Orientierungshilfe

„Datenschutz in drahtlosen Netzen“

erstellt vom
Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
unter Mitwirkung des Arbeitskreises „Medien“

Stand: September 2005

Inhaltsverzeichnis

1 Einleitung

Denkmalschützer finden es toll, Datenschützer nicht so sehr. Mobile Kommunikation zwischen zahlreichen Endgeräten, bei denen niemand mehr direkt nachvollziehen kann, welche Daten übermittelt werden, ist möglich: „Anytime, Anywhere“.

„Anytime, Anywhere“ ist die Vision von mobiler Kommunikation, die Bob Allen, damals CEO von AT&T, 1996 formuliert hat. Diese Vision ist Realität geworden. Mobiles Kommunizieren, die mobile Nutzung von elektronischen Diensten sind heute gang und gäbe. Die Möglichkeiten gehen dabei weit über das simple Telefonieren hinaus: Persönliche Digitale Assistenten (PDAs) lotsen Autofahrer und Fußgänger durch Straßennetze und Großstadtdschungel, Handys senden und empfangen E-Mails. Die Anwendungen sind vielfältig.

Notwendige Basis für die meisten der mobil nutzbaren Dienste ist eine Vernetzung der mobilen Kommunikationsgeräte untereinander. Dafür existieren neben den herkömmlichen Mobilfunknetzen für die Telefonie zunehmend andere Technologien (z. B. WLAN oder Bluetooth), gerade für die lokal begrenzte Kommunikation.

Durch die drahtlose Kommunikationsinfrastruktur wird eine Verbesserung von Komfort, (lokaler) Mobilität, Effizienz und Flexibilität erzielt. Arbeitsplätze können kurzfristig ohne kostenintensive Neuverkabelung eingerichtet werden, in denkmalgeschützten Gebäudekomplexen wird eine Vernetzung von Arbeitsplätzen untereinander oft erst ermöglicht. Mobile Arbeitskräfte, z. B. Außendienstmitarbeiter, können problemlos mit ihrem Notebook am Firmennetz teilnehmen, sobald sie in der Firma tätig sind, in Familie oder Wohngemeinschaften werden einzelne Computer mittels Funktechnologien miteinander vernetzt, um den schnellen Internet-Zugang zu nutzen oder auch auf einem zentralen Drucker Dokumente drucken zu können.

1.1 Risiken

Diese Verbesserung von Mobilität und Flexibilität wird (oft) durch einen Sicherheitsverlust für die via Funk übertragenen Daten sowie die drahtgebundenen Netze und Infrastrukturen, an die die Funkkomponenten angeschlossen sind, erkauft. Zudem steigt die Gefahr von Verlust oder Diebstahl mobiler Endgeräte und somit der darauf gespeicherten Daten.

Aus der Sicht von Datensicherheit und Datenschutz ist der Vorteil der drahtlosen Kommunikation gleichzeitig deren Geißel: Es besteht keine direkte physikalische Verbindung der Geräte untereinander; sie sind Teilnehmer an einem offenen Medium. Offen bedeutet dabei, dass eine räumliche Begrenzung auf bestimmte Bereiche, z. B. nur die Geschäftsräume eines Unternehmens, nahezu unmöglich ist. Funkwellen breiten sich unkontrolliert und unbegrenzt aus. Ist ein Gebäude komplett mit der Funkinfrastruktur „ausgeleuchtet“, so ist mit an Sicherheit grenzender Wahrscheinlichkeit auch immer außerhalb des Gebäudes irgendwo ein Empfang der Funkwellen möglich. Wo, das hängt von vielen Faktoren wie Dicke und Material der Gebäudewände, Metallbedampfung der Fenster, Reflektionen der Funkwellen an anderen Gebäude ab. Vorhersagen lässt sich dies in der Regel aber nicht. Und diese Nichtvorhersehbarkeit ist wiederum eine Basis für Angriffe, Mitschnitte, Auswertungen und Manipulationen. Egal, ob sie aus krimineller Energie oder sportlichem Ehrgeiz heraus stattfinden.

Denial-of-Service-Attacken (DoS-Attacken) sind in ungeschützten Funknetzen relativ einfach durchführbar, ebenso wie Man-in-the-Middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegenstellen vorgegaukelt werden und dadurch z. B. die Datenübertragungen zu bestimmten Segmenten innerhalb von Netzen blockiert werden kann. Große Gefahren lauern auch, wenn die Geräte „Out-Of-The-Box“ eingesetzt werden, ohne Anpassungen von Konfigurationen und der „per Default“ eingetragenen Standard-Passwörter.

Überhaupt ist man einem Trugschluss unterlegen, wenn man sich auf die eingebauten, im jeweiligen Standard definierten Sicherheitsmechanismen auch nach deren Konfiguration verlässt. So ist das WEP-Verfahren, das im Standard zu WLAN festgeschriebene Verschlüsselungsverfahren, vollständig kompromittiert. Entsprechende Tools zum Durchbrechen und Informationen darüber, wie diese Tools einzusetzen sind, können jederzeit aus dem Internet heruntergeladen werden.

Werden zusätzlich herstellerspezifische, außerhalb des jeweiligen Standards liegende Sicherungsmöglichkeiten angeboten, ist eine genaue Prüfung dieser Mechanismen wichtig. So kann es beispielsweise sein, dass bestimmte Sicherungsmechanismen nur (bei WLAN-Technologien) zwischen Client und Access Point funktionieren, die gleichen Mechanismen zwischen Access Points (wenn diese z. B. als Funkbridge eingesetzt werden) aber nicht möglich sind. Hintergrundinformationen kann hier auch in sehr vielen Fällen das Internet liefern.

Es sind für den Einsatz von drahtloser Kommunikation also zusätzliche Maßnahmen zu treffen, um Vertraulichkeit, Authentizität und Integrität der Daten zu gewährleisten und die herkömmlichen drahtgebundenen Netze und die daran angeschlossenen Computer gegen Angriffe aus dem Funk-LAN heraus abzusichern. Alles, was drahtlos passiert, ist aus Sicht der Sicherheit als Aktivität in „dreckigen Netzen“ zu sehen. Herkömmliche drahtgebundene Netze sollten also gegen die Funknetze in gleicher geeigneter Weise (z. B. Einsatz von Firewalls etc.) abgeschottet sein wie gegen das Internet oder andere Netze, zu denen eine Verbindung besteht.

Zusätzlich zur Gefahr für Netze und Daten bestehen aber weitere Gefährdungspotenziale. So ist es relativ problemlos möglich, Bewegungsprofile mobil kommunizierender Komponenten und somit auch mobil kommunizierender Personen zu erstellen.

1.2 Schutzniveaus und Schutzziele

Gesundheits-, Sozial-, Steuer- und Personaldaten sind, wie alle übrigen sensiblen personenbezogenen oder personenbeziehbaren Daten, Daten mit besonderem Schutzbedarf. Schutzziel des technischen Datenschutzes ist es, diese Daten - soweit erforderlich - mit geeigneten und angemessenen technischen Methoden gegen missbräuchliche Nutzung, Manipulation oder unbefugte Kenntnisnahme zu sichern. Dabei ist davon auszugehen, dass über nahezu alle Netze im öffentlichen Bereich (Verwaltung), im nicht-öffentlichen Bereich (Privatwirtschaft) und im privaten Bereich sensible personenbezogene Daten übertragen werden; deren Übertragung also keinen Sonderfall darstellt. Für den öffentlichen Bereich sind entsprechende technische und organisatorische Maßnahmen in den Landesdatenschutzgesetzen festgeschrieben, für den nicht-öffentlichen Bereich sind diese im Bundesdatenschutzgesetz (BDSG) geregelt. In einigen Datenschutzgesetzen sind Risikoanalysen vorgeschrieben, die in Sicherheitskonzepten münden.

In Sicherheitskonzepten bzw. Datenschutzkonzepten wird konkretisiert, welche Daten in welcher Weise verarbeitet und welche Maßnahmen zu deren Schutz erfasst werden sollen, also je nach zu verarbeitenden Daten unterschiedliche Schutzniveaus definiert.

Besonderen Schutzbedarf haben dabei (erweiterte Definition gemäß Artikel 8 „Verarbeitung besonderer Kategorien personenbezogener Daten“ der EG-Datenschutzrichtlinie, Richtlinie 95/46/EG vom 24.10.1995) im Wesentlichen Daten über

- soziale oder steuerliche Verhältnisse,
- rassische oder ethnische Herkunft,
- religiöse oder philosophische Überzeugungen,
- politische Meinungen,
- die Gesundheit,

- das Sexualleben,
- Dienst- und Arbeitsverhältnisse und
- die Zugehörigkeit zu Gewerkschaften.

Es müssen in Datenschutz- bzw. Sicherheitskonzepten entsprechende technische und organisatorische Maßnahmen definiert werden, um diesen Daten mit angemessenem Aufwand den maximalen Schutz zukommen zu lassen. Die Maßnahmen müssen in Theorie und Praxis kontinuierlich überprüft und ggf. angepasst werden. Sicherungsmaßnahmen müssen dabei auf ihre Aktualität und Angreifbarkeit hin überprüft und bei Bedarf angepasst werden, beispielsweise durch Einspielen neuer Software-Releases oder Bug-Fixes, Erweiterung der Maßnahmen um neue technische Möglichkeiten oder ein Redesign der Sicherungsmaßnahmen, Neudefinition der Schutzniveaus bei veränderter Datenverarbeitung innerhalb der DV-Infrastruktur.

1.3 Ziele und Aufbau der Orientierungshilfe

Diese Orientierungshilfe soll in komprimierter Form eine Übersicht über mögliche Gefährdungen und geeignete Schutzmaßnahmen beim Einsatz von drahtlosen Technologien geben. Die Orientierungshilfe richtet sich an behördliche Datenschutzbeauftragte, IT-Verantwortliche und Administratoren, die sich mit der Planung, dem Aufbau und dem Betrieb von drahtlosen Netzen beschäftigen. In dieser Orientierungshilfe werden folgende Themen behandelt:

In **Kapitel 2** wird auf Wireless Local Area Networks (WLANs) eingegangen. Diese Art von drahtlosen Netzen nach dem IEEE[1] 802.11 Standard hat sich in vielen Bereichen etabliert. WLANs sind leicht zu installieren und die erforderlichen Sicherheitsmechanismen zum Schutz von sensiblen personenbezogenen Daten stehen in neueren WLAN-Komponenten zum größten Teil bereits standardmäßig zur Verfügung.

Kapitel 3 setzt sich mit den Gefährdungen und den Risiken bei der Nutzung von Bluetooth-Netzen auseinander. Es werden Empfehlungen zum datenschutzgerechten Einsatz dieser Netze gegeben. Der überwiegende Teil dieses Kapitels wurde dankenswerterweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellt.

Die Infrarotschnittstelle wird in **Kapitel 4** näher erläutert. Im Vergleich zu WLANs und Bluetooth-Netzen erfolgt der Datenaustausch nur über kurze Distanzen.

Kapitel 5 beschreibt mögliche Gefährdungen und Schutzmaßnahmen die beim Einsatz mobiler Endgeräte, wie Tastaturen, Mäusen und Personal Digital Assistant zu berücksichtigen sind.

Im **Kapitel 6** werden allgemeingültige Sicherheitsmaßnahmen (u. a. Firewall, Verschlüsselung, Virenschutz) beschrieben, die grundsätzlich in allen Funknetzen umgesetzt werden können.

In **Kapitel 7** werden datenschutzrechtliche Aspekte beim Einsatz drahtloser Netze betrachtet. An Hand ausgewählter Einsatzszenarien erfolgt eine Einordnung in das System des Informations- und Kommunikationsrechts.

[1] IEEE Institute of Electrical and Electronics Engineers ist ein Normungsgremium für elektrische und elektronische Verfahren. Verschiedene Arbeitsgruppen bemühen sich um die Standardisierung internationaler Anwendungen. Mit mehr als 360.000 Mitgliedern aus 150 Ländern ist die IEEE die führende Organisation auf den Gebieten Raumfahrt, Computer und Telekommunikation.

2 Wireless Local Area Networks (WLANs)

2.1 Grundlagen

Der Wireless Local Area Networks (WLAN)-Standard geht auf das Jahr 1990 zurück. Damals wurden in der Arbeitsgruppe IEEE 802.11 unter dem Titel "Wireless Local Area Network" Zugriffsverfahren und physikalische Kommunikationsschicht schnurloser LANs definiert. Aus diesen ersten Festlegungen entwickelte sich dann der Standard IEEE 802.11. Er wurde am 26. Juni 1997 durch das IEEE Standards Activity genehmigt. Er enthält grundlegende Festlegungen für WLANs bezüglich der OSI-Schichten 1 (Physical Layer) und 2 (MAC-Layer). Damit sind für alle Hersteller weltweit die Voraussetzungen gegeben, Funk-LAN-Komponenten zu entwickeln, denn der Standard IEEE 802.11 stellt die Kompatibilität der standardkonformen Systeme unterschiedlicher Hersteller sicher. Der Standard unterstützt neben Infrarot zwei unterschiedliche Funkverfahren, Direkt-Sequence und Frequency-Hopping.

Die meisten WLAN-Komponenten, die heute am Markt verfügbar sind, folgen dem IEEE 802.11g-Standard. Die wichtigsten Eckpunkte dieses Standards sind:

- Übertragungsband: 2,4 GHz
- 13 Übertragungskanäle
- Übertragungsverfahren CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
- Bandbreite im Normalfall bis 54 Mbit/s

Die weltweite Standardisierung mit der daraus folgenden weitestgehenden Interoperabilität der angebotenen Systeme sowie die stetig steigende Zahl verschiedener Anbieter sichern breite Einsatzmöglichkeiten sowie die Nachhaltigkeit der WLAN-Technologie. Der Markt der WLAN-Komponenten wächst und führt zu einer sehr hohen Verbreitung dieser Technologie, da die Komponenten preisgünstiger sind und Netze sehr flexibel aufgebaut werden können.

Neben dem IEEE 802.11 Standard existieren noch weitere Standards, die sich mit Funkübertragung befassen:

- IEEE 802.15 Wireless Personal Area Networks (WPAN, dahinter verbirgt sich die Bluetooth-Technologie) (s. 3)

- HomeRF

  Die Schwächen des IEEE 802.11 versucht der HomeRF-Standard (RF = Radio Frequency) auszugleichen. Er erlaubt parallel zum Datenverkehr die synchrone Übertragung von Sprach- bzw. Multimediapaketen. Bisherige HomeRF-Hardware erreichte nur Übertragungsraten von max. 2 Mbit/s, die Spezifikation soll allerdings für Übertragungsraten bis 10 Mbits/s erweitert werden. Derzeit engagieren sich etwa 100 Unternehmen bei HomeRF. HomeRF hat sich vor allem in den USA verbreitet; nach einer Erhebung von PC Data aus 2000 basieren dort etwa 95% aller privaten Wireless Netze auf dem HomeRF-Standard.

- IEEE 802.16 Wireless Metropolitan Area Networks (WMAN)

Eine Zusammenführung dieser Standards ist zwar geplant, aber noch in weiter Ferne. Im Wesentlichen unterscheiden sie sich in der Definition der Quality-of-Service für Sprache, Daten und Multimediaübertragungen sowie in der Reichweite (s. Abb. 1).

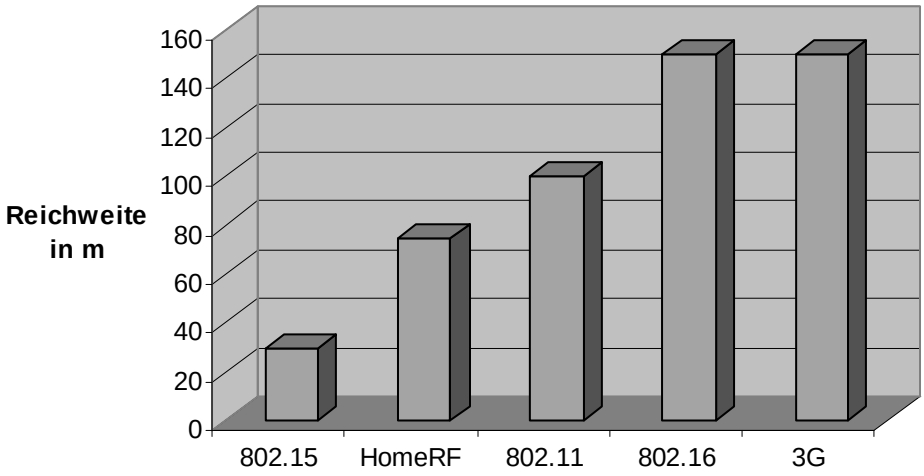


Abb. 1: Wireless-Zugriffsreichweite[2]

2.1.1 Betriebsmodi von WLAN-Netzen

Durch die verschiedenen Betriebsmodi der so genannten Access Points (Infrastructure-Mode, Bridge-Mode, Multipoint-Bridge-Mode) und der WLAN-Karten in den Clients (Ad-hoc-Mode, Infrastructure-Mode) sind die folgenden Netzwerkkonzepte realisierbar:

- **Ad-hoc-Netzwerk** (Peer-to-Peer-Kommunikationsverbindung)

  Im Ad-hoc-Modus (s. Abb. 2) kommunizieren zwei oder mehrere Endgeräte (Desktop-PC, Notebook, PDA, Drucker etc.), die mit einer Funk-LAN-Karte ausgestattet sind, direkt miteinander. Es ist darunter die klassische Peer-to-Peer-Verbindung zu verstehen, die es auch bei drahtgebundenen Systemen gibt.

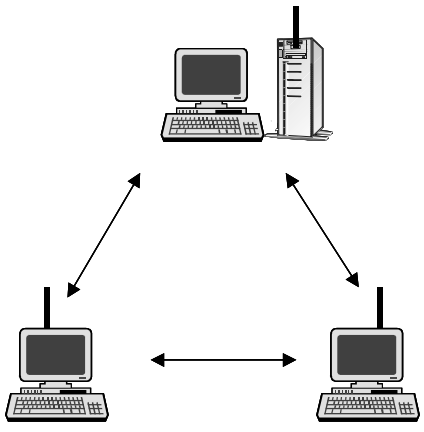


Abb. 2: Ad-hoc-Modus

- **Isoliertes Funknetz** (Nutzung eines Access Points zur Kommunikation zwischen mehreren Clients)

[2] Anmerkung zum Schaubild: 3G ist eine allgemeine Bezeichnung, die eine Reihe künftiger Mobilfunktechnologien inklusive UMTS umfasst. 3G kombiniert mobilen Hochgeschwindigkeits- Netzzugang über Internet Protocol (IP) basierte Dienste.

In der Regel werden Funknetze im Infrastruktur-Modus (s. Abb. 3) betrieben. Die Kommunikation zwischen den Clients wird dabei über eine zentrale Funkbrücke – dem so genannten Access Point – eingerichtet und gesteuert. Über die zentrale Funkbrücke kann auch eine Kopplung mit einem drahtgebundenen Netz erfolgen, beispielsweise der Anschluss des im häuslichen Bereich aufgebauten Funknetzes mit dem Festnetz des Telefonanbieters.

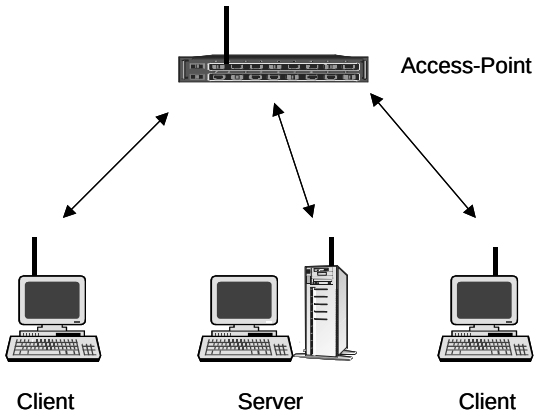


Abb. 3: Infrastruktur-Modus

- **Verbundene WLAN-Funkzellen**

  Werden mehrere WLAN-Funknetze realisiert, deren Funkzellen sich überlappen, so dass gewährleistet ist, dass beim Übergang von einer Funkzelle in eine andere die Funkverbindung nicht abreißt, spricht man von verbundenen WLAN-Funknetzen. Die Reichweite einer Funkzelle kann abhängig vom verwendeten Verfahren und von den vorliegenden Umweltbedingungen zwischen 10 und 150 m liegen.

- **Richtfunkstrecke** (Einsatz einer Funkbridge zur Verbindung von Netzwerken)

  Sollen mehrere Liegenschaften miteinander verbunden werden, kann dies mithilfe von Access Points mit Richtfunkantennen realisiert werden. Hier sind je nach Hersteller und baulichen Gegebenheiten Reichweiten von einigen Kilometern erreichbar.

2.1.2 WLAN – Übertragungsverfahren

Es sind verschiedene Übertragungsgeschwindigkeiten möglich. Die heutigen Endgeräte sind in der Lage, diese abhängig von der Übertragungsqualität (Störungen, Signalpegel) selbstständig anzupassen, d. h., sie können während der Datenübertragung die Übertragungsgeschwindigkeiten erhöhen oder senken. Je nach Standard werden folgende Übertragungsraten verwendet [3]:

Jahr	Standard	Übertragungsrate	Frequenz	Bandspreizung
1997	IEEE 802.11	max. 1 Mbit/s	2,4-GHz-ISM-Band	FHSS/DSSS
1999	IEEE 802.11b	max. 11 Mbit/s	2,4-GHz-ISM-Band	DSSS
1999	IEEE 802.11a	max. 54 Mbit/s	5-GHz-Band	OFDM
2002	IEEE 802.11h	max. 54 Mbit/s	5-GHz-Band	OFDM
2003	IEEE 802.11g	max. 54 Mbit/s	2,4 GHz-ISM-Band	OFDM/DSSS
2005	IEEE 802.11n[3]	max. 600 Mbit/s	2,4 GHz-ISM-Band	OFDM

[3] Der Standard befindet sich derzeit noch in der Entwicklung [7].

Für die Datenübertragung benutzen WLANs das so genannte ISM-Band im Frequenzbereich von 2,4000 - 2,4835 GHz. Dieser Bereich ist weltweit für unlizensierte Funkanwendungen mit begrenzter Sendeleistung (in Europa 100 mW) vorgesehen. Die Abkürzung ISM steht für "Industrial, Scientific and Medical", also für Hochfrequenzgeräte in Industrie, Wissenschaft und Medizin. Die international zugewiesenen ISM-Frequenzen waren ursprünglich für leistungsstarke Geräte wie Funkenerosionsmaschinen, Mikrowellenherde oder für die Hochfrequenzbestrahlung in der Medizin (Diathermie) gedacht, werden zunehmend jedoch auch für andere Funkübertragungssysteme mit geringer Sendeleistung des täglichen Gebrauchs wie Funkfernbedienungen oder Funkkopfhörer verwendet. Vorteil für Anwendungen bei ISM-Frequenzen ist der Wegfall der Anmeldepflicht und der gebührenfreie Betrieb; sie benötigen nur eine gerätespezifische Prüfung und Zulassung (CE-Zeichen).

Würden die Daten in einem WLAN einfach auf einen Träger aufmoduliert, entstünde ein sehr schmalbandiges Ausgangssignal. Dieses wäre erstens relativ leicht abzuhören und zweitens sehr störanfällig. Deswegen wird das Signal bei der Modulation auf den Träger auf eine wesentlich höhere Bandbreite "gespreizt".

Die Bandspreizung (Spread-Spectrum) ist eine bewährte Methode, Daten und Rauschen auseinander zu halten. Die ersten 802.11-WLANs setzten als Übertragungstechnologie - wie Bluetooth - auf Frequency Hopping Spread Spectrum (FHSS) und erzielten damit Bruttodatenraten von 1 und später - durch Übertragung von 2 Bit pro „Symbol“ - 2 Mbit/s. Beim FHSS-Verfahren wird die Trägerfrequenz 2,5 mal pro Sekunde gewechselt. Solche Komponenten werden aber heute kaum mehr angeboten.

Neben dem FHSS-Verfahren wird in modernen Geräten heute Direct Sequence Spread Spectrum (DSSS) als Übertragungstechnologie benutzt. Mit DSSS lassen sich Bruttodatenraten von 11 Mbit/s erzielen. Aus Gründen der Abwärtskompatibilität (und beim Verbindungsaufbau) müssen IEEE802.11b-Geräte jedoch noch die Datenraten bis herab zu 1 Mbit/s beherrschen. Um Übertragungsraten von 22 bis 54 Mbit/s erreichen zu können, wird als Übertragungstechnologie Orthogonal Frequency Division Multiplexing (OFDM) eingesetzt.

Übrigens: Werden Geräte nach der WLAN-Norm und Bluetooth-Endgeräte zusammen eingesetzt, kann es - insbesondere wegen des wesentlich agressiveren Medienzugriffsverfahrens bei Bluetooth – zu sehr deutlichen Performanceeinbrüchen im WLAN kommen [1].

2.1.3 Störquellen

Bedingt durch die große Anzahl von ISM-Geräten (alleine in Deutschland mehrere Millionen) ist eine gegenseitige Beeinflussung bzw. Störung oft unvermeidbar[4]: Die jeweiligen Empfänger empfangen ja nicht nur die eigenen, gewünschten Signale, sondern auch die von anderen, in der Nachbarschaft betriebenen Geräten. Im Gegensatz zum Mobilfunk findet hier keine kontrollierte Aufstellung oder Kontrolle der vorhandenen Sendeanlagen und deren Frequenzen statt. Die Hersteller versuchen, die dadurch entstehenden Probleme zwar durch entsprechende Bauweise wie etwa Codierung der geräteeigenen Signale zu vermindern, doch dies hilft (besonders bei einfach und preiswert gefertigten Geräten) nur in begrenztem Maße. Störungen durch gegenseitige Beeinflussung sind deshalb unausweichlich.

Nicht ohne Grund steht in den Nutzungsbestimmungen der in Deutschland gültigen Frequenzbereichszuweisungsplanverordnung zu den ISM-Frequenzen: "Funkdienste, die innerhalb dieser Frequenzbereiche wahrgenommen werden, müssen Störungen, die durch diese Anwendungen gegebenenfalls verursacht werden, hinnehmen." Der Einsatz von Geräten,

[4] Beispiele: Babyphones, Fahrzeugöffner, Funkalarmanlagen, Handfunkgeräte, Garagentoröffner, PC-Funkmäuse, Funkmikrophone, Wegfahrsperren, Drahtlose PC-Tastaturen, Funk-Kopfhörer, Zutrittskontrollsysteme, Paging-Systeme, Videoübertragungssysteme, Funkthermometer, Fernsteuerungen, Drahtlose Bewegungsmelder

welche mit ISM-Frequenzen arbeiten, ist also nur dann sinnvoll, wenn es nicht so sehr auf eine störungsfreie Funkverbindung ankommt, Störungen nur vorübergehend auftreten und hingenommen werden können und nur kurze Entfernungen zu überbrücken sind.

Dies ist der Preis, der dafür zu zahlen ist, dass auf Wunsch der Verbraucher und Hersteller mit den ISM-Frequenzen die Möglichkeit geschaffen wurde, mit preiswerten Geräten ohne große Formalitäten einfache Funkübertragungen zu realisieren.

2.1.4 Szenarien

Durch breite Nutzung der Mobilfunknetze ist auch die Nachfrage nach mobilen schnellen Internetverbindungen gestiegen. Mobile Benutzer benötigen einen Internet-Zugang vor allem dann, wenn sie sich irgendwo stationär aufhalten. Um in solchen Situationen einen Internet-Zugang zu ermöglichen, werden auf der Basis von Funknetzen so genannte Hotspots eingerichtet. Unter einem Hotspot (auch Public Spot) versteht man einen Bereich, der über ein WLAN dem Benutzer Zugang zum Internet gewährt. In der Regel werden hierzu handelsübliche Access Points, die nach dem Standard 802.11g arbeiten, verwendet. Zunächst gab es solche Angebote nur in den Wartebereichen von Flughäfen, in Hotels und Kongresszentren oder Internet-Cafés. Doch die Angebote wachsen; auch andere Anbieter, große Handelsketten beispielsweise, bieten heute Hotspots an. Das Hotspot-Angebot ist allerdings in der Regel nicht kostenlos. Für den mobilen Netzzugang ist eine Gebühr zu entrichten, die über verschiedene Wege erhoben und abgerechnet wird. Für Hotspots gibt es eine Reihe von Angeboten, grundsätzlich gilt aber bei allen:

- Der Anwender muss neben einem WLAN-Anschluss über keine besonderen Komponenten verfügen.
- Der Betreiber definiert seine eigenen Gebühren, je nach Angebot.
- Die Onlinezeit wird beispielsweise über "Rubbelkarten" (Scratch-Cards) auf kundenfreundlicher Minutenbasis abgerechnet.
- Bei großen Hotels besteht oft das Angebot eines 24-Stunden Accounts (unabhängig von der Onlinezeit).
- Darüber hinaus gibt es die Möglichkeit eines festen Vertrages und somit monatlicher Abrechnung für den Endkunden.

Neben den öffentlichen Netzzugängen (Hotspots) wird die WLAN-Technik auch zur Vernetzung von Firmennetzen und Krankenhausnetzen eingesetzt. Das Ziel dort ist nicht der öffentliche Netzzugang, sondern die Kommunikation der verschiedenen Unternehmens- und/oder Organisationsbereiche.

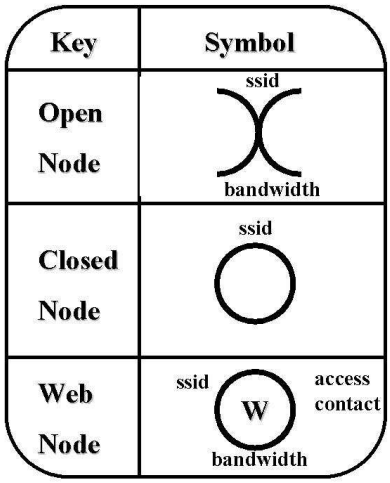
Im privaten Bereich werden WLAN-Funknetze in der Regel dazu verwendet, den Internetzugang über einen DSL-Anschluss kostengünstig zu realisieren.

2.2 Gefahren beim Einsatz

2.2.1 Abhören von WLAN-Verbindungen

Eine der häufigsten beschriebenen Gefahren ist das Ausspionieren und Ausspähen von WLAN-Funknetzen. Im Internet stehen hierzu kostenlose Cracker-Tools zur Verfügung, mit denen selbst Laien auf recht einfache Art und Weise Mängel in WLANs aufdecken können. Mit nur geringfügig mehr Know-how können transferierte Daten abgehört und nach Analyse einer entsprechend großen Datenmenge in Echtzeit entschlüsselt werden. In der Folge ist es dann kein großer Aufwand mehr, manipulierte Daten in WLANs einzuspeisen oder aber die Access Points der WLAN-Verbindungen gezielt anzugreifen, um so Zugang zu den "verkabelten" Netzwerken herzustellen.

Das Ausspähen von offenen WLANs ist heute weit verbreitet. Zur Erleichterung der Suche werden ausgespähte WLANs durch Kreidezeichnungen an Wänden etc. gekennzeichnet (Warchalking = „neues Hobby“ um gefundene Netze durch Kreidekreiszeichen zu markieren). Im Einzelnen sind folgende Kennzeichnungen möglich:



2.2.2 Erstellung von Bewegungsprofilen

Jedes WLAN-Gerät besitzt eine eindeutige MAC-Adresse. Die übertragenen MAC-Adressen werden auch bei der Nutzung von WEP nicht verschlüsselt. Die MAC-Adressen können zum Verfolgen einzelner WLAN-Geräte missbraucht werden. Mit Hilfe sog. „Location-Tracking“-Systeme sind Benutzer mit einer Genauigkeit von ca. 10 m lokalisierbar. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen.

2.2.3 Stören der Funkverbindung

Eine weitere Gefahrenquelle bildet das gezielte Stören von Funkverbindungen, um den Datenaustausch zu unterbinden. Es existieren derzeit keine effektiven Verfahren, die Verfügbarkeit der Funkverbindung sicherzustellen. Schon bei der Planung von Funknetzen sollten daher entsprechende Backup- und Notfallkonzepte vorgesehen werden.

2.3 Sicherheitsmaßnahmen

Funknetze sind leichter abzuhören oder zu beeinflussen als drahtgebundene Netze oder gar Lichtwellenleiter. Es ist daher unabdingbar, die in den WLAN-Komponenten implementierten Sicherheitseinrichtungen zu nutzen. Sollen sensible personenbezogene Daten (z. B. Gesundheits- und Personaldaten) in Funknetzen übertragen werden, so reichen die derzeit standardmäßig in den WLAN-Komponenten enthaltenen Sicherheitsfunktionalitäten nicht aus. Es müssen daher geeignete zusätzliche Maßnahmen (s. 2.4) ergriffen werden.

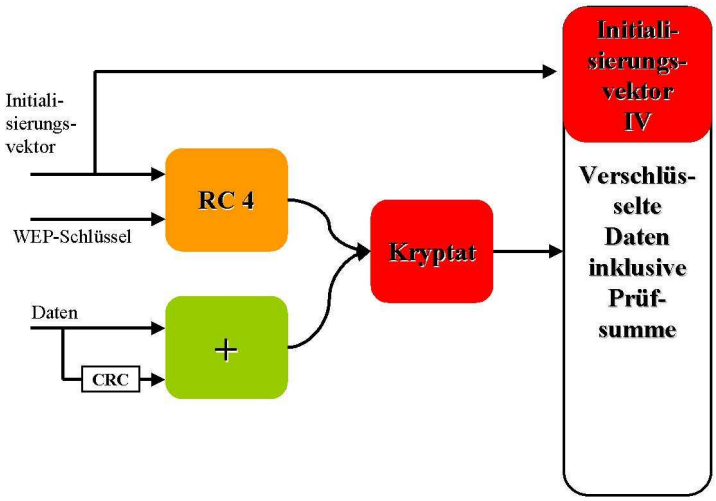
Schon bei der Planung von Funknetzen sollte geprüft werden, ob die zu beschaffenden WLAN-Komponenten dem Stand der Technik entsprechen und die derzeit aktuellen Sicherheitsfunktionalitäten auch unterstützen (s. 2.3.4 und 2.3.6).

2.3.1 Schwache Verschlüsselung mit WEP

Zur Verhinderung des Abhörens von WLANs wurde das Wired Equivalent Privacy (WEP) Protokoll entwickelt. Dieses soll ein Abhören der Funkübertragung verhindern oder zumin-

dest erschweren. Ein sekundäres Ziel war die Realisierung einer Zugriffskontrolle auf das WLAN. WEP soll etwa das Sicherheitsniveau eines Kabel-Ethernet erreichen. WEP enthält folgende Elemente:

- Verschlüsselung mit Stream Cipher RC4
  RC4 ist ein Algorithmus zur Stromchiffrierung der Firma RSA Security. Das von Prof. Ronald Rivest entwickelte symmetrische Verfahren verschlüsselt Byte-weise mit einem Schlüssel variabler Länge. Der Algorithmus basiert auf der Benutzung einer zufälligen Permutation. Er gilt als eine schnelle Methode zur Verschlüsselung (der Algorithmus war sieben Jahre lang geheim, bis 1994 der Quellcode anonym veröffentlicht wurde).
- den Partnern ist ein geheimer Schlüssel bekannt (shared secret key)
- Integrity Check zur Integritätsprüfung linear, d. h. leicht für einen Angreifer stimmend zu machen!
- 24 Bit Initialization Vector (IV) soll identische verschlüsselte Daten bei identischem Klartext verhindern, wird unverschlüsselt übertragen.



Nach den Vorgaben des Standards kommt dabei der Algorithmus RC4 mit einem 64-Bit-Schlüssel zum Einsatz. Die ersten 24 Bit werden als so genannter Initial Vector benutzt; damit reduziert sich die verwendbare Schlüssellänge auf 40 Bit.

Der im WEP-Protokoll verwendete 40 Bit lange Schlüssel (Key) muss in einem WLAN sowohl dem Access Point als auch dem WLAN-Client bekannt sein. Er wird deshalb über eine spezielle Management-Software des Access Point oder bei den Eigenschaften der WLAN-Karte eingegeben. Sowohl am Access Point wie auch beim Client sind die zu verwendenden WEP-Schlüssel manuell zu konfigurieren.

Dem eingegebenen Schlüssel werden intern noch 24 Bit, der so genannte Initialisierungsvektor (Initialization Vector), vorangestellt; daraus ergibt sich dann die Schlüssellänge von 64 Bit. Aus diesem Startwert berechnet der WEP-Algorithmus einen fortwährenden Strom aus Chiffrierbits (Stream Cipher). Mit diesen werden die zu übertragenden Daten mit Hilfe der logischen Exklusiv-Oder-Funktion (XOR) kodiert. Vor das auf diesem Weg entstandene Datenpaket wird der Initialisierungsvektor gestellt und das Ergebnis an den Empfänger geschickt. Anhand des mitgelieferten Initialisierungsvektors ist dieser in der Lage, denselben Chiffrierstrom zu berechnen, der zur Verschlüsselung der Informationen verwendet wurde. Durch erneute Anwendung der XOR-Funktion entschlüsselt der Empfänger die erhaltenen Informationen. Die Übermittlung des zur Codierung verwendeten Initialisierungsvektors im Klartext ist eine der Schwachstellen von WEP. Beim Einsatz von Chiffrierströmen ist tunlichst

darauf zu achten, dass nie zwei Nachrichten mit demselben Schlüssel kodiert werden. Der Grund ist einfache Mathematik. Es sei S der verwendete Schlüssel, N1 und N2 die Nachrichten, dann gilt für die verschlüsselten Informationen C1 und C2:

C1 = N1 xor S
C2 = N2 xor S

Fängt nun ein Lauscher beide Nachrichten C1 und C2 ab, kann er eine einfache Berechnung anstellen:

C1 xor C2 = N1 xor S xor N2 xor S

oder umgruppiert:

C1 xor C2 = N1 xor N2 xor S xor S

da sich die beiden XOR-Verknüpfungen mit S gegenseitig aufheben ergibt sich also:

C1 xor C2 = N1 xor N2

Mit anderen Worten: Der Lauscher ist im Besitz der XOR-Verknüpfung beider Originalnachrichten. Mit Hilfe einfacher stochastischer Verfahren lässt sich damit in vielen, wenn nicht sogar in den meisten Fällen, der Originaltext beider Nachrichten herausfinden. Dies beruht zum Teil auf dem zu kleinen Schlüsselraum des genannten Initialisierungsvektors (IV) wie folgendes Rechenbeispiel zeigt:

8 Mbit/s, 1000-Byte-Pakete, d. h. 1 ms/Paket ergibt 16777,216s für 2^24 Pakete, ca. 4,6h

Der Initialisierungsvektor wiederholt sich also nach einigen Stunden, damit liegt dann auch der gleiche Schlüsselstrom vor.

Als Ergebnis kann letztendlich festgehalten werden, dass WEP nicht dem Stand der Technik entspricht und auch keine genügende Datensicherheit mehr bietet.

2.3.2 Verschlüsselung mit WEP128

Aufgrund der mangelnden Sicherheit von WEP wurde die Schlüssellänge auf 128 Bit erhöht, was zu einer verwendbaren Nutzungsschlüssellänge von 104 Bit führt. Diese Version wird manchmal mit WEP128 bezeichnet.

Trotzdem gibt es nach wie vor Kritik an WEP. Hintergrund hierfür sind Attacken, die auch bei der Verwendung von 128 Bit-Schlüsseln durch bloßes Mithören der Funkstrecke zu einer Rekonstruktion der Schlüssel führen können[5].

Insgesamt gesehen wird durch den Einsatz von WEP mit 128-Bit-Schlüsseln das Funk-LAN kaum sicherer, denn die Probleme mit dem Verschlüsselungsalgorithmus RC4, den zu kurzen Initialisierungsvektoren sowie dem Schutz der Checksumme gegen Manipulationen bleiben weiterhin bestehen.

[5] Avi Rubin und John Joannidis von den AT&T Research Labs sowie Adam Stubblefield von der Rice University haben eine Arbeit veröffentlicht, in der sie nachweisen, dass nur wenige Stunden notwendig sind, um auf einem mittelmäßig ausgelasteten drahtlosen Netzwerk einen WEP128-Schlüssel (104 Bit) zu rekonstruieren. Die dazu erforderliche Ausrüstung bestand aus einem handelsüblichen Wireless-LAN-Adapter unter Linux sowie Tools wie TCPDUMP oder dem frei verfügbaren Netzwerkanalysator Ethereal.

Aufgrund der bekannten Schwachstellen sollte das WEP-Protokoll auch mit 104 Bit langen Schlüsseln nicht mehr verwendet werden. Alternative Lösungsmöglichkeiten stehen mit dem neuen Sicherheitsstandard IEEE 802.11i (s. 2.3.4) bereits zur Verfügung.

2.3.3 Wi-Fi Protected Access (WPA)

WPA steht für Wi-Fi Protected Access. Hierbei zertifiziert die Wi-Fi Alliance [4] neue Implementierungen für mehr Sicherheit und bildet eine Teilmenge des WEP-Nachfolgestandards 802.11i. Hierbei soll z. B. TKIP als verbesserte Funktion zur Verschlüsselung die WEP-Schwäche kompensieren. Während WEP ausschließlich einen statischen Schlüssel benutzt, der sich durch das Analysieren vieler Pakete ermitteln ließe, ist die Schüsselvergabe hier dynamisch - es wird nach jedem gesendeten 10-Kbyte-Paket ein neuer Schlüssel vergeben. Auch wurde der Initialisierungsvektor erweitert. Eine weitere Komponente ist der Message Integrity Check. Hier erfolgt eine Überprüfung der Nachricht auf Integrität, was viel Performance benötigt. Eine offensichtliche Schwäche könnte jedoch auch vorliegen, da der TKIP-Algorithmus ebenfalls auf dem RC-4 Stromverschlüsselungsverfahren basiert.

2.3.4 Neuer Sicherheitsstandard IEEE 802.11i

Ende Juni 2004 wurde der Sicherheitsstandard IEEE 802.11i verabschiedet. Dieser Standard wird von der WiFi Alliance [4] auch als Wi-Fi Protected Access 2 (WPA2) bezeichnet und basiert weitgehend auf WPA. Damit stehen neue Sicherheitsmechanismen für WLANs zur Verfügung:

- Temporal Key Integrity Protocol (TKIP)
  - Message Integrity Check (MIC) "Michael" mit 64-Bit-Schlüssel
  - Sequenznummer gegen Replay (48 Bit)
  - Verschlüsseln mit "Per-Packet"-Schlüssel (aus Basisschlüssel, Sequenznummer ...)

- Counter-Mode-CBC-MAC (CCMP)
  - Advanced Encryption Standard (AES) als Verschlüsselungsverfahren
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) zur Integritätssicherung

Für das Schlüsselmanagement nutzt IEEE 802.11i das Extensible Authentication Protocol (EAP). Mit Hilfe von EAP können Kommunikationspartner die verwendete Authentifizierungsmethode aushandeln.

Wird WPA mit einem vorher ausgetauschten Schlüssel (PSK = pre-shared key) genutzt, so muss dieser Schlüssel vor unberechtigter Kenntnisnahme geschützt werden. Hier stellt sich dieselbe Problematik wie beispielsweise bei der Nutzung eines einheitlichen Administratorkennworts für alle Rechner.

Außerdem wurde bereits kurz nach der Verabschiedung des Sicherheitsstandards IEEE 802.11i in [27] beschrieben, dass im Standard IEEE 802.11i ein bekanntes Sicherheitsproblem bei der Verwendung von PSK nicht im nötigem Umfang berücksichtigt wurde. Es besteht unter Umständen die Möglichkeit, dass die Übertragung von verschlüsselten Sitzungsschlüsseln zwischen Radius-Server und Access Point abgehört werden kann. Bei der Auswahl der Radius-Passwörter sollten daher zu kurze oder triviale Zeichenketten vermieden werden.

2.3.5 Netzwerkname SSID

Unter SSID - Service Set Identifier Description ist der Name für ein WLAN, das auf IEEE 802.11 basiert, zu verstehen. Der Name kann nach dem Standard bis zu 32 Zeichen lang sein. Er wird in der Regel im Access Point eines WLANs konfiguriert und ist von allen

Clients, die darauf Zugriff haben sollen, einzustellen. Der Name wird allen Paketen unverschlüsselt vorangestellt und ist somit über die Luftschnittstelle auslesbar. Der Netzwerkname dient dazu, mehrere Netzwerke voneinander zu unterscheiden. Das erleichtert den Benutzern, das richtige Netz zu finden, aber leider auch dem Angreifer. Verlangt ein Client den Zugang zu einem WLAN, senden alle erreichbaren Access Points ihre SSID, so dass aus einer Liste ausgewählt werden kann, zu welchem man Zugang wünscht. Da dies eine Sicherheitslücke darstellen kann, sollte der Broadcast der SSID am Access Point deaktiviert werden.

In der Regel verschicken alle Wireless-Geräte ihre SSIDs per Default, dies führt dazu, dass es zu unerwünschter Kommunikation zwischen Geräten kommen kann. Deshalb sollte diese Funktion abgeschaltet werden, damit können nur die Karten mit der korrekten SSID miteinander kommunizieren. Stockwerke, Organisationsnamen oder Namen sind als SSID völlig ungeeignet, denn sie verraten einem potenziellen Angreifer bereits, wem das Netzwerk gehört, wo es sich befindet und ob sich ein Einbruchsversuch lohnen könnte. Als SSID bieten sich Namen an, die für den Anwender eine Bedeutung haben, aber für niemanden sonst. Beim Betrieb eines Hotspot wird die SSID ANY (engl. beliebig) eingestellt, um den Zugang zu ermöglichen.

2.3.6 Reduzierung der Sendeleistung

Neuere Access Points ermöglichen eine dynamische Anpassung ihrer Sendeleistung an die Notwendigkeit der vorhandenen WLAN-Clients. Damit wird erreicht, dass die Sendeleistung des WLANs auf ein erforderliches Maß reduziert wird. Dadurch können die unerwünschte Abstrahlung und damit potenzielle Angriffe auf das Funknetz reduziert werden.

2.3.7 Abschalten der Access Points

Access Points sollten außerhalb der normalen Nutzungszeiten abgeschaltet werden. Damit ist ein unberechtigter Zugang zum Funknetz ausgeschlossen. In der Praxis hat sich hierbei der Einsatz von Schaltuhren bereits bewährt.

2.3.8 MAC-Filterlisten

Die MAC-Filterliste in einem Access Point definiert, welche MAC-Adressen als Teilnehmer des WLANs zugelassen sind. Die Verwendung solcher MAC-Filterlisten bieten jedoch nur einen geringen Schutz gegen unberechtigte Nutzer, da die MAC-Adressen der WLAN-Adapter in den meisten Fällen relativ leicht manipuliert werden können.

2.4 Zusätzliche Sicherheitsmaßnahmen

Werden personenbezogene Daten mit niedrigem oder mittlerem Schutzbedarf in einem WLAN übertragen, so ergibt sich nach dem derzeitigen Stand der Technik folgende Zuordnung zu den systemimmanenten Sicherheitsstandards:

	WEP/WEP128	**WPA**	**802.11i (WPA2)**
Verschlüsselung	RC4	RC4	AES
Schlüssellänge	40 Bit/104 Bit	128 Bit	128 Bit
Initialisierungsvektor	24 Bit	48 Bit	48 Bit
Key Management	nicht vorhanden	EAPol-basiert	EAPol-basiert
Übertragung personenbezogener Daten	nur mit zusätzlicher Verschlüsselung (siehe Abschnitt 6.2)	Daten mit mittlerem Schutzbedarf	Daten mit mittlerem Schutzbedarf

Die in den vorherigen Abschnitten aufgezeigten Sicherheitsmaßnahmen entsprechen entweder nicht mehr dem aktuellen Stand der Technik (z. B. schwache Verschlüsselung mit

WEP), bieten nur teilweisen Schutz (z. B. Abschaltung des Access-Points) oder sind mehr oder minder leicht überwindbar (z. B. MAC-Filterlisten, Reduzierung der Sendeleistung).

Lediglich WPA2 bzw. IEEE 802.11i bietet (bei ausreichender Schlüssellänge und -komplexität) mit Pre-Shared-Keys ("Private") oder aber in Verbindung mit verschiedenen Varianten von EAP ("Enterprise") einen ausreichenden Schutz für Daten mit mittlerem Schutzbedarf.

Bei der Beschaffung von neuer oder dem Ersatz von alter Hardware und der Planung von neuen Infrastrukturen sollte aus diesem Grund darauf geachtet werden, dass lediglich Geräte eingesetzt werden, die den aktuellen Sicherheitsstandards (WPA2, IEEE 802.11i) genügen.

Dennoch bleibt festzuhalten, dass sämtliche bisher vorgestellten Sicherheitsmaßnahmen für einen datenschutzgerechten Einsatz bei der Verarbeitung von sensiblen personenbezogenen Daten nicht ausreichend sind.

Hierbei sollten die Grundbedrohungen wie Verlust der Vertraulichkeit (ausschließlich Befugte können die übertragenen Daten zur Kenntnis nehmen), Verlust der Integrität (die Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell) und Verlust der Authentizität (die Daten können jederzeit ihrem Ursprung zugeordnet werden) gewährleistet sein.

Die nun folgende Aufzählung soll kurz aufzeigen, wie eine Reduzierung der Risiken durch den Einsatz verschiedenster Technologien umgesetzt werden kann:

- Die Trennung von Internet, Intranet und WLAN durch jeweils eine **Firewall** sollte obligatorisch sein. Hierbei sollen unberechtigte Zugriffe auf ein Netz oder Netzsegment blockiert werden. Zwar könnten die übertragenen Daten abgehört werden, aber das interne Netz bleibt hinter der Firewall geschützt (s. 6.1).

- Für die Absicherung des Datenstroms auf der Funknetzstrecke sollte ein **VPN-Tunnel**, der die auszutauschenden Daten zwischen dem WLAN-Client und der Firewall durch zusätzliche Verschlüsselungstechnik – z. B. IPSec – schützt, aufgebaut werden (s. 6.2).

- Eine weitere Maßnahme zur Erhöhung der Sicherheit bei der Anmeldung an der Basisstation stellt der **Radius-Server** dar, der für eine gesichertere Authentifikation sorgt (s. 6.3).

- Zum Schluss darf natürlich nicht die Sicherheit der WLAN-Clients und hier insbesondere die **Problematik von Schadprogrammen** vergessen werden, da der Komfort dieser mobilen Computer leider auch Angriffsmöglichkeiten, z. B. von Viren, nach sich zieht. Hierbei könnten Daten z. B. verfälscht oder gelöscht werden. Da die Sicherheitsmechanismen eines Betriebssystems meist nicht ausreichen, kann durch den Einsatz von Virenschutzprogrammen und einer Personal Firewall, die meist durch den Nutzer selbst installiert, konfiguriert und verwaltet werden, sehr wirksam gegen Angriffe z. B. aus dem Internet begegnet werden (s. 6.4).

Auf dieser Grundlage können die Risiken für WLANs durch Anwendung der beschriebenen Sicherheitsmechanismen minimiert werden - zumindest was die heutigen Angriffstechniken betrifft. Dies setzt aber voraus, dass die bereitstehenden Sicherheitsmaßnahmen auch tatsächlich umgesetzt werden. Natürlich muss auch die Verhältnismäßigkeit gewahrt bleiben, sodass Teile der oben genannten Lösungen für Netzwerke, wo keine Verarbeitung von sensiblen personenbezogenen Daten erfolgt, kaum realisierbar erscheinen. Hier muss eine Abwägung des Schutzbedarfs erfolgen.

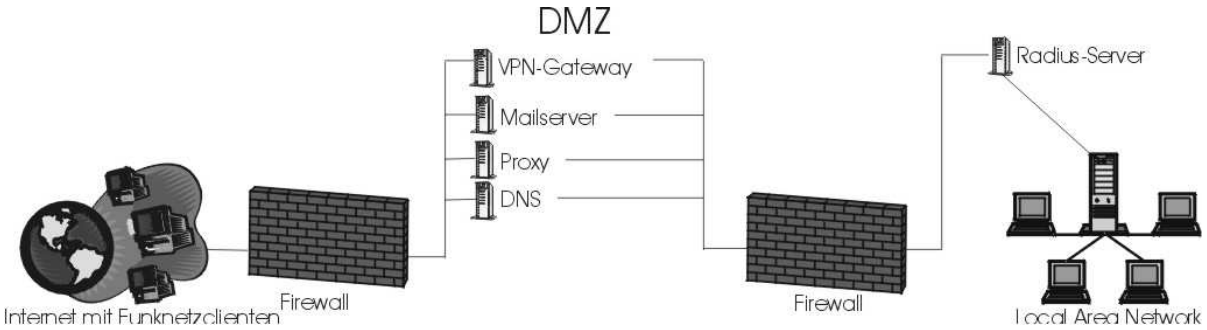
Weiterhin muss die Sicherheit stets überprüft und verbessert werden (Sicherheits-Management). Z. B. muss auf neue Gefahren reagiert werden oder die in der Zwischenzeit entdeckten Sicherheitslücken müssen mit so genannten Patches behoben werden.

Über die technischen Möglichkeiten hinaus sollte dringend eine Sensibilisierung der Nutzer im Umgang mit WLANs erfolgen. Es sollten organisatorische Maßnahmen getroffen werden, die folgende Punkte enthalten:

- Aufstellung einer Sicherheitsrichtlinie, die sich am Sicherheitskonzept für das LAN orientiert. Diese Richtlinie ist ständig auf Aktualität zu prüfen und gegebenenfalls anzupassen.

- Die Erstellung dieser Sicherheitsrichtlinie ist für das Erkennen und Ausschließen von möglichen Risiken von grundlegender Bedeutung. Doch deren zeitnahe Umsetzung und Prüfung auf Einhaltung gewähren erst die gewünschte und wohl auch notwendige Sicherheit.

Die folgende Skizze soll zusammenfassend veranschaulichen, wie eine mögliche Konfiguration aussehen könnte:



Kurze Erläuterung zur Skizze: Die Funknetzwerkclienten verschlüsseln den Datenverkehr per VPN-Tunnel im Internet, gehen durch die Firewall zum VPN-Gateway, dann durch die zweite Firewall ins Local Area Network, wo z. B. der Radius-Server für die Authentifizierung steht.

Natürlich gibt es weitere Lösungsmöglichkeiten. Für einen geringeren Schutzbedarf kann die Lösung heißen, dass die Firewall und das VPN-Gateway im Access Point integriert sind. Von Vorteil ist hier, dass z. B. nicht so viele Geräte benötigt werden und dadurch auch der Administrationsaufwand geringer ist. Wird dieses „Multifunktions“-Gerät jedoch kompromittiert, so ist möglicherweise das gesamte LAN gegenüber Angriffen ungeschützt.

2.5 Proprietäre Lösungen

Natürlich entstehen auch proprietäre Lösungen zur Absicherung eines WLANs. Z. B. wird beim Lightwight- Extensible Authentication Protocol (LEAP) von Cisco das Message-Integrity-Check (MIC)-Verfahren benutzt, um das Verfälschen von Nachrichten zu verhindern. Dies dient z. B. der Verhinderung von Man-in-the-Middle-Angriffen, da sich der WLAN-Client und Access Point gegenseitig authentifizieren müssen.

Eine andere Lösung ist „Dynamic Link Security“ der Firma 3Com. Es erfolgt eine 128-Bit-Verschlüsselung, die nicht auf dem RC-4-Verfahren beruht. Jede Session und Anwender erhalten einen dynamischen Schüssel.

Diese beiden Beispiele sollen aufzeigen, dass auch proprietäre Lösungen von Firmen entwickelt werden. Der Nachteil ist jedoch meist, dass man sich auf die Produkte eines einzigen Herstellers festlegen muss, da Fremdprodukte in dieser Umgebung nicht funktionieren. Wei-

terhin besteht bei proprietären Lösungen die Gefahr, dass entsprechende Produkte nicht mehr weiterentwickelt werden.

2.6 Ausblick

Ende Juni 2004 ist der neue Standard IEEE 802.11i verabschiedet worden. Damit stehen neue Sicherheitsmechanismen (u. a. AES und TKIP) für WLANs zur Verfügung. Die Wi-Fi-Alliance hat bereits erste Produkte zertifiziert.

Noch in Arbeit befindet sich derzeit der Standard IEEE 802.11e. Er soll Voice- und Video-Anwendungen im WLAN durch QoS unterstützen. Damit wird erreicht, dass zeitkritischen Diensten im WLAN eine höhere Priorität zugewiesen werden kann.

3 Bluetooth

Für den Aufbau drahtloser Ad-Hoc-Verbindungen über kurze Distanzen zwischen Geräten unterschiedlicher Art ist der Bluetooth-Standard gedacht, der inzwischen von mehr als 2500 Herstellern unterstützt wird. Durch sinkende Chippreise ist zu erwarten, dass Bluetooth mit konkurrierenden Kommunikationsstandards wie DECT, WLAN, IrDA, ISDN und UMTS mithalten kann und zukünftig auch vermehrt für die Übertragung sensibler Daten genutzt wird.

Der Bluetooth Standard verdankt seine Entstehung einer Initiative von Ericsson Mobile Communications. Zusammen mit Nokia, IBM, Intel und Toshiba gründete Ericsson im Mai 1998 die „Special Interest Group“ (SIG) mit dem Ziel, einen herstellerunabhängigen Standard für Peer-to-Peer-Datenkommunikation über kurze Distanzen zu schaffen, die sich zu geringen Hardware-Kosten realisieren lassen.

Der Standard wurde nach dem Wikinger Harald Blåtand (deutsch: Harald Blauzahn, englisch: Harald Bluetooth), König von Dänemark (940-981 n. Chr.) benannt, der die Christianisierung und die Vereinigung von Dänemark und Norwegen bewirkte. In Jelling (DK) errichtete Harald Blåtand einen Runenstein mit der Inschrift: “König Harald errichtete dieses Monument zu Ehren von Gorm, seinem Vater und Thyre, seiner Mutter, der (selbe) Harald, der alle Dänen und Norweger gewann und die Dänen zu Christen machte“. In Analogie wurde im September 1999 am Hauptsitz von Ericsson Mobile Communications in Lund ein Runenstein zu Ehren von Harald Blåtand errichtet.

3.1 Grundlagen

Bluetooth ist ein offener Industriestandard (vgl. IEEE 802.15.1-2002 [5]) für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking).

3.1.1 Technische Grundlagen

Bluetooth arbeitet im 2,4-GHz-ISM-Frequenzband auf 79 Kanälen bei den Frequenzen f = (2402 + k) MHz, k = 0,...,78.

Die Übertragung der GFSK-modulierten Datenpakete erfolgt zeitschlitzgesteuert (TDD) in Verbindung mit einem Frequenzsprungverfahren (FHSS). Dies dient zur Reduzierung der Empfindlichkeit gegenüber Störungen. Die Zeitschlitzlänge beträgt 625µs; daraus resultiert eine Frequenzwechselhäufigkeit von bis zu 1600 hops/s (für 1-slot-Pakete). Die Hopping-Sequenz ist pseudozufällig und wiederholt sich nach ca. 23,3 Stunden.
Bluetooth unterstützt asynchrone verbindungslose (ACL-)Übertragung mit maximal 723,2 kbit/s in der einen und 57,6 kbit/s in der anderen Richtung (asymmetrisch) bzw. mit maximal 433,9 kbit/s in beide Richtungen (symmetrisch). Für Sprachübertragung stehen bei Bluetooth bis zu drei synchrone verbindungsorientierte (SCO-) Kanäle mit je 64 kbit/s zur Verfügung; die Sprachkodierung erfolgt entweder über PCM oder CVSD-Modulation.

Die Reichweite hängt von der Sendeleistung ab und reicht von bis zu 10 Metern bei Klasse3-Geräten (bis 1mW Sendeleistung) bis zu ca. 100 Metern bei Klasse1-Geräten mit bis zu 100 mW Sendeleistung.
Hinsichtlich der Sendeleistung und Reichweite werden drei Geräteklassen unterschieden:

Klasse 1:	Sendeleistung	1-100mW (0bis 20dBm, Reichweite ca. 100m)
Klasse 2:	Sendeleistung	0,25-2,5mW (-6bis 4dBm, Reichweite ca. 10m)
Klasse 3:	Sendeleistung	bis 1mW (bis 0dBm, Reichweite ca. 0,1-10m)

Zur Senkung des Stromverbrauchs sind Spar-Modi (Sniff-, Park- und Hold-Mode) und Sendeleistungsregelung (Power Control) spezifiziert.

3.1.2 Protokollarchitektur

Neben den hardwarenahen Protokollen (Funktechnik und Basisband) definiert die Spezifikation für das Verbindungsmanagement eine Link-Schicht, die neben Fehlerkorrekturverfahren auch kryptographische Sicherheitsmechanismen bereitstellt. Zusätzlich verfügt sie über eine Host-Controller-Schnittstelle sowie diverse weitere Protokolle für unterschiedliche Applikationen. Eine ausführliche Beschreibung des Bluetooth Protokollstacks findet man in der Literatur (z. B. in [8]). Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, hat die SIG so genannte Anwendungs-Profile definiert. Neben grundlegenden Profilen wie zum Beispiel dem Generic Access Profile, dem Serial Port Profile oder dem Generic Object Exchange Profile gibt es beispielsweise ein Headset Profile, ein LAN Access Profile, ein PAN (Personal Area Networking) Profile usw.

3.1.3 Verbindungsaufbau und Netztopologien

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die so genannte Bluetooth Device Address.

Der Verbindungsaufbau erfolgt über Inquiry und Paging.

Inquiry

Per Inquiry-Prozedur kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Nach einem Inquiry liegen alle Geräteadressen und Zeittakte der gefundenen kommunikationsbereiten Geräte vor.

Paging

Durch eine Paging-Anforderung kann nun eine Kommunikationsverbindung zu einem dieser Geräte aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Für den Verbindungsaufbau wird die Sprungsequenz des Slaves verwendet, die so genannte Page-Hopping-Sequence. Während des Pagings sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave. Für die weitere Kommunikation wird anschließend die Sprungsequenz des Masters verwendet, die so genannte Channel-Hopping-Sequence.
Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten unterstützt Bluetooth auch Punkt-zu-Mehrpunkt-Verbindungen.
Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem so genannten Piconet als Slaves im Park-Mode mit einem Master vernetzt sein. Zusätzlich können bis zu 7 Slaves gleichzeitig aktiv mit dem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel-Hopping-Sequence und dem Zeittakt des Masters. Prinzipiell sieht Bluetooth sogar die Möglichkeit einer Vernetzung von bis zu zehn Piconets zu einem so genannten Scatternet vor. In der Praxis kommen solche komplexen Netztopologien aber zurzeit noch selten vor.
Zusammenfassend gibt es drei verschiedene Bluetooth-Kommunikationsverbindungen:

- **Punkt zu Punkt-Verbindung** zwischen genau zwei Bluetooth Einheiten, dabei agiert eine Einheit als Master, die andere als Slave.

- **Piconet:** Kleines Netzwerk von bis zu acht Bluetooth-Einheiten; auch hier haben wir einen Master und bis zu sieben Slaves.

- **Scatternet:** Zusammenschluss von bis zu zehn Piconets; hier übernimmt jeweils eine Einheit gegenüber den eigenen Piconet die Funktion des Masters, reagiert aber gegenüber dem Master des Piconets als Slave.

3.1.4 Kryptographische Sicherheitsmechanismen

Da Bluetooth ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass "unberechtigte" bluetoothfähige Geräte die Bluetooth-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Die in der Bluetooth-Spezifikation vorgesehenen kryptographischen Sicherheitsmechanismen haben die Ausschaltung dieser zwei Bedrohungen zum Ziel. Neben nicht-kryptographischen (Korrektur-)Verfahren zum Schutz gegen Übertragungsfehler sieht die Spezifikation kryptographische Authentisierungs- und Verschlüsselungs-Algorithmen vor. Diese sind bereits auf Chip-Ebene implementiert und stehen auf der Link-Schicht einheitlich zur Verfügung.
Basis aller eingesetzten kryptographischen Verfahren sind Verbindungsschlüssel (Link Keys), die jeweils zwischen zwei Bluetooth-Geräten während der so genannten Paarung vereinbart werden.

Paarung (Pairing) und Verbindungsschlüssel

Wenn zwei Bluetooth-Geräte kryptographische Sicherheitsmechanismen nutzen wollen, müssen sie zuvor miteinander "gepaart" werden. In der Regel wird dabei ein nur für die Verbindung dieser beiden Geräte genutzter, 128 Bit langer Kombinationsschlüssel (Combination Key) erzeugt und in jedem Gerät für die zukünftige Nutzung als Verbindungsschlüssel gespeichert.

Bei der Erzeugung dieses Kombinationsschlüssels gehen die Geräteadressen und von beiden Geräten je eine Zufallszahl ein. Für die gesicherte Übertragung dieser Zufallszahlen wird ein Initialisierungsschlüssel verwendet, der sich aus einer weiteren (öffentlichen) Zufallszahl, einer Geräteadresse und einer PIN berechnet. Dazu muss in beide Geräte die gleiche PIN eingegeben werden. Die PIN kann 1 bis 16 Byte lang sein und ist entweder durch den Nutzer konfigurierbar oder fest voreingestellt. Verfügt eines der Geräte über eine feste PIN, so muss diese in das andere Gerät eingegeben werden. Zwei Geräte mit fest voreingestellter PIN können nicht gepaart werden.

Neben den Kombinationsschlüsseln erlaubt der Standard weitere Möglichkeiten für Verbindungsschlüssel:

- Geräteschlüssel (Unit Keys) können als Verbindungsschlüssel genutzt werden. Der Geräteschlüssel wird bei der erstmaligen Verwendung eines Bluetooth-Gerätes erzeugt und normalerweise nicht mehr geändert. Geräteschlüssel werden beispielsweise verwendet, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt oder ein Gerät einer großen Gruppe von Nutzern zugänglich sein soll.

- Master-Schlüssel (Master Keys) können für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, wenn ein Master mehrere Geräte unter Verwendung desselben Chiffrierschlüssels erreichen will. Master-Schlüssel werden nur bei Punkt-zu-Mehrpunkt-Verbindungen eingesetzt und über die aktuellen Verbindungsschlüssel gesichert vom Master an die Slaves übertragen.

Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird grundsätzlich einseitige Authentisierung verwendet, das heißt, ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier).

Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.

Die Authentisierung läuft wie folgt ab: Der Verifier sendet eine Zufallszahl an den Claimant. Dieser beweist, dass er das gemeinsame Geheimnis (den Verbindungsschlüssel) kennt, indem er unter Benutzung des Verbindungsschlüssels aus der Zufallszahl und seiner eigenen Geräteadresse eine 32 Bit lange Antwort berechnet und zum Verifier zurücksendet. (Dabei berechnet er gleichzeitig aus diesen Daten einen 96 Bit langen sog. Authenticated Cipher Offset, der geheim gehalten wird und bei Bedarf - als ein Teil - bei der Erzeugung eines Verschlüsselungsschlüssels verwendet wird.) Der Verifier überprüft die Antwort, indem er die gleiche Berechnung durchführt. Sind die Ergebnisse identisch, ist der Claimant authentisiert.

Verschlüsselung

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat. Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels. Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl an den Slave sendet. Der Chiffrierschlüssel berechnet sich aus dem Verbindungsschlüssel, einem Cipher Offset und der Zufallszahl.

Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei Punkt-zu-Punkt-Verschlüsselung wird der Authenticated Cipher Offset des Authentisierungsprotokolls als Cipher Offset verwendet. Bei Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Masters als Cipher Offset genutzt. Außerdem muss der Verbindungsschlüssel durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird.

Zum Verschlüsseln wird eine Stromchiffre (im Standard mit E0 bezeichnet) eingesetzt. Für jedes Datenpaket wird dabei ein neuer Initialisierungsvektor ("Spruchschlüssel") aus der Geräteadresse sowie dem Zeittakt des Masters berechnet. Verschlüsselt sind die Daten nur während des Transports per Funk. Vor der Aussendung bzw. nach Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor; es handelt sich also nicht um Ende-zu-Ende-Verschlüsselung (d. h. Verschlüsselung der Daten von der Eingabe in Endgerät A bis zur Ausgabe/Bearbeitung in Endgerät B).

Übersicht aller Schlüsselbezeichnungen:

- **Pin Code (Pin)**
  Wird manuell eingegeben und ist optional. Sie wird z. B. zur Generierung des Init-Keys verwendet.

- **Unit-Key (Geräteschlüssel)**
  Der Unit-Key wird bei der erstmaligen Verwendung eines Bluetooth-Gerätes erzeugt und im Normalfall nicht geändert. Er kann als Verbindungsschlüssel verwendet werden, wenn z. B. ein Gerät nicht genügend Speicherplatz für weitere Schlüssel hat.
  Der Unit-Key wird zur Erzeugung anderer Schlüssel verwendet.

- **Combinations-Key (Verbindungsschlüssel)**
  128 Bit langer Kombinationsschlüssel, der für zukünftige Verbindungen gespeichert wird. Er besteht aus der Geräte-Adresse und einer Zufallszahl je Gerät und wird bei der Initialisierung verwendet. Die Zufallszahl wird hier durch einen Pseudozufallsgenerator gebildet.

- **Master-Key (Master-Schlüssel)**
  Der Master-Key wird temporär für die Dauer einer Sitzung zwischen mehreren Geräten vereinbart. Er wird ausschließlich bei Multi-Slave-Verbindungen eingesetzt und über den aktuellen Verbindungsschlüssel gesichert an die Slaves versendet.

- **Init-Key (Initialisierungsschlüssel)**
  Er wird für die gesicherte Übertragung der Combinations-Keys verwendet. Er besteht aus einer Pin (hier muss die gleiche Pin in die Geräte eingegeben werden), dem Unit-Key sowie einer Zufallszahl.

- **Encryption-Key (Chiffrierschlüssel)**
  Der Encryption-Key berechnet sich aus dem Verbindungschlüssel, einem „Cipher-Offset“ und einer Zufallszahl. Die Zufallszahl wird für jede Session neu generiert. Der Chiffrierschlüssel dient zur Verschlüsselung der Daten während der Übertragung.

3.1.5 Sicherheitsbetriebsarten

Die Spezifikation beschreibt im Generic Access Profile 3 Sicherheitsmodi:

- **Non-Secure Mode** (Sicherheitsmodus 1): Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheitsmechanismen, reagiert aber auf Authentisierungsanfragen anderer Geräte. In dieser Betriebsart werden keine speziellen Sicherheitsmechanismen genutzt. Eine Authentifikation findet nicht statt. Das Abhören wird lediglich durch Frequency Hopping mit 16000 Frequenzwechseln pro Sekunde zwischen 79 Kanälen erschwert.

- **Service-Level Enforced Security** (Sicherheitsmodus 2): Auswahl und Nutzung von Sicherheitsmechanismen werden abhängig vom Bluetooth-Gerät ("trusted" oder "non-trusted") und vom Dienst auf Anwendungsebene (Application Layer) festgelegt. Das Gerät leitet erst dann Sicherheitsprozeduren ein, wenn es eine Aufforderung zum Verbindungsaufbau erhalten hat.

- **Link-Level Enforced Security** (Sicherheitsmodus 3): Auf der Verbindungsschicht (Link) bietet der Bluetooth-Standard zwei Sicherheitsdienste: eine kryptographische Authentifikation sowie eine Verschlüsselung der übertragenen Nutzdaten. Es ist generell eine Authentisierung beim Verbindungsaufbau erforderlich; die Verschlüsselung der zu übertragenden Daten ist optional.

Zusätzlich sind für die Erkennbarkeit von Bluetooth-Geräten beim Inquiry die Modi "non-discoverable" (Gerät antwortet nicht auf Inquiry) bzw. "limited discoverable" und "general discoverable" spezifiziert. Weiterhin gibt es die Betriebsmodi "non-connectable" (keine Reaktion auf Paging-Anforderungen) bzw. "connectable" sowie "non-pairable" (keine Paarung möglich) und "pairable".

3.2 Gefahren beim Einsatz

Zu all den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (vgl. [9]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

3.2.1 Schwächen im Sicherheitskonzept

Verschlüsselung ist nicht vorgeschrieben

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der übertragenen Daten optional und muss von den Anwendungen explizit beantragt werden.

Unsichere Voreinstellungen sind nicht ausgeschlossen

Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert: Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind häufig abgeschaltet und PINs auf "0000" eingestellt. Wenn Geräte keine Eingabemöglichkeit besitzen (z. B. Headsets), ist eine Änderung der voreingestellten Werte gar nicht oder nur schwer möglich.

Schwache PINs können erraten werden

Wird bei der Gerätepaarung eine schwache PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss der Angreifer nur die Paarung und die folgende Authentisierung abhören. Anhand der Aufzeichnungen der abgehörten Protokolle kann der Angreifer überprüfen, ob die PIN von ihm korrekt geraten wurde. Auf diese Weise ist es möglich, kurze oder triviale (z. B. "1234567890") PINs zu ermitteln.
Als sicherheitskritisch anzusehen ist, dass PINs als einzige geheime Parameter bei der Verbindungsschlüsselerzeugung eingehen. Erfahrungsgemäß lassen sich hier schwache - weit verbreitete - Nutzergewohnheiten nur schwer durchbrechen.

Geräteschlüssel sind unsicher

Werden Geräteschlüssel von einem Gerät als Verbindungsschlüssel verwendet, so wird für jede Verbindung mit diesem Gerät immer der gleiche Schlüssel benutzt. Gelingt es dem Angreifer, eine Verbindung mit diesem Gerät aufzubauen, ist er anschließend in der Lage, sich für dieses Gerät auszugeben oder jede Kommunikation mit diesem Gerät abzuhören.

Schwache Integritätssicherung

Zur Integritätssicherung wird ein Cyclic Redundancy Check (CRC, codierungstheoretisches Verfahren zur Erkennung von Übertragungsfehlern) verwendet. Dadurch werden zwar zufällige Störungen bei der Übertragung von Datenpaketen mit hoher Wahrscheinlichkeit erkannt, aber gegen eine absichtliche Manipulation von Datenpaketen bieten CRC-Verfahren keinen ausreichenden Schutz.

Qualität des Zufallsgenerators

Zur Zufallserzeugung sind im Bluetooth-Standard keine Mechanismen festgelegt worden. Erfahrungsgemäß ist damit zu rechnen, dass die Güte der Zufallsgeneratoren hersteller- und implementierungsabhängig stark variiert.

3.2.2 Man-in-the-Middle-Angriffe

Ein weiteres Sicherheitsproblem von Bluetooth besteht darin, dass in bestimmten Konfigurationen so genannte "Man-in-the-Middle"-Angriffe möglich sind [10].
Dabei schiebt sich ein Angreifer, der (unberechtigt) Zugriff auf ein Bluetooth-Gerät erhalten will, "mitten zwischen" zwei berechtigte Geräte. Anschließend kommunizieren die beiden Geräte über den Angreifer miteinander, der die Datenpakete abfängt und manipulieren kann. Folgende Szenarien sind denkbar:

- Der Angreifer baut aktiv eine Verbindung zu beiden Geräten auf.

  Der Angreifer verbindet sich mit beiden Geräten und gibt dabei vor, jeweils das andere Gerät zu sein. Sofern sich das Gerät des Angreifers gegenüber einem Gerät authentisieren muss, reicht es die Authentisierungsanfrage an das andere Gerät weiter und sendet die Antwort zurück. Anschließend kann der Angreifer mit dem Gerät beliebig interagieren. Als Voraussetzung für die erfolgreiche Durchführung dieses Angriffs müssen beide Geräte "connectable" sein (s. 3.1.5).

- Der Angreifer schaltet sich ein, während die Geräte eine Verbindung aufbauen.
  Während des Verbindungsaufbaus müssen sich die Geräte auf die Sprungsequenz synchronisieren. Der Angreifer kann diese Synchronisation verhindern, so dass beide Geräte zwar die gleiche Sequenz, aber verschiedene Offsets in der Sequenz verwenden.

3.2.3 Probleme bei der Verschlüsselung

Die von Bluetooth optional verwendete Verschlüsselung hat einige Schwächen:

- Sicherheit der Stromchiffre E0
  Obwohl E0 Schlüssellängen von 1-16 Bytes (8-128 Bit) akzeptiert, haben Fluhrer und Lucks gezeigt, dass die erreichbare Sicherheit je nach Stärke des Angreifers 73 bzw. 84 Bit nicht übersteigt [11].

- Der Initialisierungsvektor ist nicht vom vollständigen Zeittakt abhängig.
  Jedes übertragene Datenpaket wird unter Verwendung eines neuen Initialisierungsvektors verschlüsselt. Dieser errechnet sich unter anderem aus dem Zeittakt des Masters. Es wird allerdings das höchstwertige Bit des Zeittaktes "vergessen"; so sind selbst bei eingesetzter Verschlüsselung Man-in-the-Middle-Angriffe (s. 3.2.2) möglich.

- Verschlüsselte Daten können manipuliert werden.
  Selbst wenn eine starke Verschlüsselung eingesetzt wird, können übertragene Daten manipuliert werden. Aufgrund der Eigenschaften von Stromchiffren ist es möglich, die über einen "Man-in-the-Middle"-Angriff (s. 3.2.2) abgefangenen Daten gezielt zu verändern, wenn der verschlüsselte Klartext teilweise bekannt ist. So ist es beispielsweise möglich, IP-Header gezielt zu manipulieren.

3.2.4 Unkontrollierte Ausbreitung der Funkwellen

Der Funkverkehr von Bluetooth-Verbindungen kann mit Hilfe von Bluetooth-Protokollanalysatoren passiv mitempfangen und aufgezeichnet werden. Die Synchronisation auf die Frequency-Hopping-Sequenz gelingt bei Kenntnis der Geräteadressen auch dann, wenn sich die Geräte im "Non-discoverable"-Modus befinden. Alle Schichten des Bluetooth-Protokoll-Stacks können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten (Payload) ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen Bluetooth-Signals kann ein solcher "Lauschangriff" auch noch in einer gegenüber der Funktionalitätsreichweite größeren Entfernung durchgeführt werden. Eine Sendeleistungsregelung ist optional und wird nicht von jedem Bluetooth-Gerät unterstützt. In der Literatur zum Thema findet man gelegentlich die Behauptung, dass allein die Verwendung des Frequenzsprungverfahrens eine unberechtigte Teilnahme bzw. den Empfang und das Abhören von Bluetooth-Verbindungen wesentlich erschwere - für einen ausreichend informierten Angreifer stellt dies allein jedoch kein ernsthaftes Hindernis dar. Der Grund für die Verwendung eines Frequenzsprungverfahrens liegt darin, Übertragungsfehler aufgrund von Störungen durch den Betrieb anderer Geräte (z. B. drahtlose LANs), die dasselbe Frequenzband nutzen, klein zu halten und somit eine gute Verfügbarkeit sicherstellen zu können.

3.2.5 Bewegungsprofile

Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

3.2.6 Verfügbarkeitsprobleme – Denial of Service

Die Verfügbarkeit kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- Störungen durch andere Nutz-Anwendungen im gleichen ISM-Band
- Störung durch gezielt eingesetzte Störsender
- Angriffe auf die Energiereserven einzelner Geräte durch Abhalten vom Ruhe-Modus

3.2.7 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu berücksichtigen:

- Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.

- Authentisieren muss sich bei Bluetooth nur das Gerät, in der Regel aber nicht der Benutzer gegenüber dem Gerät. Bei Abhandenkommen mobiler, gepaarter Geräte sind diese also in der Regel ohne weiteres durch unbefugte Dritte im Herkunftsbereich nutzbar.

- Bluetooth-Geräteadressen sind mit geeignetem Equipment manipulierbar (Flash-Memory).

- Auch in Ad-hoc-Netzwerken existiert die Gefahr der Verbreitung von Computer-Viren und trojanischen Pferden.

- Das Abhören bzw. Aufzeichnen von Raumgesprächen unter Verwendung von handelsüblichen oder speziell manipulierten Bluetooth-Geräten (z. B. Headset mit 100 mW Sendeleistung) ist grundsätzlich nicht auszuschließen (s. hierzu auch [12]).

- Aufgrund von fehlerhaften Bluetooth-Implementierungen können Sicherheitslücken entstehen. Erste Missbrauchsfälle bei Windows-Bluetooth-Adaptern (Buffer-Overflow) sind bereits bekannt geworden.

3.3 Sicherheitsmaßnahmen

Bluetooth-Geräte, die mindestens einen sicherheitsrelevanten Dienst anbieten, sollten Verschlüsselung mit Kombinationsschlüsseln unterstützen; die Geräte dürfen keine Geräteschlüssel verwenden. Außerdem müssen sie in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen ergriffen werden können und welche Rest-Risiken bestehen.

3.3.1 Absicherung von Bluetooth-Geräten

Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und wenn möglich zu ändern:

- Die Bluetooth-Geräten beiliegende Installations-Software versucht häufig, möglichst viele Dienste zu aktivieren, damit alle Möglichkeiten der Kommunikation mit anderen Geräten genutzt werden können. Nicht benötigte Dienste sollte der Anwender stets deaktivieren.

- Bluetooth-Geräte sollten möglichst wenig "offen" konfiguriert werden, das heißt, es ist empfehlenswert, Connectability, Discoverability und Pairability so weit wie möglich einzuschränken.

- Falls die Sendeleistung variabel ist, sollte sie so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich eingestellt werden.

- Als Default-PIN sollte eine möglichst lange und zufällig gewählte PIN verwendet werden (s. 3.3.2).

- Wenn ein Gerät Authentisierung verwendet, muss es so konfiguriert werden, dass es nach erfolgreicher Authentisierung immer auch eine starke Verschlüsselung verwendet.

- Wenn ein Gerät Verschlüsselung der Kommunikation erzwingt, muss die Schlüssellänge mindestens 64 Bit betragen, und als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung akzeptiert werden. Die Schlüssellänge sollte so groß wie möglich gewählt werden.

Stationäre Geräte

Zur Absicherung von stationären Geräten, bei denen Bluetooth als Kabelersatz - zum Beispiel zur Verbindung mit immer den gleichen Peripheriegeräten - verwendet wird, sollten die Geräte in abhörgefährdeten Einsatzumgebungen mit Authentisierung und aktivierter Verschlüsselung betrieben werden. Die Länge der verwendeten PIN sollte über die minimal empfohlene PIN-Länge (s. 3.3.2) hinausgehen.

Mobile Geräte

Bluetooth-Geräte, die mobil verwendet werden und mit fremden Geräten (d. h. Geräten unterschiedlicher Besitzer) kommunizieren, müssen besonders gesichert werden:

- Die Paarung zweier fremder Geräte sollte immer in abhörsicherer Umgebung durchgeführt werden. Die bei der Paarung verwendete PIN muss ausreichend lang sein (s. 3.3.2).

- Jedes Gerät, das mehrere Dienste mit unterschiedlichen Sicherheitsniveaus anbietet, sollte in Sicherheitsmodus 2 betrieben werden. In diesem Fall ist darauf zu achten, dass die Sicherheitspolicies sorgfältig erstellt werden.

- Geräte, die nur einen Dienst oder mehrere Dienste mit gleichem Sicherheitsniveau anbieten, sollten im Sicherheitsmodus 3 betrieben werden.

- Die Geräte sollten ausgeschaltet werden, wenn sie nicht benutzt werden.

- Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Gerätes sollten alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden.

3.3.2 Hinweise zur Wahl von PINs

PINs sollten eine möglichst zufällige Folge aus den verwendbaren Zeichen sein, triviale PINs wie "0000" oder "1234" sind unbedingt zu vermeiden (vgl. [9]). Für eine ausreichende Sicherheit bei der Paarung zweier Bluetooth-Geräte ist eine ausreichend lange PIN notwendig. Eine sichere PIN sollte zumindest eine Länge von circa 64 Bit aufweisen. PINs mit bis zu 40 Bit Länge können beispielsweise auf einem handelsüblichen, modernen PC gebrochen werden. Da es bei Bluetooth-Geräten nur möglich ist, PINs in Form von Ziffern bzw. alphanumerischen Zeichen einzugeben, gibt Tabelle 1 Empfehlungen für die Anzahl der zu verwendenden Zeichen.

Verwendete Zeichen	Min. empfohlene PIN-Länge	Minimale PIN Länge
0-9 (10 Zeichen)	19 Stellen (= 63 Bit)	12 Stellen (= 40 Bit)
0-9, A-Z (36 Zeichen)	12 Stellen (= 62 Bit)	8 Stellen (= 41 Bit)
0-9, A-Z, a-z (62 Zeichen)	11 Stellen (= 65 Bit)	7 Stellen (= 42 Bit)
(druckbares) ASCII (95 Zeichen)	10 Stellen (= 66 Bit)	6 Stellen (= 39 Bit)

Tabelle 1: Wahl von PINs

Beispiel: Akzeptiert das Gerät nur Ziffern und Großbuchstaben als PIN, sollte in jedem Fall eine PIN von mehr als 8 Stellen verwendet werden; empfohlen werden jedoch PINs mit mindestens 12 Stellen.

Anmerkung: Unter Umständen gibt es Geräte, bei denen 19-stellige PINs nicht eingegeben werden können. Im Falle, dass nur Ziffern eingegeben werden können, sind dann aber zum Beispiel 16 Stellen für eine ausreichende Sicherheit nicht genug.

3.4 Weitere Schutzmaßnahmen

Über die in 3.3.1 genannten Maßnahmen hinaus sollten auf Bluetooth-Geräten - falls dies technisch möglich ist - weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz (s. 6.4)
- Personal Firewall (s. 6.1)
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

usw.

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [9].

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen (vgl. auch [12]).

3.5 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von Bluetooth-Geräten immer folgende Rest-Risiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (s. 3.2.5) kann nicht verhindert werden.
- Die Gefährdung der Verfügbarkeit (s. 3.2.6) ist ebenfalls nicht vermeidbar.
- Man-in-the-Middle-Angriffe (s. 3.2.2) sind auch bei optimal konfigurierten Geräten theoretisch möglich. Abhilfe ist nur durch die Verwendung zusätzlicher Sicherheitsmaßnahmen möglich, zum Beispiel durch die Verwendung von Sicherheitsdiensten in transportorientierten Schichten des ISO-Referenzmodells (z. B. IPSec oder SSL) oder direkt auf Anwendungsebene (Ende-zu-Ende-Sicherheit).

3.6 Ausblick und Literatur

Die Bluetooth-Spezifikation Version 1.2 wurde im November 2003 verabschiedet.

Zukünftige Versionen des Bluetooth-Standards werden die Verwendung des Geräteschlüssels als Verbindungsschlüssel nicht mehr erlauben. Zusätzlich wird das Konzept der Gruppenschlüssel eingeführt. Gruppenschlüssel sollen Roaming ermöglichen, so dass ein Gruppenschlüssel nicht verbindungsindividuell zwischen zwei Geräten ausgehandelt wird, sondern dienstindividuell.

Es ist ebenfalls davon auszugehen, dass die Erstellung eines Kombinationsschlüssels nicht mehr ausschließlich durch die Eingabe einer PIN gesichert wird. Anstelle dessen wird der Kombinationsschlüssel über das Diffie-Hellmann-Verfahren vereinbart. Bei diesem Protokoll wird der Schlüssel über ein asymmetrisches kryptographisches Verfahren berechnet. Die PIN dient nur noch zur Kontrolle, ob die Berechnung nicht manipuliert wurde.
Das Erstellen von Bewegungsprofilen soll durch den neuen Standard erschwert werden, indem die feste Geräteadresse durch temporäre Adressen ersetzt wird. Die feste Geräteadresse wird dann nur noch zum Verbindungsaufbau verwendet.

Ausführliche Informationen zur Bluetooth-Spezifikation in deutscher Sprache kann man unter anderem den Büchern [8] und [13] entnehmen. Eine genauere Beschreibung der Bluetooth-Sicherheitsarchitektur ist zum Beispiel in [14] enthalten. Aktuelle Informationen zu Bluetooth findet man unter [15] und [16].
Eine ausführliche Beschreibung verschiedener Schwächen im Sicherheitskonzept von Bluetooth findet sich in [17]. Ferner sei an dieser Stelle auf eine umfangreiche Publikation vom amerikanischen National Institute of Standards and Technology [18] hingewiesen, die unter anderem ebenfalls Informationen zum Thema dieser Broschüre enthält.

4 Die Infrarotschnittstelle

Die Infrared Data Association (IrDA) [19] hat eine Gruppe von Protokollen für die Infrarotübertragung für kurze Entfernungen definiert. Man unterscheidet zwischen der IrDA Data und der IrDA Control Spezifikation. Die Bezeichnung IrDA wird auch als Synonym für das IrDA Data Protokoll verwendet. Die erste IrDA (Data) Spezifikation wurde 1994, ein Jahr nach Gründung des Normierungsgremiums, veröffentlicht. Mit Hilfe der IrDA-Schnittstelle können Daten über kurze Entfernungen zwischen Geräten wie PDA (Personal Digital Assistants), Druckern, Digitalkameras, tragbaren Computern, Mobiltelefonen mit dem PC oder untereinander ausgetauscht werden. Die IrDA-Schnittstelle wird von modernen Betriebssystemen standardmäßig unterstützt.

Bei der Spezifikation IrDA Control handelt es sich um eine Reihe von Protokollen, die die Kommunikation von Peripheriegeräten wie Tastaturen, Mäusen, GamePads und Fernbedienungen mit intelligenten Hosts (z. B. PCs und Fernsehgeräte) ermöglichen.

4.1 Grundlagen

Die Infrarot-Schnittstelle arbeitet bidirektional im Halbduplex-Verfahren mit Licht der Wellenlänge von 850 – 900 nm und einem Abstrahlungswinkel von +/-30° bei IrDA Data und von bis zu +/-50° bei IrDA Control.

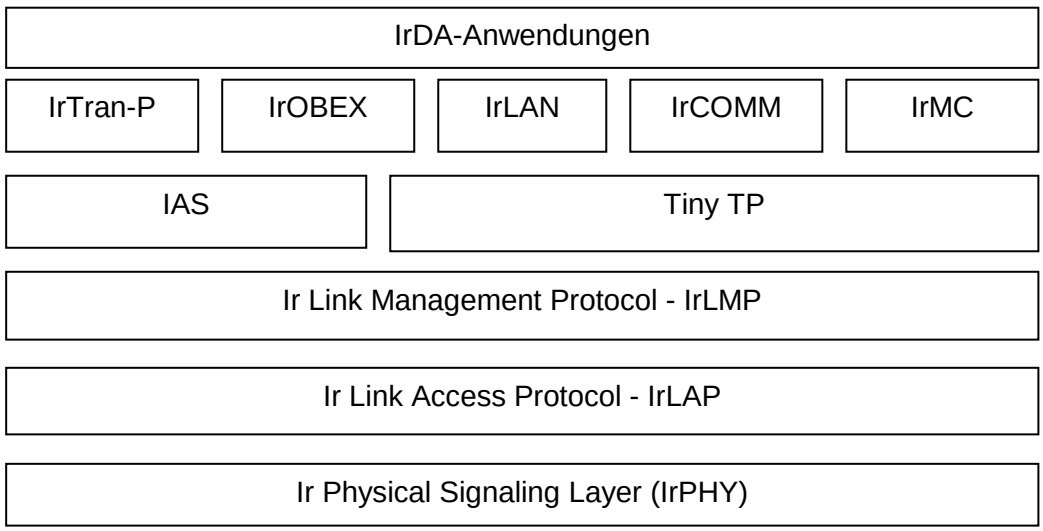
Mit der IrDA-Version 1.0 wurden lediglich Übertragungsgeschwindigkeiten von 115,2 Kbit/s erreicht. Die IrDA-Version 1.0 wurde auch als SIR (Serial Infrared) bezeichnet. Im Laufe der Zeit wurde die IrDA-Spezifikation erweitert. In der zweiten IrDA-Version wurden Geschwindigkeiten bis 4 Mbit/s (Fast Infrared, FIR) definiert. Da Multimediaanwendungen (u. a. Übertragung von Grafiken und Bildern) höhere Datenübertragungsraten benötigen, wurde in der aktuellen IrDA-Version 1.4 die Datenrate auf 16 Mbit/s (Very Fast Infrared, VFIR) erhöht. Bei IrDA Control beträgt die Datenübertragungsrate max. 75 Kb/s. Die Entfernung zwischen zwei Geräten kann bei IrDA Data max. 2 Meter und bei IrDA Control max. 5 Meter betragen.

Die Geräte müssen so aufeinander ausgerichtet werden, dass eine direkte Sichtverbindung besteht. Zu helle Lichtquellen oder Sonneneinstrahlung können die Verbindung stören.

4.2 Die Protokollarchitektur

4.2.1 IrDA Data Protokoll

In der IrDA Data Spezifikation wird ein relativ umfangreicher Protokollstack festgeschrieben. Die folgende Grafik veranschaulicht die wesentlichsten Protokolle der Spezifikation:



In der IrDA-Spezifikation wird zwischen festen (verbindlichen) und optionalen Protokollen unterschieden. Folgende Protokolle sind verbindlich zu implementieren:

- **Ir Physical Signaling Layer (IrPHY)**

  Der Ir Physical Signaling Layer beschreibt die bidirektionale Kommunikation zwischen Geräten auf der physikalischen Bitübertragungsschicht. Die Datenpakete werden mit einer CRC-Prüfsumme gegen Fehler gesichert.

- **Ir Link Access Protocol (IrLAP)**

  Das Ir Link Access Protocol ist für den Verbindungsaufbau zuständig. Nach erfolgreichem Verbindungsaufbau zwischen zwei kommunikationsfähigen Geräten werden die Leistungsparameter zwischen den Geräte ausgetauscht.

- **Ir Link Management Protocol (IrLMP)**
  Befindet sich mehr als ein Gerät in Reichweite, so wird mittels IrLMP die Verbindung „gemultiplext“.

Die folgenden Protokolle sind optional, das heißt, sie können, aber müssen nicht implementiert werden:

- **Tiny Transport Protocol (TinyTP)**
  Tiny TP steuert die Flusskontrolle. Mit diesem Protokoll erfolgt der eigentliche Datenaustausch.

- **Information Access Service (IAS)**
  IAS ist eine Sammlung von Objekten, welche die verfügbaren Leistungsmerkmale beschreibt.

- **IrTran-P**
  Ermöglicht den Austausch von Bildern, wie sie u. a. in Digitalkameras verwendet werden.

- **Ir Object Exchange Protocol (IrOBEX)**
  Ermöglicht „object exchange services“ so wie z. B. HTTP.

- **IrLAN**
  Beschreibt ein Protokoll, um IrDA-Geräte in LANs einbinden zu können.

- **IrCOMM**
  Emuliert für Anwendungen eine serielle und parallele Schnittstelle.

- **IrMC**
  Spezifiziert die Kommunikation zwischen Mobiltelefonen oder anderen Anwendungen für Sprache.

4.2.2 IrDA Control Protokoll

Das IrDA Control Protokoll besteht aus folgenden 3 verbindlichen Protokollen:

- Physical Layer (PHY),
- Media Access Control (MAC),
- Logical Link Control (LLC).

4.3 Risiken und Schutzmaßnahmen

Obwohl die Reichweite bei der Übertragung von Daten über die Infrarotschnittstelle auf wenige Meter begrenzt ist, kann ein Mithören des Datenverkehrs nicht in jedem Fall ausgeschlossen werden. Da im IrDA Data- und auch im IrDA Control-Standard keine Sicherheitsmechanismen zur Gewährleistung der Vertraulichkeit festgelegt werden, sind bei der Übertragung sensibler personenbezogener Daten in Räumen, in denen ein Mithören von Daten möglich ist, zusätzliche Sicherheitsmaßnahmen auf Anwendungsebene, z. B. der Einsatz kryptographischer Verfahren, erforderlich. Auch sollte geprüft werden, ob bei der Übertragung von personenbezogenen Daten nicht besser kabelgebundene Verbindungen genutzt werden können. Wird die Infrarotschnittstelle nicht benötigt, so sollte sie deaktiviert werden.

5 Drahtlose Peripheriegeräte und PDAs

Die beschriebenen Standards für die drahtlose Kommunikation sind nicht nur abstrakt zu betrachten, sondern auch in ihrer Implementation in konkreten Geräten. Dabei treten nicht selten zusätzliche Defizite zu Tage, und es wird erkennbar, ob optionale Elemente eines Standards nutzbar sind oder nicht. Während für Standard-PC eine große Bandbreite von Hard- und Software für die drahtlose Kommunikation verfügbar ist und somit auch die Auswahl zwischen Geräten mit mehr oder weniger implementierter Sicherheit besteht, gilt dies für andere Geräte nicht in diesem Maße.

5.1 Tastaturen und Mäuse

Der kabellose Betrieb von PC-Eingabegeräten, insbesondere Tastatur und Maus, ist mit verschiedenen Techniken möglich. Etabliert haben sich Funk und Infrarot, wobei die funkbasierten Lösungen meistens herstellerspezifische Entwicklungen darstellen. In geringerem Umfang sind auch auf Bluetooth basierende Produkte am Markt verfügbar.
Die Eigenschaften (insbesondere die Sicherheit) der Geräte mit Standardverfahren (Infrarot, Bluetooth) ergibt sich aus dem in den entsprechenden Kapiteln dieser Orientierungshilfe Gesagten. Für die anderen Systeme sind folgende Gemeinsamkeiten erkennbar:

- Benutzung von Funkfrequenzen, die für die allgemeine Nutzung freigegeben sind (27 MHz oder 2,4 GHz).
- Verfügbarkeit verschiedener Funkkanäle und Gerätekennungen, um eine gegenseitige Störung verschiedener Geräte zu vermeiden.
- Betriebs-Reichweiten von max. 5 bis 10 Metern.
- Keine oder keine nachprüfbare Sicherheit bei der Übertragung.

Bei dem Betrieb solcher Geräte ist zum einen eine gegenseitige Beeinflussung möglich, zum anderen besteht die Gefahr, dass die Signale mit einem gleichartigen Gerät oder mit besonderer Abhörtechnik von Unberechtigten empfangen werden. Dabei ist zu berücksichtigen, dass die Entfernungen, in der die Signale mit geeigneten Empfängern empfangen werden können, deutlich größer sind als die von den Herstellern angegebenen Reichweiten, die sich auf die zugehörigen Empfangsteile beziehen. Sofern keine Verschlüsselung der übertragenen Signale erfolgt, können auf diese Weise z. B. Tastatureingaben direkt zur Kenntnis genommen werden. Da solche Eingaben typischerweise auch sehr vertrauliche Informationen wie Kennwörter umfassen, ist das dadurch gegebene Risiko erheblich.

Diejenigen Geräte, bei denen eine Verschlüsselung implementiert ist, bieten in dieser Hinsicht mehr Schutz. Da die Verschlüsselungsverfahren seitens der Hersteller in der Regel nicht spezifiziert werden und – unter Berücksichtigung der geringen Datenverarbeitungskapazitäten der eingebauten Prozessoren – einer professionellen Kryptoanalyse vermutlich nicht standhalten, sind jedoch Zweifel an der Qualität dieses Schutzes angebracht.
Insgesamt ist daher von der Verwendung kabelloser Peripheriegeräte und insbesondere kabelloser Tastaturen aus datenschutzrechtlicher Sicht abzuraten, sofern nicht Übertragungsverfahren mit überprüfbarer Sicherheit verwendet werden.

5.2 PDA

Ein Personal Digital Assistant (Organizer, Handheld-Computer, Pocket-PC, Smart-Phone etc.) ist als Gerät, das explizit für die mobile Datenverarbeitung konzipiert ist, in besonderer Weise für die drahtlose Kommunikation prädestiniert. Dementsprechend verfügt die aktuelle Generation dieses Gerätetyps in der oberen Leistungsklasse über integrierte WLAN- und Bluetooth-Funktionalität. Sofern entsprechende Schnittstellen (PC-Card, Compact Flash) vorhanden sind, können diese Funktionen alternativ mittels Steckkarten hinzugefügt werden. Zudem bieten nahezu sämtliche Geräte die Möglichkeit, Daten per Infrarot zu übertragen.

Für die auf PDAs eingesetzten Standard-Verfahren für die drahtlose Kommunikation gelten die in den entsprechenden Abschnitten dargelegten Hinweise und Anforderungen. Dabei sind hier jedoch die besonderen Bedingungen zu beachten, die sich aus der im Vergleich zu einem PC oder einem Laptop deutlich geringeren Datenverarbeitungs- und -speicherungskapazität dieser Geräte ergeben:

- Sicherheitslösungen auf Anwendungs- oder Netzwerkebene wie IPSec, SSL, PGP usw. sind häufig nicht verfügbar oder nicht in einer akzeptablen Performanz nutzbar. Maßnahmen, die auf solchen Techniken beruhen, kommen daher i. Allg. nicht in Betracht, wenn PDAs in drahtlose Netze integriert werden sollen.

- Der Zugriffschutz ist bei PDAs in der Regel vergleichsweise schwach. Gespeicherte Daten wie z. B. Zugangsdaten zu WLAN können daher von Unberechtigten ausgelesen oder direkt genutzt werden.

- Sicherheits-Software wie Personal Firewall oder Virenscanner, die für PC zum Standard gehört, ist für PDAs kaum verfügbar. In (drahtlose) Netze integrierte PDA stellen daher ein potenzielles Sicherheitsrisiko dar, insbesondere dann, wenn sie in verschiedenen, insbesondere auch externen Netzen (z. B. in einem öffentlichen Hotspot) zum Einsatz kommen.

Insgesamt bedeutet dies, dass die Integration von PDAs in drahtlose Netze nur mit besonderen zusätzlichen Maßnahmen datenschutzgerecht möglich ist. Da nicht alle Geräte die Möglichkeit bieten, entsprechende Software zu installieren, stellt die Geräteauswahl – anders als bei Standard-PC bzw. -Laptop – einen wichtigen Faktor zur Vorbereitung eines datenschutzgerechten Betriebs dar. Auf keinen Fall sollte die Gesamtsicherheit eines Funknetzes auf das Niveau eines PDA als schwächstem Bestandteil abgesenkt werden.

6 Allgemeine Sicherheitsmaßnahmen

6.1 Einsatz von Firewalls

Eine Firewall ist die definierte und kontrollierte Schnittstelle zwischen einem zu schützenden und einem nicht vertrauenswürdigen Netz. Im zu schützenden Netz bestehen ein einheitlicher Schutzbedarf und ein einheitliches Sicherheitsniveau. Eine weitere Differenzierung nach Sicherheitsstufen geschieht, zumindest auf der Ebene des Netzes, nicht. Eine Firewall ist folglich ein Schutz vor Einbruchsversuchen in lokale Netze, die über einen Anschluss an öffentliche Netze verfügen (z. B. Internet, WLAN). Ähnlich eines Grenzkontrollpunkts erlaubt sie den Zugang nur an einer definierten Stelle. Damit lässt sich der Datenverkehr von und nach außen kontrollieren. Normalerweise sind zahlreiche Rechner des Unternehmens, die unter diversen Betriebssystemen laufen, direkt aus dem öffentlichen Netz erreichbar. Eine Firewall kanalisiert die Kommunikation, indem alle Daten von und nach außen über dieses System laufen müssen. Die Kanalisierung erhöht zudem die Chancen, einen Einbruchsversuch anhand ausführlicher Protokoll-Dateien zu erkennen, da der Eindringling erst die Firewall passieren muss.

Eine Firewall vom Typ „Paketfilter“ kontrolliert den eingehenden und ausgehenden Netzverkehr. Hierbei werden die Quell- und Zieladresse (IP-Adresse und TCP/UDP-Port) eines Pakets überprüft und entschieden, ob es passieren darf oder nicht. Der Vorteil besteht in der Transparenz für den Anwender. Diese Transparenz ist aber zugleich von Nachteil: Paketfilter können nicht zwischen Nutzern und deren Rechten unterscheiden. Auch die Inhalte der IP-Pakete werden nicht kontrolliert. Das bedeutet, dass Viren oder aktive Elemente in Webseiten (z. B. Javascript oder Active X) nicht von einfachen WWW-Seiten unterschieden werden. Auch können fremde Dienste über zugelassene Ports „geschmuggelt“ werden (Tunneling). Paketfilter sind im Allgemeinen auf Routern angesiedelt und werden heute von den meisten Herstellern mitgeliefert. Intelligente so genannte „stateful Paketfilter“ analysieren zusätzlich die Art der Pakete und erkennen auch die Zulässigkeit von dazugehörigen Verbindungen („Related“ Verbindungen), die einfache Paketfilter nicht erlauben würden (z. B. Datenverbindung bei ftp).

Neben dem „Paketfilter“ existieren noch weitere Typen von Firewalls. Circuit Level Gateways sind mit Paketfiltern vergleichbar, arbeiten jedoch auf einer anderen Ebene des Protokollstacks. Verbindungen durch solch ein Gateway erscheinen einem entfernten Rechner, als bestünden sie mit dem Firewall-Rechner. Somit lassen sich Informationen über geschützte Netzwerke verbergen.

Application Gateways, auch 'Proxy' (Stellvertreter) genannt, stellen ein anderes Firewall-Konzept dar. Hierbei wird auf dem Firewall-Host für jede zulässige Anwendung ein eigenes Gateway-Programm installiert. Der Client oder auch Nutzer muss sich dabei oftmals gegenüber dem Proxy-Programm authentifizieren. Dieser Proxy führt dann alle Aktionen im LAN stellvertretend für den Client aus. Damit lassen sich zum einen benutzerspezifische Zugangsprofile (welche Zeiten, welche Dienste, welche Rechner) erstellen, zum anderen kann man die Festlegung der zulässigen Verbindungen anwendungsbezogen vornehmen. Die daraus resultierenden separaten kleinen Regelsätze bleiben besser überschaubar als der komplexe Regelsatz eines Paketfilters. Application Gateways sind typische Vertreter der 'Verboten-was-nicht-erlaubt'-Strategie und als die sicherste, aber auch aufwendigste Lösung einzuschätzen.

Eine Firewall setzt eine definierte Sicherheitspolitik (Security Policy), die für das zu schützende Netz definiert wurde, voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen. Grundsätzlich existieren zwei Arten, Regeln einer Firewall zu definieren:

1. „Jegliche Kommunikation ist erlaubt, mit Ausnahme der Kommunikationswege, die verboten werden.“

Dieser Ansatz schließt die Nutzung bestimmter Dienste generell aus. Der Vorteil dieser Lösung liegt in seiner einfachen Handhabung und der Benutzerfreundlichkeit, da neue Dienste automatisch erlaubt sind. Der Administrator sperrt nur die nach seiner Meinung „gefährlichen“ Ports. Der Nachteil dieses Ansatzes liegt in der hohen administrativen Belastung, da das Verhalten von Anwendungen und Programmen ständig beobachtet und rechtzeitig Gegenmaßnahmen getroffen werden müssen.

2. „Jegliche Kommunikation ist verboten, mit Ausnahme der Kommunikationswege, die erlaubt werden.“

   Der Vorteil liegt in dem sehr viel höheren Maß an Sicherheit, da Zugriffe auf unbekannte Ports unterbunden werden, die aus Sicherheitslücken im Betriebssystem und Anwendungsprogrammen stammen. Der Nachteil dieser Strategie ist, dass sie von Nutzern als hinderlich angesehen werden, da diese neuen Dienste immer wieder neu eingerichtet werden müssen. Weiterhin muss vor Einrichtung einer Firewall eine Kommunikationsanalyse durchgeführt werden, um die Funktionalität aller benötigten Dienste sicherzustellen.

Der zweite Sicherheitsansatz ist in den meisten Fällen zu bevorzugen, da hier eine effektiv höhere Sicherheit erreicht wird.

Neben dem Aufbau einer Firewall ist auch der Standort im Netz von entscheidender Bedeutung. Gemeint ist nicht der physikalische Standort, sondern die logische Platzierung im Netz.

Eine Firewall kann aus einer einzelnen Maschine oder aus einer mehrstufigen Anordnung bestehen. Eine mehrstufige Anordnung ist vor allem dann sinnvoll, wenn man bestimmte Dienste der Öffentlichkeit zur Verfügung stellen will, etwa einen WWW- oder ftp-Server. Die entsprechenden Server können dann in einem Zwischennetz, einer so genannten DMZ (Demilitarisierten Zone) isoliert werden.

Je einfacher eine Firewallarchitektur ist, desto weniger ist sie anfällig für Fehler. Es gilt der Grundsatz, wenn mehrere Komponenten betreut und konfiguriert werden müssen, steigt auch die Anzahl der potentiellen Fehlerquellen. Eine Firewall mit einem hohen Sicherheitsniveau ist bedingt durch den höheren Aufwand an Ressourcen teurer, als eine Firewall mit einem niedrigen Sicherheitsniveau. Bei der Auswahl sollte darauf geachtet werden, dass die zu treffenden Schutzmaßnahmen in Relation zum schützenden Gegenwert liegen.

Die Sicherheit eines Netzes wird durch die Serienschaltung diverser Sicherheitsstufen, mit jeweils anderem Firewallsystem, immens erhöht. Bei einer solchen Architektur sind der Aufwand der Administration und die Anforderungen an den Administrator sehr hoch. Es wird zwischen vier verschiedenen Firewallarchitekturen (Dual-Homed-Host, Screened-Host, Screening-Router und Screened-Subnet) unterschieden.

Grundsätzlich gilt jedoch, dass keine Firewall einen absoluten Schutz gegen ein Eindringen in ein System gewährleisten kann. Sie kann lediglich einen Einbruch so schwer wie möglich und damit auch so unwahrscheinlich wie möglich machen. Dies bedeutet, dass eine Firewall zwar großen Schutz, jedoch keine absolute Sicherheit bietet.
Sie kann Angriffe oder deren Versuche auf niedriger Protokollebene feststellen, meist abblocken, teilweise auch protokollieren und zurückverfolgen, gegen Angriffe auf höherer Ebene ist sie jedoch nutzlos. Eine Firewall ist nicht in der Lage, Viren oder schadhafte aktive Komponenten (z. B. bösartige Active-X WWW-Seiten) zu filtern (s. 6.4).

Schutz kann die Firewall auch nur dann bieten, wenn die gesamte Kommunikation mit externen Systemen über diese Firewall abgewickelt wird. Ein einziger Kommunikationskanal (z. B.

Modem) reicht aus, um das gesamte Netz zu gefährden, da so die Firewall umgangen werden kann.

Weiterführende Informationen können z. B. der Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, die vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegeben wurde, entnommen werden [23].

6.2 VPN-Tunnel

Der Einsatz eines VPN kann insbesondere die Vertraulichkeit der übertragenen Daten gewährleisten, beispielsweise in WLANs, in denen nur die unsichere WEP-Verschlüsselung zur Verfügung steht.

VPN steht für Virtual Private Network und setzt auf der Internet-Technologie auf, wobei eine sichere Verbindung zwischen dem Client und dem vertrauenswürdigen Netz hergestellt wird.

Grundsätzlich wird zwischen den folgenden drei Anwendungsbereichen unterschieden:

- Site-to-Site-VPN: Hier werden interne Netzwerke über das Internet verbunden, wobei eine Datenverschlüsselung ausschließlich zwischen den Gateways, die die Schnittstellen zum Internet bilden, stattfindet. Nach außen treten hier die Gateways auf.

- Site-to-Client-VPN: Hier wird der Zugriff der mobilen Endgeräte an das interne Netz geregelt. Während zwischen dem Gateway und den Clients eine Datenverschlüsselung stattfindet, werden die Daten vom zentralen Gateway unverschlüsselt in das interne Netz weitergeleitet. Dies würde dem WLAN-Einsatz entsprechen.

- Client-to-Client-VPN: Hierbei werden zwei Clienten (z. B. zwei Rechner) direkt miteinander verbunden, wobei die Kommunikation verschlüsselt stattfindet.

Für die Kommunikation wird zwischen den beiden Endpunkten ein so genannter Tunnel aufgebaut. Hierfür wird die Internet-Technologie genutzt, wobei zwei öffentliche IP-Adressen benötigt werden. Die zu übertragenden Daten werden vom Sender verschlüsselt und in ein neues Datenpaket verpackt und anschließend beim Empfänger wieder ausgepackt. Während der Übertragung können im Internet lediglich die Umschläge, jedoch nicht deren Inhalt eingesehen werden.

Man unterscheidet zwischen den folgenden zwei Standards zum Aufbau eines kryptographischen Tunnels:

- SSL VPN steht für Secure Socket Layer Virtual Private Network und ist auf der Applikationsschicht implementiert. Sie eignet sich somit für Anwender, die auf einzelne web-fähige Applikationen zugreifen. Der Vorteil dieses Standards ist, dass die Anwender mit ihrem gewohnten Browser auf die Anwendungen zugreifen können. Z. B. wird SSL für das Online-Banking benutzt.

- IPSec over LAN steht für Internet Protocol Security over Local Area Network. Es ist auf der Netzwerkschicht (Layer 3) implementiert und somit für jegliche Applikation nutzbar. Diese Lösung galt lange Zeit als einzige logische Wahl für sichere Netzwerkverbindungen. Ein Nachteil ist, dass diese Lösung kostenintensiv ist, da eine entsprechende Softwareinstallation und -konfiguration für jeden Clienten vorgenommen werden muss.

Wichtig für die Verschlüsselung ist natürlich, dass ausschließlich als sicher anerkannte Algorithmen eingesetzt werden. Hierbei wird grundsätzlich zwischen den folgenden drei Formen der Verschlüsselung unterschieden:

- Symmetrische Verschlüsselung, d. h., es wird ein- und derselbe Schlüssel zum Ver- und Entschlüsseln eines Textes benutzt. Als problematisch muss gesehen werden, dass sich im vorhinein darauf geeinigt werden muss, welcher Schlüssel - der natürlich vorher ausgetauscht wurde - benutzt wird (z. B. 3DES, IDEA und AES).

- Asymmetrische Verschlüsselung, d. h., es gibt zwei verschiedene Schlüssel, einen öffentlichen und einen privaten. Während der öffentliche Schlüssel allgemein bekannt ist, wird der private Schlüssel zum Entschlüsseln bzw. Unterschreiben benutzt. Der Anwender A benutzt den öffentlichen Schlüssel von B. B bekommt die so verschlüsselte Nachricht von A und kann diese mit seinem privaten Schlüssel entschlüsseln. A könnte diese Nachricht noch mit seinem privaten Schlüssel unterzeichnen, so könnte B mit dem öffentlichen Schlüssel von A feststellen, dass diese Nachricht wirklich von A kommt (z. B. RSA).

- Anstelle von reinen asymmetrischen Verfahren werden in der Regel Hybridverfahren verwendet, die die Vorteile der symmetrischen und der asymmetrischen Verschlüsselung nutzen (z. B. PGP mit Public-Key-Verfahren).

Zu Schlüsselübermittlung, Schlüsselmanagement, Schlüssellänge wird auf die Orientierungshilfe zum Einsatz kryptographischer Verfahren der Arbeitsgruppe Kryptographie des Arbeitskreises für technische und organisatorische Fragen des Datenschutzes der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen [28].

6.3 Radius-Server (Remote Authentification Dail-in User Service-Server)

Neben der schon angesprochenen Verschlüsselung des Datenstroms ist natürlich auch die Authentifizierung von besonderer Bedeutung. Es ist schließlich zu gewährleisten, dass ausschließlich für berechtigte Nutzer – evtl. mit bestimmten Endgeräten – ein Zugriff auf das interne Netz möglich ist. Hierbei findet eine Identifikation – z. B. anhand einer Kennung – und eine anschließende Authentifikation – z. B. das geheime Passwort – statt. Die Übertragung dieser Daten (z. B. per PAP – Password Authentification Protocol) sollte verschlüsselt erfolgen.

Hierbei wird meist das Protokoll EAP (Extensible Authentification Protocol) genutzt. Die Authentisierung erfolgt portbasiert und beruht auf dem Standard IEEE 802.1X. Dies bedeutet, dass der Zugang zum WLAN erst dann erlaubt wird, wenn sich der Funknetzwerkclient eindeutig am Radius-Server identifiziert hat.

Der Radius-Server übernimmt hierbei einen Authentifizierungsdienst und bietet dabei ein sehr ausführliches Management bzw. Regelwerk an. Bestandteile sind die Authentifikation, Autorisierung und das Accounting. So können z. B. auch die MAC-Adressen verwaltet werden. Werden mehrere Access Points eingesetzt, so können diese auf das zentral hinterlegte Regelwerk zugreifen, was die Administrationsarbeiten vereinfacht.

Weiterhin kann durch den Einsatz des Radius-Server die Sicherheit bei der WEP-Verschlüsselung verbessert werden. Dies geschieht dadurch, dass durch den Radius-Server oder die LEAP (Lightwight- Extensible Authentication Protocol) Technologie die WEP Verschlüsselung bei jeder Anmeldung ausgehandelt wird. Hierdurch wird die Entschlüsselung eines WEP-Schlüssels durch Beobachtung des Datenverkehrs erschwert.

Folgendermaßen kann eine Authentifizierung mittels Radius-Server (hier: Cisco-Produkt) erfolgen:

- Der Client meldet sich über den Uncontrolled Port beim Access Point an.

- Der AP blockiert alle Requests des Clients über den Controlled Port (z. B. IP Requests), bis dieser sich am Netzwerk angemeldet hat.

- Der User am Client meldet sich über seine normale Netzwerk-Anmeldung (Network Logon) mit Username und Passwort beim Radius-Server an, wobei der Access Point diese Anfrage weiterleitet.

- Der Radius-Server authentifiziert den User. Hierzu wird ein MD5-Hash-Paket (Message Digest) mit einem zu verschlüsselnden Text (Challenge Text) über den Access Point an den Client übertragen.

- Der Client sendet seine Antwort (Response) über den Access Point an den Radius-Server.

- Auf diese Weise kann auch der Client den Radius-Server authentifizieren. Er sendet einen zu verschlüsselnden Text über den Access Point an den Radius-Server.

- Der Radius-Server sendet seine Antwort (Response) über den Access Point an den Client.

- Radius-Server und Client berechnen den Session Key, der für die WEP-Verschlüsselung eingesetzt wird. Dieser wird berechnet unter Einbeziehung des User-Passworts sowie der Challenge Requests und Responses von Client und Server.

- Der Radius-Server sendet den Session Key an den AP.

- Der AP verschlüsselt seinen Broadcast-Key mit dem Session Key und sendet ihn an den Client.

- Radius-Server und Client haben sich nun wechselseitig authentifiziert und verfügen nun ebenso wie der Access Point über einen user- und sitzungsspezifischen Schlüssel. Die verschlüsselte Datenübertragung kann nun also beginnen.

6.4 Schutz der Funknetzwerkclienten vor Computerviren

Natürlich darf nicht vergessen werden, dass nicht nur das LAN geschützt werden muss, sondern dass auch der Funknetzwerkclient mit einem entsprechenden Schutz ausgestattet werden muss, sonst ist die Datenübertragung per VPN verschlüsselt, der Client aber ansonsten gegenüber dem Internet ungeschützt und somit auch für Angriffe offen. Grundsätzlich sind die Sicherheitsfunktionen des Betriebssystems zu aktivieren. Darüber hinaus muss ein dem Schutzzweck der Daten angemessener Schutz evtl. noch zusätzlich installiert bzw. implementiert werden.

Eine Bedrohung stellen Angriffe in Form von Computer-Viren dar. Hiergegen muss ein entsprechender Schutz sowohl auf der Clienten-Seite als auch auf der Seite des Netzwerkes eingerichtet werden.

Die Viren stellen jedoch nur eine bestimmte Form der Angriffe auf die Computer dar. Deshalb soll von Computeranomalien gesprochen und Unterscheidungsmerkmale sollen erläutert werden. Man spricht von Computeranomalien immer dann, wenn der PC sich abweichend von seiner Spezifikation verhält. Hierfür gibt es die Möglichkeiten, dass Programme unvollständig oder fehlerhaft ausgeführt werden oder Programme Zusatz- oder Fehlfunktionen enthalten, deren Ausführung der Benutzer nicht bemerkt.

Man spricht auch von Malicious Programs bzw. Codes und meint Programme, die den Anwender schädigen, behindern, verunsichern oder arglistig täuschen sollen. Um die Band-

breite des Themas zu verdeutlichen, seien hier die am häufigsten vertretenen Arten - ohne Rücksicht auf Wertigkeit oder Vollständigkeit - aufgezählt:

- „Trojanische Pferde“ sind vollständige Programme, die neben den Funktionen für die eigentliche Aufgabe weitere, nicht dokumentierte Funktionen ausführen, die unerwünschte oder gar schädliche Wirkungen haben (z. B. Auslesen von Passwörtern).

- „Würmer“ treten bevorzugt in Computer-Netzen auf und sind ebenfalls eigenständige Programme. Sie veranlassen ihre „Wirts-Computer“, sie in Datennetzen weiter zu verteilen, sodass sie in weiteren Computersystemen ihre unheilvolle Funktion ausführen können.

- „Computer-Viren“ sind dagegen keine selbstständigen Programme. Es handelt sich um Programmteile, die sich selbst reproduzieren, indem sie sich an andere Programme – die so genannten Wirtsprogramme - anhängen oder sich in sie hinein kopieren. Charakteristisch für einen Virus ist, dass er mindestens aus den zwei Komponenten besteht. Eine Komponente ist für die Infektion (Vermehrung) verantwortlich und die andere verursacht den Schaden, wenn eine bestimmte Bedingung erfüllt worden ist (z. B. Erreichen eines bestimmten Datums, Aufruf einer bestimmten Datei). Der Virus kann dann zu Manipulationen am Betriebssystem (Systembereich), an Programmen oder deren Umgebung führen. Damit können bedeutende Schäden verursacht werden, zum Beispiel durch Verlust oder Verfälschung von Daten. Computerviren werden danach unterschieden, welche Bereiche sie infizieren: Datei-Viren, Bootsektor-Viren oder Makro-Viren, um die am häufigsten auftretenden Virenarten zu nennen.

Ganz etwas anderes, aber im Zusammenhang mit Computeranomalien immer wieder gesehen und mit kaum geringerer Schadenswirkungen sind sog. „Hoaxes“. Dabei handelt es sich um Falschmeldungen, die vor angeblichen Virengefahren warnen und oft im guten Glauben kettenbriefartig weitergereicht werden. Sie schaden, weil die „gewarnten“ Benutzer - natürlich überflüssigerweise - Gegenmaßnahmen treffen, die Kosten durch Zusatzarbeit, Ausfall von Rechnerverfügbarkeit und Zeitverzögerungen verursachen.

Es gibt viele Möglichkeiten, wie Computeranomalien, wie etwa ein Virus, auf die Festplatte bzw. in den Speicher übertragen werden können. Früher geschah es meistens durch das Starten eines infizierten Programms von einer Diskette. Dadurch nistete sich der Virus im Speicher ein und konnte von dort aus, solange der Rechner eingeschaltet war, sein Unwesen treiben. Heute hat sich dies verändert. Eine Infektion erfolgt meist durch das Kopieren von Programmen von einer CD-ROM auf die Festplatte oder durch das Herunterladen von Programmen aus dem Internet. Der Virus wird jedoch meistens nicht sofort aktiv, sondern erst dann, wenn das betroffene Programm zum wiederholten Male (je nach Bedingung für den Schadenseintritt) gestartet wurde. Damit soll die Entdeckung und Zurückverfolgung verhindert sowie die Verbreitung bzw. Infektion gefördert werden.

Am weitesten verbreitet sind zurzeit die Würmer. Diese werden meistens als Anhang (Attachment) einer Email versandt. Wird dieser Anhang aufgerufen, können die böswilligen Attacken ihren Lauf nehmen, es sei denn, der Virus wurde erkannt und beseitigt.

Die Palette der möglichen Schäden ist sehr groß. Welcher Schaden tatsächlich angerichtet werden kann, hängt einzig und allein von der Phantasie und den Fähigkeiten des Programmierers, der die Anomalie erzeugt hat, ab.

7 Rechtliche Aspekte des Abhörens von drahtlosen Verbindungen[6]

Bereits mit frei verkäuflichen technischen Mitteln ist es möglich, Daten bei der Kommunikation über drahtlose Netze auszuspähen. Es liegt nahe, dass derartige Angriffe (sog. „drive-by-hacking“ oder “war-driving”) rechtlich nicht gestattet sein können. Insbesondere in § 89 TKG sowie in § 202a StGB finden sich entsprechende Regelungen.

7.1 Abhörverbot nach § 89 TKG

Die Vorschrift verbietet das Abhören von Nachrichten mit einer Funkanlage, wenn diese für die Funkanlage nicht bestimmt sind. Hierunter fällt zweifelsohne das Hacking von drahtlosen Funkverbindungen.

„Nachricht“ bezeichnet nicht nur die an einen menschlichen Empfänger gerichtete Kommunikation. Auch auf den Informationsinhalt kommt es nicht an. Als Nachricht im Sinne dieser Vorschrift ist vielmehr jede Übermittlung von Signalen auch zwischen Computern ohne direkte menschliche Mitwirkung anzusehen.

Funkanlage ist nach der Definition in § 2 Nr. 3 des Gesetzes über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) „ein Erzeugnis oder ein wesentliches Bauteil davon, das in dem für terrestrische/satellitengestützte Funkkommunikation zugewiesenen Spektrum durch Ausstrahlung und/oder Empfang von Funkwellen kommunizieren kann“. Diese Voraussetzungen sind beim Hacking von drahtlosen Verbindungen gegeben.

Verboten ist nach § 89 TKG nur das bewusste (vorsätzliche) Abhören von Funkverbindungen. Das unbeabsichtigte Abhören ungesicherter drahtloser Verbindungen ist hingegen nicht von § 89 Satz 1 TKG umfasst.

Nicht verhindert werden soll durch die Vorschrift zudem das Aufdecken von Sicherheitsmängeln etwa durch die zuständigen Datenschutzaufsichtsbehörden. Diese sind befugt, auch verdeckt unsichere WLAN-Netze im Rahmen datenschutzrechtlicher Prüfungen aufzuspüren. Die Aufzeichnung von Inhalten sollte im Rahmen derartiger Prüfungen allerdings unterbleiben; sie ist zur Feststellung von Sicherheitsmängeln in der Regel auch nicht erforderlich.

Sowohl der Inhalt der Nachrichten als auch die bloße Tatsache ihres Empfangs dürfen – auch bei unbeabsichtigtem Empfang (!) – gemäß § 89 Satz 2 TKG anderen nicht mitgeteilt werden. Dies gilt wiederum nicht für die Unterrichtung zuständiger Datenschutzaufsichtsbehörden. Diesen kann das Fernmeldegeheimnis nicht entgegengehalten werden. Sie sind nach § 115 Abs. 5 TKG befugt, Nachrichteninhalte zur Kenntnis zu nehmen.

Sowohl das vorsätzliche Abhören nach § 89 Satz 1 TKG als auch die vorsätzliche unbefugte Weitergabe nach § 89 Satz 2 TKG sind nach § 148 Abs. 1 Nr. 1 TKG mit Strafe bedroht. Strafbar ist nur die vollendete Tat, nicht aber der Versuch.

7.2 Ausspähen von Daten nach § 202a StGB

Nach dieser Vorschrift ist es strafbar, sich oder einem anderen unbefugt Daten zu verschaffen, die gegen unberechtigten Zugang besonders gesichert und nicht für den Täter bestimmt sind.

Die Vorschrift schützt allein die Verfügungsbefugnis über die Daten, d. h. das Bestimmungsrecht darüber, wem die Daten zugänglich sein sollen. Auf den Inhalt oder die Bedeutung der Daten kommt es nicht an.

[6] Dieser Abschnitt wurde vom Arbeitskreis „Medien“ der Datenschutzbeauftragten des Bundes und der Länder verfasst.

Der Täter verschafft sich die Daten beim bewussten Hacking drahtloser Kommunikation jedenfalls dann, wenn er Daten auf seinem Computer gespeichert hat, die nicht für ihn bestimmt sind. Dieses Merkmal dürfte bei Hacking von drahtlosen Verbindungen in der Regel gegeben sein. Der Versuch ist hingegen nicht strafbar.

Entscheidend für eine Strafbarkeit ist jedoch, ob die Daten bei der Übertragung gegen unberechtigten Zugang gesichert sind. Eine solche Zugangssicherung besteht bei der Übertragung in drahtlosen Netzen insbesondere dann, wenn die Daten bei der Übertragung wirksam verschlüsselt werden. Die vom Gesetz gemeinte Zugangssicherung soll in erster Linie den Zugang zu den Originaldaten, d. h. den Inhalten, verhindern. Das bloße Abgreifen verschlüsselter Daten wäre deshalb wegen der fehlenden Möglichkeit, auf die Inhalte zugreifen zu können, nicht nach § 202a StGB strafbar, eine Entschlüsselung dieser Daten würde die Strafbarkeit jedoch begründen.

Nicht gegen unberechtigten Zugang gesichert ist die Datenübertragung insbesondere dann, wenn die Sperren ohne größeren Aufwand überwunden werden können. Werden keine besonderen Sicherungssysteme, d. h. vor allem Verschlüsselungsverfahren, verwendet oder sind diese zum Zeitpunkt ihrer Einrichtung bekanntermaßen und objektiv völlig ungeeignet, ist keine besondere Sicherung gegen unberechtigten Zugang gegeben. Eine Strafbarkeit nach § 202a StGB wäre in diesen Fällen zumindest fraglich.

Eine Strafverfolgung ist gemäß § 205 StGB nur auf Antrag des Verletzten möglich.

Unabhängig von der Frage der Strafbarkeit werden die Anbieter selbstverständlich nicht ihrer Pflichten enthoben, die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen und so erfolgreiche unbefugte Zugriffe auf die übertragenen Daten zu verhindern.

8 Literatur und Links

[1] http://www.i-m.de/home/datennetze/dn_wlan2.htm
[2] http://standards.ieee.org/wireless
[3] A. Kral und H. Kreft: Wireless LANs, Networker’s Guide. München: Markt+Technik Verlag 2003
[4] http://www.wi-fi.org/OpenSection/index.asp
[5] http://www.ieee802.org/15/pub/TG1.html
[6] http://www.bluetooth.org
[7] http://de.wikipedia.org/wiki/IEEE_802.11n
[8] J. F. Wollert: Das Bluetooth-Handbuch. Poing: Franzis Verlag 2002
[9] Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb
[10] D. Kügler, "Man in the Middle" Attacks on Bluetooth, Financial Cryptography '03, Lecture Notes in Computer Science, Springer-Verlag (noch nicht erschienen)
[11] S. R. Fluhrer und S. Lucks: Analysis of the E_0 Encryption System, Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Seiten 38-48, Springer-Verlag, 2001, http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz
[12] GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen, BSI 2002, http://www.bsi.bund.de/literat/doc/mobiltel/mobiltel.pdf
[13] N. J. Muller: Bluetooth. Bonn: MITP-Verlag 2001
[14] D. Fox: Bluetooth Security, Secorvo White Paper 2002, http://www.secorvo.de/whitepapers/secorvo_wp05.pdf
[15] http://www.bluetooth.com
[16] http://www.palowireless.com
[17] M. Jakobsson und S. Wetzel: Security Weaknesses in Bluetooth. Progress in Cryptography - CT-RSA 2001, Lecture Notes in Computer Science 2020, Seiten 176-191, Springer-Verlag, 2001, http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf
[18] T. Karygiannis und L. Owens: Wireless Network Security, National Institute of Standards and Technology (NIST) Nov. 2002, http://www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
[19] Infrared Data Organization http://www.irda.org
[20] Linux Infrared HOWTO von Werner Heuser http://www.tldp.org/HOWTO/Infrared-HOWTO/index.html
[21] BSI 2003, Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte, Abschnitt "Drahtlose Tastaturen und Mäuse"
ISECOM 2003, OSSTMM Wireless, Kapitel 4 und 5 (http://isecom.securenetltd.com/osstmm.en.2.9.wireless.pdf)
[22] http://www.jurpc.de/rechtspr/20030126.htm, Abs. 36
[23] http://www.lda.brandenburg.de/media/2473/onet.pdf
[24] http://www.lda.brandenburg.de/sixcms/detail.php?id=86550&template=allgemein_lda
[25] http://www.bfd.bund.de/information/Leitfaden.pdf
[26] International Working Group on Data Protection in Telecommunications, Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke, Allgemeine Empfehlungen, 35. Sitzung am 14./15. April 2004 in Buenos Aires
[27] http://www.heise.de/newsticker/meldung/print/49484
[28] http://www.datenschutz-berlin.de/to/kryptoverfahren.pdf

9 Abkürzungsverzeichnis

ACL	Asynchronous connection-less
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining
CCMP	AES-CTR/CBC-MAC Protocol
CHAP	Challenge Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CVSD	Continous Variable Slope Delta (-Modulation)
DFS	Dynamic Frequency Selection
DSSS	Direct Sequence Spread Spectrum
E0	Stromchiffre zur Verschlüsselung
EAP	Extensible Authentication Protocol
EAPoL	EAP-over-LAN-Authentifizierung
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
IAS	Information Access Service
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IrCOMM	Infrared Communications Protocol
IrDA	Infrared Data Association, auch Synonym für das IrDA-Protokoll
IrLAN	Infrared Local Area Network Access Extensions
IrLAP	Infrared Link Access Protocol
IrLMP	Infrared Link Management Protocol
IrTinyTP	Infrared Tiny Transport Protocol
ISM	Industrial, Scientific, Medical (2,4 GHz-Band)
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LEAP	Lightwight Extensible Authentication Protocol
MAC	Message Authentication Code
MIMO	Multiple Input Multiple Output
OBEX	Object Exchange Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PAP	Password Authentification Protocol
PC	Personalcomputer
PCM	Puls Code Modulation
PDA	Personal Digital Assistants
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
QoS	Quality-of-Service
RADIUS	Remote Authentication Dial-in User Service
SCO	Synchronous connection-oriented
SIG	(Bluetooth) Special Interest Group
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TACACS	Terminal Access Controler Access Control-System
TDD	Time Division Duplex
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TPC	Transmission Power Control
TTLS	Tunneled Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network

10 Stichwortverzeichnis