgeleitet.

Dabei benutzen sog. symmetrische Verfahren auf Sende- und Empfangsseite die gleiche Variable. Dies hat den Nachteil, dass diese vor der Benutzung über einen sicheren Weg vom Sender an alle möglichen Empfänger verteilt werden muss.

Besser geeignet sind so genannte ‚asymmetrische' Verfahren, die zur Ver- und Entschlüsselung zwei getrennte Variablen benutzen. Bei bekannten *‚Public Key*-Verfahren sind dies beispielsweise der ‚private' ‚geheime' und der ‚öffentliche' Schlüssel. Bei diesem Verfahren kann eine Nachricht, die mit dem ‚öffentlichen' Schlüssel des Empfängers verschlüsselt wurde nur von diesem unter Nutzung seines ‚geheimen' bzw. ‚privaten' Schlüssels wieder in Klartext umgewandelt werden. Der Empfänger kann seinen ‚öffentli-

chen' Schlüssel jedoch ungeschützt verteilen, da mit diesem verschlüsselte Nachrichten ausschließlich mit Hilfe des geheimen Schlüssels wieder in Klartext verwandelt werden können.

Umgekehrt kann eine Nachricht, die mit dem geheimen Schlüssel des Senders verschlüsselt wurde, zwar von jedem Empfänger, der den öffentlichen Schlüssel besitzt entschlüsselt werden, allerdings weiß dann der Empfänger auch, dass die Nachricht genau von dem Besitzer des passenden geheimen Schlüssels stammt. Die Nachricht erhält so eine Art von Beglaubigung. PC-Benutzer kennen diese Verfahren von den allgegenwärtigen ‚Sicherheitszertifikaten'.

Durch Kombination beider Wege kann eine Nachricht erzeugt werden, die nur der gewünschte Empfänger lesen kann, bei deren Inhalt der Empfänger jedoch sicher sein kann, dass diese von dem entsprechenden Sender stammt. Dies kann erzielt werden, ohne dass einer der ‚kritischen' privaten Schlüssel übertragen werden muss.

Gute Verschlüsselungsverfahren sind auch dann sicher, wenn das Verfahren, der ‚Algorithmus' nach dem verschlüsselt wird allgemein bekannt ist. Verfahren die darauf beruhen, dass der Algorithmus geheim bleibt müssen als minderwertig betrachtet werden, denn was bleibt heute im Zeitalter globaler Information denn schon geheim?

Gute Verfahren sollten auch dann Sicherheit bieten, wenn zu einem Teil Kryptotext der passende Klartext bekannt ist. Nicht bei allen Algorithmen sind diese Voraussetzungen gegeben, wie wir bei GSM-Systemen sehen werden.

Also bleibt als Geheimnis nur, die Kryptovariable selbst geheim zu halten und häufig genug zu ändern, um so genannten ‚*Brute Force'*-Angriffen zu begegnen. Bei diesen versucht ein Angreifer mit massiver Rechenleistung und unter Kenntnis des Algorithmus durch Probeverschlüsseln und Variation der Variablen die passende Variable rückzurechnen. Dies ist bei entsprechend schwachen Verfahren wie wir am Beispiel drahtlose Netzwerke (WLAN) sehen werden ohne weiteres möglich.

Um es Angreifern schwerer zu machen, werden in vielen Fällen bei der Verschlüsselung nicht nur die Variable sondern auch zeitvariante oder anderweitig zufällig erzeugte Daten als ‚Startwert' mit eingerechnet. Diese Daten werden auch als ‚*Initialisierungsvektor'* bezeichnet, da durch sie die Pseudozufallsfolge mit verschiedenen Anfangswerten gestartet werden. Dadurch soll sichergestellt werden, dass zwei aufeinander folgende Sendungen nicht mit der identischen Pseudozufallsfolge (Schlüsseltext) verschlüsselt wird.

Als weiteres kritisches Szenario muss man das ‚Spoofing' betrachten, d.h. das unbefugte Eindringen in eine Verbindung und Manipulation oder Fälschung der übertragenen Information. Hierzu gehört auch die Vortäuschung der Identität oder der Berechtigung.

Private, kommerzielle und behördliche Anwender benötigen den Schutz gegen unbefugte Benutzung und Sabotage. Im harmlosesten Fall um zu verhindern, dass Unberechtigte auf fremde Kosten telefonieren, surfen oder sich Zugang zu Rechnersystemen verschaffen. In kritischeren Fällen geht es um unbefugte Transaktionen oder Manipulationen an Zahlungssystemen.

Im Regelfall sollen Authentisierungsverfahren diesen Schutz bringen. Wir haben dies bei der Diskussion der asymmetrischen Verschlüsselung bereits kurz kennen gelernt. Hier kann der Empfänger sich darauf verlassen dass ein Datensatz von einem bestimmten Sender stammt, sofern er mit dem öffentlichen Schlüssel eben dieses Senders entschlüsselt werden konnte.

Andere Verfahren wie etwa *Challenge-Response* basieren darauf, dass einer der Partner den anderen veranlasst einen möglichst nicht vorhersehbaren Wert (‚Challenge') zu verschlüsseln und diesen verschlüsselten Wert zurückzusenden (‚Response'). Dann vergleicht er die verschlüsselte Antwort mit einem Chiffrat, das er mit dem gleichen Schlüssel und Initialisierungsvektor bei sich selbst, d.h. lokal verschlüsselt hat. Stimmt die ‚Response', also die Antwort des Partners mit der lokal verschlüsselten ‚Challenge' überein, so gilt der Partner als ‚authentisch' bzw. ‚beglaubigt.

Zwei Fallstricke gibt es hier: Die Challenge muß einen großen Wertebereich besitzen und darf von einem potentiellen Angreifer nicht vorher gesehen werden können. Sonst könnte dieser sich einen Vorrat passender Challenge-Response-Paare anlegen und auch ohne Kenntnis der Variablen eine jeweils passende Antwort zurücksenden.

Zum zweiten sollten die Variablen für die Authentisierung und die für die Verschlüsselung der Nutzdaten nicht gleich sein. Wird eines der Verfahren ‚gebrochen' ist damit auch automatisch das andere kompromitiert. Wir werden eine derartige Schwachstelle bei WLAN sehen.

Doch nun genug der Theorie! Betrachten wir ein paar aktuelle Systeme und deren Sicherheitskonzepte.

Systeme

Mobiltelefon

Die Technik der Mobiltelefone nach dem GSM-Standard (*Groupe Spéciale Mobile*, *Global Standard for Mobile Communication*) wurde bereits an anderer Stelle ausführlich beschrieben [z.B. UKW97]. Hier nur ein kurzer Update:

GSM war historisch insbesondere für Telefonie ausgelegt. Marketing-Anstrengungen der Mobilfunkbetreiber ändern das Nutzungsverhalten der ‚Normalverbraucher' zunehmend von diesem reinen Telefoniebetrieb hin zu Mehrwertdiensten wie Kurznachrichten (*Short Message Service*, SMS), Bildübertragung und Internet-Zugriff (*Wireless Access Protocol*, WAP). Im kommerziellen Einsatz spielen mobile *Telematik*- und Security-Dienste, z.B. [SecuTruck], eine weitere wichtige Rolle.

In Europa sind zwei Bandabschnitte vorgesehen, zum einen stehen 124 Duplex-Kanäle zwischen 890 MHz und 960MHz und 375 Duplex-Kanäle zwischen 1710 und 1980 MHz zur Verfügung. Auf ihnen werden Daten mit 270.833 kBit/s im TDMA-Verfahren zwischen dem Mobilteil und den Basisstationen (BTS + BSC) ausgetauscht. Dabei wird Sprache mit 13 bzw. 6,5 kBit per Vocoder digitalisiert. Da vor einem Gespräch wie beim drahtgebundenen Telefon eine Verbindung durch Wählen aufgebaut wird, spricht man von dieser als ‚Circuit Switched'.

Dieser Verbindungstyp ist auch die einfachste Datenübertragungsart, die mit GSM erreichbar ist. Bitraten bis zu 9600 Baud sind auf Standardstrecken erzielbar. Allerdings ist dies für Breitbanddienste langsam und zudem teuer, da die Gebührenerfassung nach Verbindungszeit erfolgt. Es gibt ‚schnellere' Übertragungsverfahren wie das HSCSD (*High Speed Circuit Switched Data*), bei dem mehrere Kanäle bzw. Zeitschlitze gebündelt werden um so Übertragungsraten bis zu 57 kBit/s zu erzielen.

Für Datenanwendungen sehr interessant ist GPRS (*General Packet Radio Service*) bei dem ebenfalls Kanäle gebündelt werden, diese jedoch ‚paketorientiert' genutzt werden. Die Gebührenabrechnung erfolgt volumenabhängig und ist unabhängig von der Nutzungszeit. Datenraten von 50kBit/s, theoretisch bis 171kBit/s sind erreichbar.

Im Netz kommunizieren die Mobilteile mit ‚*Base Transceiving Stations'* (BTS) im Gelände über zugeordnete ‚*Base Station Controller'* (BSC). Diese Basisstationen ‚sprechen' mit Vermittlungsknoten, den *‚Mobile Switching Center'* (MSC). Hier werden die Verbindungen untereinander und zum Festnetz hin vermittelt.

Das MSC hat Zugriff auf Datenbanken, die für unsere Sicherheitsüberlegungen interessant sind. Im sogenannten ‚*Home Location Register'* (HLR) sind Teilnehmernummer, freigegebene Dienste (z.B. Telefonie, FAX, Daten) und andere Verwaltungsdaten gespeichert. Ist der Telefonbenutzer unterwegs, speichert das System im ‚*Visitor Location Register'* (VLR) des jeweiligen Vermittlungsknotens die Daten um zu sehen, ob der Teilnehmer im Netz eingebucht ist, damit er von überall her erreicht werden kann.

Ob der Teilnehmer berechtigt ist, das Netz zu benutzen, wird über das *Authentication Center* (AUC) überprüft. Im ‚*Equipment Identity Register'* (EIR) können weiterhin Ausschlusslisten geführt werden, beispielsweise die IMEI von gestohlenen Geräten, die dann vom Betrieb auszuschließen sind.

Die ‚Beglaubigung' des Teilnehmers erfolgt über das AUC. Aus historischer Sicht haben die Väter und Mütter von GSM das Hauptaugenmerk darauf gerichtet, dass sich der Teilnehmer am Netz authentisiert, vermutlich, da man den Missbrauch (*Fraud*) im Auge hatte, der in U.S. Mobilfunknetzen wegen der schwachen Authentisierung gang und gäbe war (und ist).

Es gibt kein Authentisierungsverfahren, mit dem das Mobilteil feststellen kann, dass das Netz in das es sich einbuchen will auch wirklich das gewünschte ist. Dazu gleich mehr!

Auf der SIM-Karte (*Subscriber Indentity Module*), die der Mobilfunkbetreiber bereitstellt ist eine weltweit eindeutige 15 Ziffern lange Kennung, die *International Mobile Subscriber Identity* (IMSI), zusammen mit dem 128 Bit langen *Individual Subscriber Authentification Key* (K_i) gespeichert. Diese sind ebenfalls im AUC hinterlegt.

Beim Einbuchen sendet nun das Mobilfunknetz nach dem Challenge-Response-Verfahren eine 128 Bit lange Zufallszahl (RAND) an den Mobilteilnehmer. Dieser verschlüsselt mit Hilfe des GSM-eigenen Algorithmus A3 und der Variablen K_i die 32 Bit lange ‚*signed response*' (SRES). Im Netz wird die Response mit einem Chiffrat aus der AUC-Datenbank verglichen und der Teilnehmer beglaubigt, wenn die Chiffrate passen. Der Schlüssel selbst wird verständlicherweise niemals über die Luft übertragen.

Jedes Gespräch verwendet einen neu errechneten Spruchschlüssel, der nur für die Dauer der Verbindung aufrecht erhalten wird. Dieser *Communication Cyphering Key* (K_c) ist 64 Bit lang und wird ebenfalls aus RAND und K_i diesmal mit dem GSM-typischen Algorithmus A8 errechnet. Die eigentliche Nachrichtenverschlüsselung erfolgt dann für diese Verbindung mit dem Schlüssel K_c über den *Stream Cypher Algorithm* A5. Nach Ende der Verbindung wird der Schlüssel nicht mehr verwendet.

Alle diese Algorithmen sind theoretisch ‚geheim', zählen aber heute zu den im Internet gut dokumentierten Verfahren. An Stelle der Algorithmen A3 und A8 wird netzabhängig der Algorithmus COMP128 eingesetzt, der aus RAND und K_i die beiden Werte SRES und K_c liefert. Dieser Algorithmus wurde 1998 an der Berkely Universität ‚reverse engineered' und rückdokumentiert. Dabei traten Schwachstellen zu Tage, durch deren Ausbeutung ein Angreifer nach Quellenangaben mit ca. 150000 RAND-Anfrage an eine SIM-Karte nach ungefähr 8 Stunden den ‚geheimen' Schlüssel K_i rekonstruieren können soll [DUD].

Wer nun aber den Schlüssel K_i seines Opfers kennt, kann dessen Identität vortäuschen, mit allen daraus resultierenden Konsequenzen.

Auch die einseitige Authentisierung ist ein Problem von GSM. Dies macht es möglich über entsprechende Hardware einem Teilnehmer ein GSM-Netz vorzutäuschen und diesen über Identitätsabfragen zu identifizieren um beispielsweise Bewegungsprofile aufzuzeichnen. Über diesen Weg besteht auch die Möglichkeit, beim Verbindungsaufbau das Mobiltelefon dazu zu bringen, die Verschlüsselung abzuschalten.

Der zur Nachrichtenverschlüsselung verwendete Algorithmus A5 ist aufgrund seiner kleinen Schlüssellänge (64 Bit) durch geschickt modifizierte ‚Brute Force' Attacken auch mit PCs angegriffen werden kann. Laut Quellenangaben [DUD] sollen einzelne Netzbetreiber diesen Schlüssel durch feste Anteile (Null-Bit) auf 54 Bit reduzieren, was den Schutz weiter unterläuft, da das ‚blinde Erwürfeln' der Variable dadurch wieder um einen Faktor 10^3 weniger Aufwand macht.

Auf der Geräteseite laufen die in vielen Geräten eingeführten Multimedia-Funktionen potentiellen Phreaks entgegen. Teilweise reagieren Telefone allergisch auf gezielt fehlerhaft formulierte SMS (Buffer Overflow Attacks) und stellen den Betrieb teilweise ein.

Auf die Problematik manipulierter Telefone, die bei [BSI] näher beschrieben wird, wollen wir hier nicht eingehen.

UMTS (Universal Mobile Telecommunications System) befindet sich heute noch in den Startlöchern. Unter der internationalen Bezeichnung IMT-2000 (International Mobile Telecommunications at 2000 MHz) soll UMTS und weitere Übertragungsvarianten der ‚3. Generation' (3G) zu einer globalen Systemfamilie zusammengefasst werden.

UMTS arbeitet auf 2GHz mit W-CDMA (Wide Band Code Division Multiple Access), d.h. in Spread Spectrum. Alle Teilnehmer senden dabei im gleichen ‚Kanal' auf ca. 5 MHz Bandbreite gespreizt, wobei die einzelnen Verbindungen durch einen individuell zugeteilten Code voneinander unterschieden werden. Wegen der beschränkten Kanalzuteilungen gibt es wie bei GSM Kanalpaare für Up- und Downlink, aber auch sog. ‚ungepaarte Kanäle' die im Zeitmultiplex für Up- und Downlink benutzt werden.

UMTS wird höhere Übetragungsraten 144 kBit/s, 384 kBit/s bis hin zu 2Mbit/s erlauben, wobei die Bitrate variabel gestaltet wird.

Der Radio Network Controller (RNC) entspricht in etwa der BSC bei GSM, das UMSC dem GSM MSC.

Bei der Sicherheit implementiert UMTS zusätzliche Funktionen, die bei GSM bekannte Angriffsmöglichkeiten unterbinden sollen. Hierzu zählt die Einführung des ‚*Authentication Token'* (AUTN). Dieses Token wird unter anderem aus einer (verschlüsselt übertragenen) Sequenznummer und einem Message Authentication Code gebildet. Dabei müssen die Sequenznummer, die im Home Environment des Users im Netz verwaltet wird und die auf der USIM-Karte geführt wird untereinander stimmig sein.

Stimmen der ‚Message Authentication Code' (MAC) mit dem erwarteten ‚Expected Message Authentication Code' (XMAC) nicht überein, wird mobilseitig mit einem ‚User Authentication Reject' abgebrochen. Die zweite Phase erfolgt analog zu GSM, eben nur mit anderen Algorithmen.

Schnurlos-Telefone

In vielen Haushalten sind inzwischen auch schnurlose Telefone installiert, bei denen ältere analoge oder hybride Geräte mehr und mehr durch digitale auf DECT basierende Systeme ausgetauscht werden. Hierbei spielen weniger technische Gründe denn Kostenüberlegungen eine Rolle Die Verbreitung von DECT-

basierenden Schnurlostelefonen in Privathaushalten wird faktisch durch die Verfügbarkeit von Geräten in Supermärkten und Discountern getrieben.

Der ETSI-Standard definiert jedoch viel mehr als nur die bekannte Schnurlos-Funktion. Es können beispielsweise Übergänge zu Mobilfunknetzen geschaffen werden und ganze Netze mit direkten Paging-Rufen von Mobilen Teilnehmern (Portable Part) geschaffen werden. Allerdings definiert DECT keine Dienste sondern das Access-Protocol.

Derzeit sind zehn Frequenzkanäle zur Nutzung durch DECT-Telefone vorgesehen: 1880.064 MHz bis 1897,344 MHz. Bedingt durch die hohe Funkbitrate von 1,152 MBit/s wurde ein Kanalabstand von 1,728 MHz festgelegt. Moduliert wird mit GMSK mit einem Frequenzhub von ±144 kHz. Der Standard sieht eine Sendeleistung von bis zu 250 mW vor.

Pro HF-Träger werden vierundzwanzig Zeitschlitze verwendet, von denen die ersten 12 den 'Downlink' von der Feststation zum mobilen Teilnehmer belegen. Die mobilen Teilnehmern senden in den zweiten 12 Zeitschlitzen. Die Rahmenlänge, bestehend aus eben diesen vierundwanzig Zeitschlitzen beträgt in Summe 10 Millisekunden. Jeweils 16 dieser Rahmen bilden einen sogenannten 'Multiframe' von 160 ms Dauer. Demnach dauert ein Zeitschlitz ca. 416µs und enthält 480 Bit. Schutzzeiten von jeweils 50 µs dienen dem Ausgleich des Jitters aus dem mobilen Einsatz. Weiteres findet man beispielsweise unter [DECT].

DECT-Systeme werden (heute) im häuslichen Bereich zum überwiegenden Teil ausschließlich zur schnurlosen Telefonie genutzt. Mehrwertdienste spielen bei dieser Nutzung eine eher untergeordnete Rolle, obgleich eine Vielzahl von ‚Profilen' für Anwendungen ISDN, Radio Local Loop und eine Vielzahl von Datendiensten definiert sind und Hardware wie LAN- oder Datenadapter am Markt verfügbar sind.

Durch die zunehmende Integration von Internet-Diensten mit Telefonie könnte sich dies vielleicht ändern.

Zur Sicherheitsseite ist folgendes zu sagen: Das System kann aus mehreren Feststationen (‚*Fixed Parts*', FP) und Mobilstationen (‚*Portable Parts'*, PP) bestehen.

Die Feststationen identifizieren sich durch die 40 Bit umfassende ‚*Radio Fixed Part Identity'* (RFPI), die im wesentlichen aus der *Primary Access Right Identity* (PARI) und der 8-Bit umfassenden *Radio Fixed Part Number* (RPN) besteht. Ein Flag zeigt an, dass weitere ‚*Secondary Access Right Identity* (SARI) folgen, die benutzt werden, wenn die jeweilige Basisstation für verschiedene Verbindungstypen in Frage kommt. Die *Access Rights Identity Classes* zeigen den Benutzungstyp an, d.h. hier ist definiert, ob es sich bei dem ‚Fixed Part' (FP) um ein Schnurlostelefon oder einen Netzübergang handelt.

Jedes Mobilgerät besitzt eine eindeutige Kennung, die sog. ‚International Portable Equipment Identity' (IPEI). Diese umfaßt 36 Bit und besteht aus dem 16 Bit langen ‚Equipment Manufacturer's Code' (EMC), welcher den Hersteller bezeichnet, sowie der 20 Bit umfassenden ‚*Portable Equipment Serial Number'* (PSN).

Die Authentisierung arbeitet wie gewohnt nach einem Challenge-Response-Prinzip. Die FP sendet zwei 64-bit lange Zufallszahlen als Challenge an das PP welches aus diesen mittels des ‚geheimen Schlüssels' eine 32-bit Antwort berechnen und diese zum FP zurück schickt. Der DECT-Standard lässt auch eine Authentisierung in Gegenrichtung zu, es bleibt jedoch dem Gerätehersteller überlassen, ob er diese Sicherheitsmaßnahme auch nutzt.

Der oben erwähnte ‚geheime Schlüssel' wird bei Schnurlostelefonen bei der (Erst-)Inbetriebnahme ausgehandelt. Er wird zwar nicht direkt über Funk übertragen, jedoch besteht zumindest die theoretische Möglichkeit, dass ein Angreifer ihn durch Mitschreiben der Prozedur nachbilden könnte. Findet die Erstinbetriebnahme in einem abhörgeschützten Bereich statt, so kann man diesen Fall in der Praxis häufig vernachlässigen.

Der physikalische Zugriff zum FP sollte jedoch unterbunden werden, damit sich ein Angreifer nicht heimlich nachträglich mit einem mitgebrachten PP an dem FP anmeldet und dieses dann betrieblich nutzt. Zu Schutzzwecken kann ein PIN-Code gesetzt werden, der zur Anmeldung benötigt wird. Vorsicht, Falle: Viele Hersteller haben triviale PIN wie 0000 oder 1234 als Werkseinstellung...

Die oben beschriebene Authentisierung erfolgt bei jedem Rufaufbau. Bei erfolgreicher Durchführung wird ein für die Dauer der Verbindung gültiger Nachrichtenschlüssel aus dem geheimen Schlüssel und der Zufallszahl als Initialisierungsvektor im FP und PP errechnet, so dass dieser niemals über Funk übertragen werden muss.

Wireless LAN

Auf dem Gebiet der Datenintegration und mobiler Internet-Zugänge besteht ein ganz erheblicher Wettbewerb zwischen unterschiedlichen Technologien. Wird DECT aufgrund seiner Geschichte von vielen Anwendern zu Unrecht als reiner Telefonie-Standard empfunden, sind drahtlose Netzwerke nach IEEE 802.11 (Wireless Local Area Network, WLAN) und Bluetooth als Datenübertragungsstandards in der Computertechnik auf breiter Front akzeptiert.

Konzeptionell ist WLAN die drahtlose Ergänzung zu drahtgebundenen Computernetzen. Der Standard ist dafür ausgelegt, dass hierüber Daten paketorientiert basierend auf den standardisierten Internet-Protokollen (IP) ausgetauscht werden können.

Der Standard der IEEE (Institute of Electrical and Electronics Engineers) geht bereits auf das Jahr 1997 zurück. Der Standard ist mehrfach überarbeitet worden, insbesondere mit dem Ziel, die Übertragungsrate zu erhöhen und inzwischen bekannte Sicherheitslücken zu stopfen. Die Systeme arbeiten in Europa auf 13 Kanälen im 5MHz-Raster im Bereich 2400..2483,5MHz, bzw. für 802.11h auf 5.1 GHz. Dabei können pro Standort jedoch nur 3 Kanäle überlappungsfrei genutzt werden, da die Bandbreite der Aussendung bis zu 22MHz betragen kann. Aktuelle Systeme arbeiten mit Direct Sequence Spread Spectrum (DSSS) und einem festen 11-bit-Code mit Datenübertragungsraten bis zu 22Mbit/s. Systeme auf 5.1 GHz arbeiten mit 54Mbit/s mit ODFM. Sendeleistungen bis zu 100mW sind definiert. Je nach Antennen kann die Reichweite einige 10 Meter bis in den Kilometerbereich betragen.

Organisiert werden WLAN entweder als ‚Ad-Hoc'-Netze die aus einzelnen Clients bestehen, die untereinander Daten austauschen, oder als ‚Infrastrukturnetzwerk' bei der über einen sogenannten ‚*Access Point'* (AP) eine Verbindung in ein drahtgebundenes LAN besteht. Letzterer Fall ist häufig, um mobilen Computern oder Laptops Kontakt zum Firmen- oder Behördennetz zu geben, oder es dem Privatanwender erlaubt, drahtlos im Internet zu surfen. Zu diesem Zweck werden Access-Points mit eingebautem DSL-Modem angeboten.

Als Sicherheitsmaßnahmen bieten WLAN nur begrenzten Schutz. Alle Maßnahmen sind mehr oder weniger einafch überwindbar (Vgl. [BSI-WLAN])

Im Prinzip ist die Datenübertragung und die Authentisierung – sofern aktiviert – schlüsselbasiert. Die sog. ‚*Wire Equivalent Privacy'* (WEP) ist ein hübscher Marketingbegriff, der hohe Sicherheit verspricht aber kritisch betrachtet werden muss.

Die Verschlüsselung arbeitet mit Variablen zu 104 Bit bzw. bei veralteten Systemen mit 40 Bit, wobei findige Marketing-Strategen 128/64 Bit angeben. Dies ist jedoch inkorrekt. Das System benutzt einen Initialisierungsvektor von 24 Bit. Aus Variable und Initialisierungsvektor wird mit der Stream Cypher RC4 eine Pseudozufallsfolge ermittelt mit der die Nutzdaten durch lineare (XOR) Operation verschlüsselt werden. Der IV wird von Paket zu Paket geändert und in Klarlage am Paketbeginn übertragen.

Jedes Datenpaket besitzt eine Prüfinformation als 32-Bit CRC, die ebenfalls verschlüsselt wird. Diese ist zwar gegen Datenfehler auf der Funkstrecke wirksam, nicht jedoch gegen gezielte Telegrammverfälschungen. Da die Position einzelner Elemente im Telegramm wohl bekannt ist – man denke beispielsweise an die IP-Adresse – können Datenfehler eingeschleust und die CRC entsprechend korrigiert werden.

Auch das Authentisierungsverfahren ist, wie man leicht erkennen kann nicht nur relativ wirkungslos sondern auch potentiell gefährlich. Zur Authentisierung erzeugt der AP nämlich eine Zufallszahl mit 128 Bit Länge. Der Client verschlüsselt diese und sendet sie an den AP zurück. Dieser entschlüsselt die Daten und vergleicht das Ergebnis mit dem Zufallsvektor.

Gelingt es nun einem Angreifer, die Authentisierung komplett mitzuschreiben, so kann er durch einfach bitweise XOR-Operation der Klardaten der ‚Challenge' mit der verschlüsselten ‚Response' 128 gültige Schlüsselbit erhalten, mit denen er zwar nicht direkt den Schlüssel bestimmen kann, jedoch jederzeit eine Authentisierung fälschen kann, indem er nämlich eben diese zurück gerechnete Schlüsselfolge zur Berechnung einer beliebigen Authentisierungsantwort benutzt.

Auch besteht kein Schutz gegen Recording-Störer. Da der IV beliebeig wiederholt werden darf, könnte sogar theoretisch die o.g. rück gerechnete Schlüsselbitfolge zur Erzeugung eines gültigen Paketes und damit für Spoofs verwendet werden. Die Folge reicht allerdings nur für 16 Oktette, so dass diese Bedrohung in praxi gering ist.

Ein weiteres praktisches Problem ist, dass die Kryptovariablen standardmäßig ‚von Hand' an AP und Client eingegeben werden müssen. Dies stellt in Netzen ein organisatorisches Problem dar, da bei einem Schlüsselwechsel alle Clients ‚in die Hand' genommen werden müssen. Aus Gründen der Bequemlichkeit werden

die Variablen häufig über lange Zeiträume gar nicht gewechselt – eine Freude für jeden Angreifer. Die einzige ‚variable' Komponente der Verschlüsselung ist dann der Initialisierungsvektor, und der ist mit seinen 24-Bit recht kurz. Man kann damit rechnen, dass sich Schlüsselbitfolgen nach vergleichsweise kurzer Zeit wiederholen – Quellen sprechen von 4000 Paketen.

Dies ist besonders unangenehm, da seit 2001 Angriffe auf den Algorithmus RC4 existieren. Nicht nur die 40-Bit-Variable die bereits durch Brute-Force Angriffe gebrochen werden kann ist damit gefährdet. Der durch Fuhrer, Mantin und Shamir beschriebene Angriff benutzt statistische Verfahren, die darauf basieren, dass die Bit des Initialisierungsvektor unterschiedlich auf die Folge der Schlüsselbit einwirken und dass Pakete auf der Klarebene (‚rot') bestimmte feste Daten enthalten (z.B. 1. Byte 0xAA). Besitzt man eine genügende Zahl von Paketen (4 bis 6 Millionen) mit bestimmten IV kann man gemäß der Quelle auch einen 104-Bit-Schlüssel nach erstaunlich kurzer Zeit (~ 65 Minuten) rekonstruieren.

Die SSID (*Service Set Identity*) zeigt den Namen des WLAN an. Sie bietet keinerlei kryptologischen Schutz, da sie im Klartext als Broadcast vom AP ausgesendet wird und von einfachen Hilfsprogrammen, teilweise bereits von Betriebssystemteilen ausgelesen und angezeigt wird.

Einen geringen aber immerhin vorhandenen Schutzlevel bildet das MAC-Filter, bei dem am AP nur Clients mit bestimmten vorher eingetragenen MAC-Adressen akzeptiert werden. Einem gezielten Angriff vermag dies nicht entgegenzustehen, da sich die MAC-Adressen leicht fälschen lassen. Außerdem ist ein Management der MAC-Adressen meist nur in kleineren Netzen organisatorisch sinnvoll möglich. Gegen Gelegenheitseinbrecher oder bei temporärem Betrieb beispielsweise auf Messen bieten die MAC-Filter einen gewissen Schutz.

Keines der Schutzmaßnahmen mag alleine überzeugen, jedoch kann man ein ausreichendes Schutzniveau erreichen, wenn man Maßnahmen miteinander kombiniert.

Wichtigstes Element ist die Begrenzung der Reichweite durch Wahl eines Antennenstandortes und der Sendeleistung falls dies der AP zulässt, um so den physikalischen Zugriff auf die Funksignale außerhalb der eigenen Liegenschaft zu erschweren.

Zudem sollte man des ESSID-Broadcast wenn möglich abschalten und als ESSID einen Kunstnamen wählen, der nichts mit dem Unternehmen oder der Organisation zu tun hat. MAC-Filter sollte man trotz der Unbequemlichkeit benutzen und möglichst feste IP-Adressen im Netz verwenden, d.h. DHCP abschalten um einem Eindringling die Identifikation nach Möglichkeit zu erschweren. Don't give the hacker a clue... Periodischer Schlüsselwechsel ist angesagt, wenn man schon nicht Authentisierungsverfahren wie RADIUS (Remote Authentication Dial-In User Service) benutzen kann.

Bluetooth

Bluetooth hingegen war ursprünglich zur drahtlosen Anbindung von Zubehörgeräten an Mobiltelefone gedacht – beispielsweise um einen drahtloses Headset oder eine Freisprecheinrichtung ohne störende Leitungen am Mobiltelefon betreiben zu können. Bluetooth kennt daher Zweiwege-Sprachübertragung als ein primäres Merkmal.

Mit dem Essen kommt der Appetit. Ein wichtiger Einsatz von Bluetooth ist die Verbindung eines Laptop oder PocketPC mit dem Mobiltelefon zur Datenübertragung im Internet. Früher war dazu die Infrarot-Schnittstelle (IrDa) vorgesehen, bei deren Nutzung sich allerdings Mobiltelefon und Computer ‚Auge in Auge' gegenüberstehen mussten, eine Voraussetzung die im Alltagseinsatz nicht immer praktikabel ist. Daher wurde die Bluetooth-Technologie als Erleichterung empfunden.

Bluetooth benutzt 79 Kanäle im ISM-Bereich 2402 MHz bis 2480 MHz und zwar im Frequenzsprungbetrieb (Frequency Hopping, FH). Die Kanalverweilzeit beträgt 625 µs, das System arbeitet also mit 1600 Hops/sec. Die Datenmodulation ist GFSK.

Aufgrund seiner Geschichte als ‚drahtlose Kabelverbindung' sind asymmetrische Nutzdatenraten definiert. Bluetooth bietet eine Reihe von Modi, beispielsweise asynchrone, verbindungslose (*Asynchronous ConnectionLess*, ACL) Übertragung mit 723,2 kBit/s in die eine und 57,6 kBit/s in die andere Richtung. Dieser Mode ist beispielsweise für das Herunterladen von Daten aus dem Internet gedacht. Es gibt auch eine symmetrische Betriebsart mit 433,9 kBit/s für beide Übertragungsrichtungen. Hinzukommen drei ‚*Synchronous Connection Oriented*' (SCO) 64-kBit/s-‚Kanäle' für den Sprachbetrieb, beispielsweise mit einem drahtlosen Headset.

Die Geräte sind nach Sendeleistungen in Klassen aufgeteilt: Klasse 1 definiert bis zu 100 mW, Klasse drei 1mW, was für den gedachten Betrieb ‚am Körper' mehr als ausreichen ist.

Jedes Bluetooth-Gerät besitzt eine weltweit eindeutige 48-Bit-Kennung.

Um in Verbindung treten zu können, müssen Bluetooth-Geräte miteinander ‚gepaart' werden. Während dieses Vorganges wird in beiden Geräten ein 128-Bit Schlüssel erzeugt, in den neben den Geräteadressen auch eine Zufallszahl eingeht. Diese Zufallszahl wird verschlüsselt übertragen. Zu diesem Zweck muß in beide Geräte ein Code (PIN) eingegeben werden. Im Falle bestimmter Geräte (z.B. Kopfhörer) ist die PIN werkseitig vorgegeben. Hier muß das Partnergerät diese PIN genannt bekommen.

Die Authentisierung ist asymmetrisch und arbeitet wieder nach dem Challenge-Response-Prinzip. Es wird ein Zufallsvektor erzeugt und dem zu authentisierenden Gerät zugesandt. Dieses wandelt diese mit dem aus der Paarung herrührenden Verbindungsschlüssel in eine 32-Bit-Antwort um und errechnet gleichzeitig einen 96 Bit Vektor für die spätere Benutzung im Verbindungsschlüssel, der jedoch nicht übertragen wird.

Die Schlüsselerzeugung basiert jedoch alleine auf der PIN, so dass hier eine mögliche Schwachstelle liegt, wenn beispielsweise Werkseinstellungen (z.B. 0000) beibehalten werden.

Man merkt Bluetooth an, dass bereits bei der Konzeptionierung Schutzmaßnahmen vorgesehen wurden. Wichtig ist, dass diese nicht nachträglich ‚aufgepfropft' wurden, sondern auf den untersten Protokollschichten bzw. auf Chip-Ebene implementiert werden und daher den höheren Schichten transparent und einheitlich zur Verfügung stehen.

Der Schutzlevel ist der Anforderung an Bluetooth angepasst, kleine ad-hoc-Netzwerke zum Anschluss von Zubehörteilen zu bieten, die auf Grund ihrer geringen Ausdehnung weitgehend unter Kontrolle des Benutzers bleiben. Wie sich die Sicherheit zukünftiger Anwendungen gestalten wird, beispielsweise beim Einsatz von Bluetooth in der Vernetzung innerhalb und um KFZ, muss sich zeigen. Wir dürfen gespannt bleiben.

Digitale nöbL

Der BOS-Funk in Deuschland ist über weite strecken analog ausgerichtet und wird in weiten Teilen zur Sprachkommunikation genutzt. Einige Ansätze für Datenanwendungen existieren in Form hybrider Systeme wie POCSAC und dem ‚Funk Melde System' (FMS) der Feuerwehren, das als Transportmedium allerdings wiederum den analogen 2m bzw. 4m Funk nutzt. Innovative Gruppen experimentieren auch mit Packet Radio.

Der BOS-Funk nutzt zugewiesene Frequenzen, beispielsweise im 4m und 2m Band, arbeitet wie der Amateur-Relaisfunk mit analoger Frequenzmodulation. Es können lediglich analoge Verschleierungsverfahren angewandt werden. Daher können Funkgespräche mit konventionellen Empfängern, Scannern und sogar Rundfunkempfängern direkt abgehört werden.

Um eine durchgängige Verschlüsselung der Kommunikation zu erreichen, denken, wenn auch mit einiger Verspätung, die verantwortliche Dienststellen mit unterschiedlicher Intensität über die Digitalisierung des Behördenfunk nach. In Deutschland ist – abgesehen von der Problematik der Abhörbarkeit und der geringen Datentauglichkeit - der Druck der Anwender im BOS nicht so groß wie man vielleicht annehmen möchte, da in unserem Land das analoge Behördennetz gut ausgebaut und von hoher Qualität ist.

Für den flächendeckenden Einsatz alternativer digitaler Verfahren müssten massive Investitionen getätigt werden, um in überschaubarer Zeit eine ähnlich gute Versorgung zu erzielen, wie sie heute mit dem analogen Netz existiert.

Dem allerdings stehen in Deutschland derzeit massive Finanzierungsprobleme entgegen. Insider sprechen von Kosten von 7 bis 11 Mrd. Euro für eine flächendeckende Einführung im Bereich BOS. Allein die Nennung dieser Beträge hat einen – nun ja – dämpfenden Effekt auf die Einführung, obgleich der Deutsche Bundestag bereits im März 2002 [BOS_DIG_BUND] die Einführung des Digitalfunks im Grundsatz beschlossen hat. Zeitliches Ziel für die Einführung war dabei die Fußball-Weltmeisterschaft 2006 in Deutschland.

Der Hemmschuh für die Einführung einer flächendeckenden sicheren Funkkommunikation auf digitaler Basis liegt für den öffentlichen Anwender also nicht so sehr auf technischem Gebiet – die Finanzierung sowie der zu geringe politische Wille sind heute (2004) das Problem. Das Ziel, ein System bis zur Fußball-Weltmeisterschaft 2006 in Deutschland in Betrieb zu haben, scheint heute bereits als verfehlt.

Mehrere Kandidaten sind vorhanden. So konkurrieren der europäische ETSI-Standard TETRA 25 (Trans European Trunk Radio Access, neuer Name: Terrestrial Trunked Radio), der Firmenstandard TETRAPOL [TETRA], [UKW97] um die Gunst der Entscheidungsträger.

Seit Mitte 2003 macht auch ein Ableger von GSM, das GSM-BOS [GSM_BOS] von sich reden. GSM-BOS wurde von einem der in Deutschland aktiven Mobilfunk-Betreiber als alternative zu den Platzhirschen TETRA25 und TETRAPOL ins Spiel gebracht.

TETRA und TETRAPOL gehören der Klasse der so genannten ‚*Private Mobile Radio'* (PMR) an, die früher in Deutschland auch als ‚Bündelfunk' bezeichnet wurde. PMR war als Ablösung alter analoger Funktechnik im kommerziellen Bereich geplant, der wirtschaftliche Erfolg der Technik ist bislang jedoch weitgehend ausgeblieben.

PMR verhalten sich im Betrieb wie ‚echte' Funkgeräte und werden in vielen Fällen in Semiduplex mit Sprechtaste (PTT) betrieben. Weiterhin können alle Teilnehmer eines Funkkreises die anderen hören, eine Grundvoraussetzung für die Führung von Verbänden im Einsatz.

Im Gegensatz dazu sind die GSM-Ableger eher Telefoniesysteme, obgleich findige Produktmanager auch Funktionen wie Gruppenruf und Priorisierungen definieren, um im Wettlauf zur BOS-Tauglichkeit mithalten zu können.

Wir wollen die Diskussion der Auswahl geeigneter Funksysteme allerdings an dieser Stelle nicht vertiefen sondern uns am Beispiel TETRA den Sicherheitsfunktionen zuwenden.

TETRA benutzt eine Authentisierung in beide Übertragungsrichtungen auf Basis eines Authentisierungsschlüssels K, der sowohl beim mobilen Teilnehmer als auch im Netz in einem AUC (*Authentification Center*) vorhanden ist.

Damit lassen sich in erster Nährung auch Beutegeräte vom Betrieb ausschließen und die Gefahr des Net Spoof wie bei GSM besteht in dieser Form nicht.

Sowohl der Signalisierungskanal als auch die Verkehrskanäle können verschlüsselt werden. Im BOS-Bereich ist vorgesehen, die Schlüssel über SIM-Karten zu verwalten.

Die Alternative GSM-BOS [GSM_BOS] wurde jüngst ins Spiel grbracht. Laut einem Gutachten von Prof. Dr.-Ing. B. Walke, TH Aachen könnte die flächendeckende Verfügbarkeit (95,5%) innerhalb 2 Jahren erzielt werden. Das Ziel der Einführung zur WM 2006 war zumindest zum Zeitpunkt des Gutachtens noch ein treibender Faktor.

Das wesentliche Argument war selbstverständlich die prognostizierte Kosteneinsparung. Das Gutachten geht von 2,3 Mrd. Euro statt der 7 bis 11 Mrd. Euro der TETRA-Fraktion aus.

Die Idee ist an sich nicht schlecht. Der Mobilfunkbetreiber reserviert ganze Frequenzen für BOS. Bereits vorhandene Endgeräte könnten mit geringen Änderungen sofort eingesetzt werden. Da ausserdem die Netzinfrastruktur im Grundsatz bereits vorhanden ist, entfällt das leidige Thema mit Antennen- und Frequenzgenehmgungen.

Durch überschaubare Änderungen in der Firm- und Software, sowie durch Ausstattung bestehender Endgeräte mit der notwendigen Verschlüsselungstechnik und der ‚Sendetaste' wären grundsätzlich bereits viele der Einführungsprobleme von TETRA oder TETRAPOL gelöst.

Die Firmwareänderungen beziehen sich zumeist auf Fragen der prioritätsabhängige Netzressourcenverteilung und Verdrängung von niederer Priorität im Notfall sowie die Geschwindigkeit des ‚Verbindungsaufbaus'. Da die Geräte ähnlich wie analoge Funkgeräte betrieben werden sollen, werden die Verbindungen angewählt und sozusagen ‚geparkt'. Durch Betätigen der Sprechtaste wird dann der Sprachweg bedarfsweise freigeschaltet.

Wie das operationelle Verhalten der Geräte beispielsweise bei Großschadenslagen ist, muss sicher noch untersucht werden.

Die Forderung nach dem ‚Direct Mode' also der Möglichkeit der Verbindung von Mobilteil zu Mobilteil ohne eine Netzinfrastruktur und die Frage der Interoperabilität mit anderen Ländern wurde – zumindest in der Planung – argumentatorisch elegant gelöst.

Die Geräte GSM-BOS sollen eine Schnittstelle zu TETRA implementieren und den „Direct Mode" im TETRA Standard im 400MHz-Band enthalten.

Die Problemkreise der Ende-zu-Ende-Verschlüsselung (E2E) als auch die der Schlüsselverteilung über Funk sind wiederum bei TETRA, TETRAPOL und GSM-BOS gelichermaßen zu betrachten.

Ersterer Fall ist für Behörden insbesondere kritisch. Am Beispiel GSM haben wir gesehen, dass zwar die ‚Luftschnittstelle' durch das Verschlüsselungsverfahren geschützt ist. Sobald jedoch die Nutzinformation die BTS passiert hat, wird sie im öffentlichen Netz in Klarlage weiterverteilt.

Der GSM-Tresor hat also eine Rückwand aus Fichtenbrettern...

Bei der E2E-Verschlüsselung werden die Daten im sendenden Gerät verschlüsselt und erst wieder im empfangenden Gerät entschlüsselt. Während des Transportes über dazwischen liegende Netze bleiben sie somit geschützt.

Gerade Sicherheitskräfte in verdeckten Einsätzen brauchen diese E2E-Verschlüsselung um sicherstellen zu können, dass Informationen auch nicht beispielsweise in Kommunikationsstellen und Leitstellen kompromittiert werden können.

Das bedeutet, daß jedes Endgerät über einen Kryptokern verfügen muß, der ggf. über eine SIM-Karte eingebracht werden kann.

Damit zusammen hängt die Problematik der Schlüsselverteilung. Diese muss sicherstellen, dass auch wirklich alle berechtigten Teilnehmer eine so verschlüsselte Sendung aufnehmen und verstehen können. Denken wir an die aus betrieblicher Sicht notwendigen Schlüsselwechsel und wollen wir verhindern, dass gestohlene oder erbeutete Geräte die Sicherheit des Netzes gefährden, so müssen wir in der Lage sein, Schlüssel einfach, sicher (secure) und handhabbar zu den einzelnen Teilnehmern zu bringen.

Für den zukünftigen digitalen Behördenfunk wurden hierzu in Verbindung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geeignete Verfahren und Techniken festgelegt.

Quellen

[BSI_BLUE]	Projektgruppe „Local Wireless Communication" ; „Bluetooth, Gefährdung und Sicherheitsmaßnahmen"; Bundesamt für Sicherheit in der Informationstechnik (BSI); 53133 Bonn; http://www.bsi.bund.de
[BSI_WLAN]	Projektgruppe „Local Wireless Communication" ; „Sicherheit im Funk-LAN (WLAN, IEEE 802.11)"; Bundesamt für Sicherheit in der Informationstechnik (BSI); 53133 Bonn; http://www.bsi.bund.de
[BOS_DIG_BUND]	Beschluss der Bundesregierung 27.3.2002; Bestätigung durch Innenministerkonferenz 5./6. 6. 2002 (Originaltext s. u.)
[DECT]	Jürgen Kozlik; Beschreibung zu DECT; http://home.tiscali.de/kozlik/dect/ (Anm. Sehr empfehlenswerte Lektüre)
[DUD]	R. Weis, S. Lucks; „Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen"; DuD Datenschutz und Sicherheit 22)998 V2.6
[GSM-BOS]	Stephan Berberig, Axel Haber, David Jerrentrup; „GSM-BOS" Abschlussarbeit „Einführung in die Sicherheitstechnik", FH Darmstadt, 2004
[SecuTruck]	AFUSOFT SecuTruck; Fahrzeug-Sicherheitssystem 6610-0000-01; http://www.afusoft.de
[TETRA]	H. Leiderer, V. Ilyasow; „Der Funkstandard TETRA"; 6/03; FH Darmstadt;
[ULNK]	http://umtslink.at (ebenfalls sehr umfangreich und gut verständlich)
[UKW97]	Franke, E.H., DK6II; " Standards kommerzieller mobiler Funknetze - Eine Übersicht"; Skriptum zum Vortrag auf der 42. UKW-Tagung 1997 in Weinheim; http://www.afusoft.de