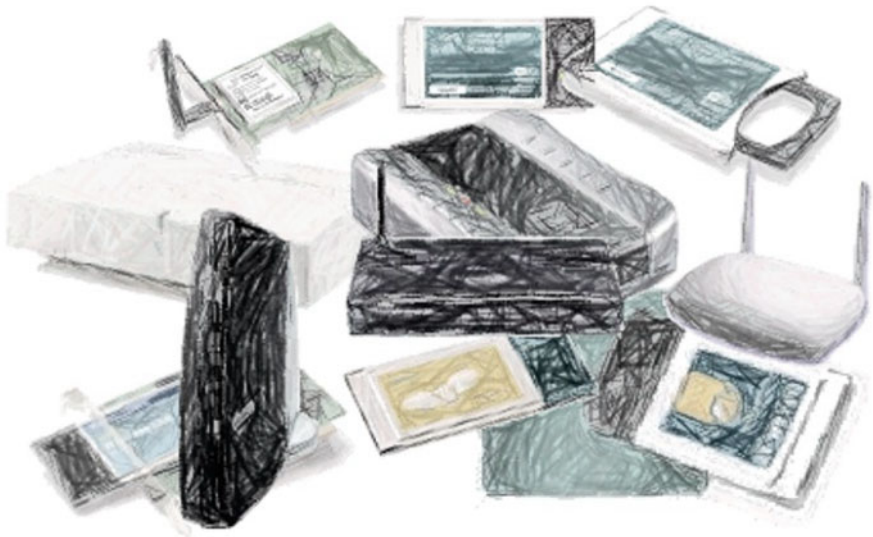
Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheit im Funk-LAN

(WLAN, IEEE 802.11)



In dieser Informationsschrift werden mögliche Gefährdungen bei der Nutzung von Funk-LANs beschrieben und geeignete Schutzmaßnahmen aufgezeigt. Sie richtet sich an Administratoren und an Endbenutzer von Wireless LAN Systemen nach IEEE 802.11. Die vorliegende Version 1.1 berücksichtigt aktuelle Entwicklungen und ersetzt die Informationsschrift Version 1.0 aus 07/2002.

Bundesamt für Sicherheit in der Informationstechnik

Projektgruppe "Local Wireless Communication"

Postfach 20 03 63

53133 Bonn

Tel.: +49 (0) 1888 9582-0

E-Mail: wlan.lwc@bsi.bund.de

Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Funk-LANs bzw. Wireless-LANs (WLANs), basierend auf dem 1997 vom Institute of Electrical and Electronics Engineers (IEEE) definierten Standard IEEE 802.11, bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netzwerke aufzubauen oder bestehende drahtgebundene Netzwerke zu erweitern.

Aufgrund der einfachen Installation werden Funk-LANs auch für temporär zu installierende Netze (z. B. auf Messen) verwendet. Darüber hinaus besteht die Möglichkeit, an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen Netzwerkzugänge, so genannte Hot Spots anzubieten, um den mobilen Benutzern Verbindungen in das Internet oder in ihr Home-Office zu ermöglichen.

Bereits seit Mitte 2001 sind Sicherheitslücken im Standard bekannt, die zu großen Sicherheitsproblemen führen können. Im Folgenden werden für Administratoren und Anwender von Funk-LANs nach IEEE 802.11 Informationen über Sicherheitsmechanismen, mögliche Sicherheitslücken und entsprechende Gegenmaßnahmen dargestellt.

2 Grundlagen

Die Mehrzahl der derzeit am Markt verfügbaren Funk-LAN Systeme basieren auf der 1999 vom IEEE verabschiedeten Erweiterung 802.11b des Standards 802.11. Die Hersteller-Vereinigung WiFi-Alliance (vormals WECA) dokumentiert die Kompatibilität zum Standard 802.11b durch die Vergabe des WiFi-Zertifikats. Seit November 2002 sind in Deutschland auch Frequenzen im 5 GHz-Bereich freigegeben, sodass auch Systeme der Standards 802.11a bzw. 802.11h zum Einsatz kommen werden. Aktuell ist auch IEEE 802.11g verabschiedet worden, sodass künftig mit dem Einsatz kompatibler Systeme zu rechnen ist.

2.1 Architekturen

Funk-LANs können in zwei verschiedenen Architekturen betrieben werden. Im Ad-hoc-Modus (siehe Abb. 1) kommunizieren zwei oder mehr mobile Endgeräte, die mit einer Funk-LAN-Karte ausgestattet sind (Clients), direkt miteinander.

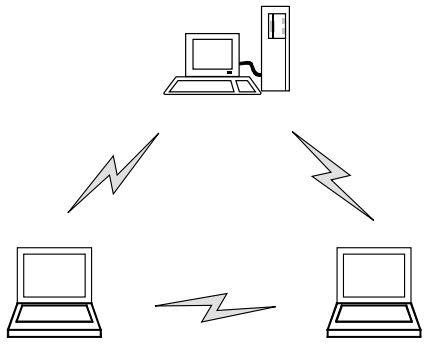


Abb. 1: Ad-hoc-Modus (Peer to Peer Kommunikation)

In den meisten Fällen wird ein Funk-LAN im Infrastruktur-Modus betrieben, d. h. die Kommunikation der Clients erfolgt über eine zentrale Funkbrücke, den sog. Access-Point (siehe Abb. 2a). Über den Access-Point erfolgt auch die Verbindung in kabelgebundene LAN-Segmente (siehe Abb. 2b).

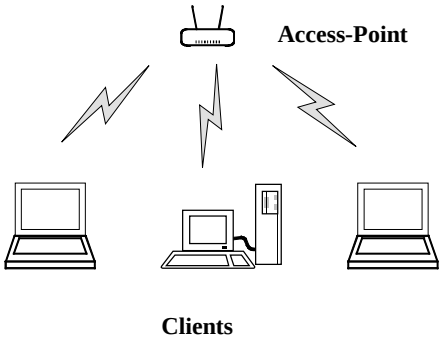


Abb. 2a:
Infrastruktur-Modus
(Clients u. Access-Point)

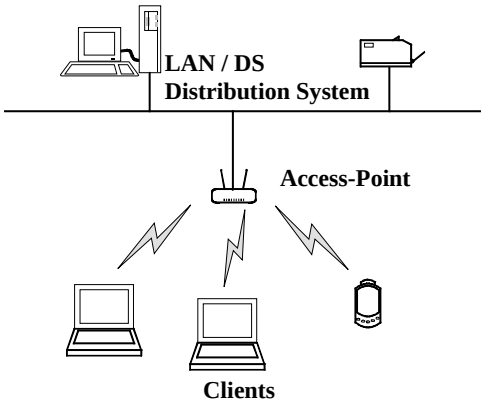


Abb. 2b:
Infrastruktur-Modus (Access- Point Anbindung an kabelgebundenes LAN)

Der Infrastruktur-Modus lässt mehrere Einsatzvarianten zu:

- Mittels mehrerer Access-Points können überlappende Funkzellen installiert werden, sodass beim Übergang eines Clients in die nächste Funkzelle die Funkverbindung aufrecht erhalten werden kann („Roaming“). Auf diese Weise können große Bereiche flächendeckend versorgt werden. Die Reichweite einer Funkzelle ist extrem abhängig von den Umgebungsbedingungen und liegt im Bereich von ca. 10 - 150 Meter.
- Zwei Access-Points können auch als Brücke (Bridge) zwischen zwei leitungsgebunden LANs eingesetzt werden. Ebenso ist der Einsatz eines Access-Points als Relaisstation (Repeater) zur Erhöhung der Reichweite möglich.
- Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access-Points kann ein Funk-LAN auch zur Vernetzung von Liegenschaften eingesetzt werden. Hier können lt. Herstellerangaben Reichweiten im Kilometerbereich erreicht werden. Die Access-Points können dabei als Relaisstation oder Brücke betrieben werden.

Der Standard verwendet die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netzwerke im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access-Point. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netzwerk wird Distribution System (DS) genannt.

2.2 Funkschnittstelle

Die in Deutschland und in fast allen Staaten Europas zugelassenen Funk-LAN-Systeme nach 802.11 und 802.11b nutzen das ISM-Frequenzband (Industrial-Scientific-Medical) zwischen 2,4 und 2,48 GHz, das gebührenfrei und ohne zusätzliche Genehmigung verwendet werden kann. Die Sendeleistung ist auf maximal 100 mW EIRP (Effective Isotropic Radiated Power) begrenzt.

Systeme des Standards 802.11 übertragen die Daten mit einer Rate von 1 bzw. 2 Mbit/s mittels Bandspreizverfahren, entweder mittels Frequenzsprung- (FHSS) oder Direct-Sequence- (DSSS) Verfahren. Der Vollständigkeit halber sei erwähnt, dass 802.11 auch eine Infrarot-Übertragung definiert, die bisher aber in der Praxis bedeutungslos geblieben ist.

Die aktuellen Systeme nach Standard 802.11b verwenden nur das DSSS Verfahren. Die zu übertragenen Daten werden mit einem festen Code gespreizt, um die Übertragung unempfindlicher gegen Störung zu machen. Der Zugriff auf den Funkkanal erfolgt, wie bei allen Systemen der 802.11 Standards, nach einem zufallsgesteuerten Verfahren, genannt Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Die Brutto-Datenübertragungsrate beträgt bei 802.11b maximal 11 Mbit/s. Die Übertragungsraten können, wie bei allen Systemen der 802.11 Standards, nicht garantiert werden, sie hängen ab von der Anzahl der Clients und der Qualität der Funkübertragungsstrecke.

Im 2,4 GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden, beispielsweise die Kanäle 2, 7 und 12 (siehe Abb. 3).

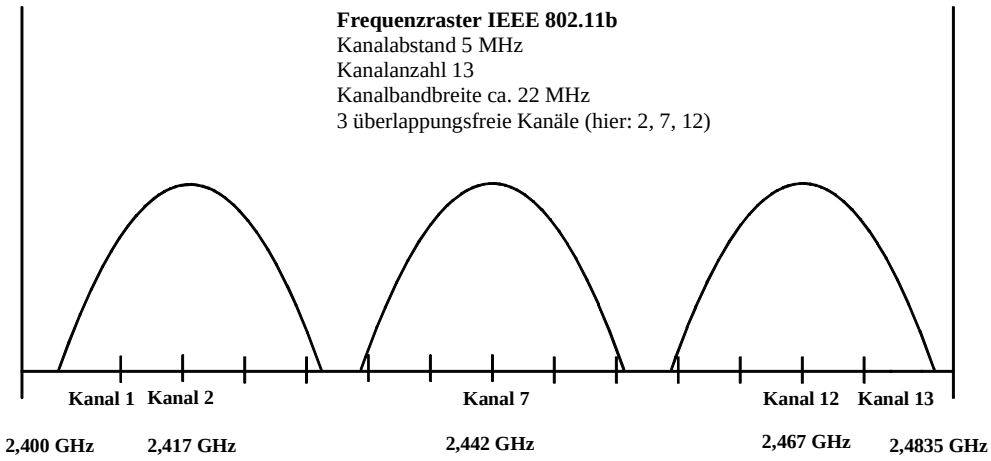


Abb. 3: 802.11b Kanalraster, überlappungsfreie Kanäle

Neben den 802.11b Systemen werden nun auch 802.11a und 802.11g Systeme angeboten und weitere Standards wie 802.11h stehen vor der Fertigstellung. Alle drei Standards definieren gegenüber 802.11b eine unterschiedliche physikalische Übertragungstechnik zur Realisierung höherer Übertragungsraten von bis zu 54 Mbit/s (brutto).

802.11g Systeme arbeiten im gleichen Frequenzbereich wie 802.11b, sodass auch hier nominell 13 Kanäle in Deutschland zur Verfügung stehen. Bei einer Bandbreite der Funksignale von 20 bzw. 22 MHz können maximal 4 Kanäle gleichzeitig in räumlicher Nähe betrieben werden ohne sich gegenseitig zu stören.

802.11a und zukünftige 802.11h Systeme nutzen den 5 GHz-Bereich. Im Frequenzbereich von 5,15 bis 5,35 GHz und bei 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden [REGTP]. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört.

2.3 Sicherheitsmechanismen

Die Sicherheitsmechanismen aller 802.11 kompatiblen Systeme sind im Standard 802.11 definiert. Die Erweiterungen a, b, g und h des Standards bieten keine zusätzlichen Sicherheitsmechanismen, erst die Erweiterung i wird neue Sicherheitsmechanismen definieren. Die zurzeit in 802.11 definierten Mechanismen dienen ausschließlich zur Sicherung der Funkstrecke zwischen den Clients und Access-Points. Darüber hinaus lässt der Standard aber auch Freiraum für proprietäre Erweiterungen.

Sämtliche Sicherheitsmechanismen des Standards 802.11, die im Folgenden dargestellt werden, sind überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen.

2.3.1 Netzwerkname (SSID)

Der Standard bietet die Möglichkeit einen Netzwerknamen (ESSID bzw. SSID: (Extended) Service Set Identity) zu vergeben. Dabei gibt es zwei Betriebsarten. Wird durch den Nutzer die Kennung „Any“ angegeben, akzeptiert die Funk-LAN-Komponente beliebige SSIDs. Im anderen Fall wird der eingetragene Name überprüft und nur Teilnehmer mit der gleichen SSID können am Netzwerk teilnehmen. Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID dazu, den nächsten Access-Point zu finden. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie mit einfachen Mitteln in Erfahrung bringen. Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden. Das Unterdrücken der SSID auf diese Weise ist jedoch nicht standardkonform.

2.3.2 MAC-Adresse

Jede Netzwerkkarte verfügt über eine eindeutige Hardwareadresse die sog. MAC-Adresse (Media Access Control-Adresse). Prinzipiell ist es möglich, in einem Funk-LAN MAC-Adressen zu definieren, denen es erlaubt ist, mit einem Access-Point zu kommunizieren. Die Adresslisten müssen hierfür allerdings „von Hand“ gepflegt werden, was einen nicht unerheblichen Aufwand nach sich zieht. In vielen Einsatzszenarien ist dies nicht möglich. Das Filtern der MAC-Adressen ist nicht im Standard enthalten. Andererseits ist die Filterung von MAC-Adressen standardkonform, da die Filterung keine Auswirkungen auf die Kompatibilität der Clients hat.

2.3.3 WEP Verschlüsselung, Integritätsschutz und Authentisierung

Vertraulichkeit, Integrität und Authentizität im Funk-LAN sollen durch das „Wired Equivalent Privacy“-Protokoll (WEP) gesichert werden. Das WEP-Protokoll basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem *Schlüssel* und einem *Initialisierungsvektor (IV)* in Chiffratdaten umgewandelt werden. Der *Schlüssel* ist dabei eine Zeichenkette von wahlweise 40 oder optional 104 Bit und muss den am Funk-LAN beteiligten Clients sowie dem Access-Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte Funk-LAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das Funk-LAN übertragen.

Über WEP soll die *Vertraulichkeit* und *Integrität* der übertragenen Daten gesichert sowie die *Authentisierung* des Endgerätes (nicht des Nutzers) durchgeführt werden. Die Realisierung geschieht wie folgt:

- **Vertraulichkeit:** Aus dem Schlüssel und dem IV wird ein pseudozufälliger Bitstrom generiert. Die Chiffratdaten ergeben sich, indem die Klardaten bitweise mit dem Bitstrom XOR-verknüpft werden (XOR = exklusives Oder). Beim Empfänger werden die Klardaten wiederum aus den Chiffratdaten ermittelt, indem derselbe Bitstrom mit den Chiffratdaten XOR-verknüpft wird.
- **Integrität:** Für jedes zu übertragene Datenpaket wird eine 32-Bit CRC-Checksumme berechnet. Anschließend wird das Datenpaket mit der angehängten Checksumme verschlüsselt. Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Ist die Checksumme korrekt, wird das Datenpaket angenommen, andernfalls wird es verworfen.

- **Authentisierung:** In Verbindung mit der WEP-Verschlüsselung kann zwischen zwei Authentisierungsmodi gewählt werden: „Open“ (hierbei findet keine Authentisierung statt) und „Shared Key“. Für die Authentisierung im „Shared Key“-Modus wird ein sog. Challenge-Response-Verfahren durchgeführt: Der Access-Point generiert 128 zufällige Bytes und sendet diese in einem Datenpaket unverschlüsselt an einen Client (Challenge). Der Client verschlüsselt das Datenpaket und sendet es zurück zum Access-Point (Response). Der Client hat sich erfolgreich authentisiert, wenn der Access-Point die Response zur Challenge entschlüsseln kann. Der Authentisierungsprozess ist nur einseitig: der Access-Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten.

Wie erwähnt und in Abbildung 4 dargestellt, verschlüsselt WEP die übertragenen Nutzdaten und die Integritätschecksumme. Management- und Steuersignale (Management- und Controll-Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

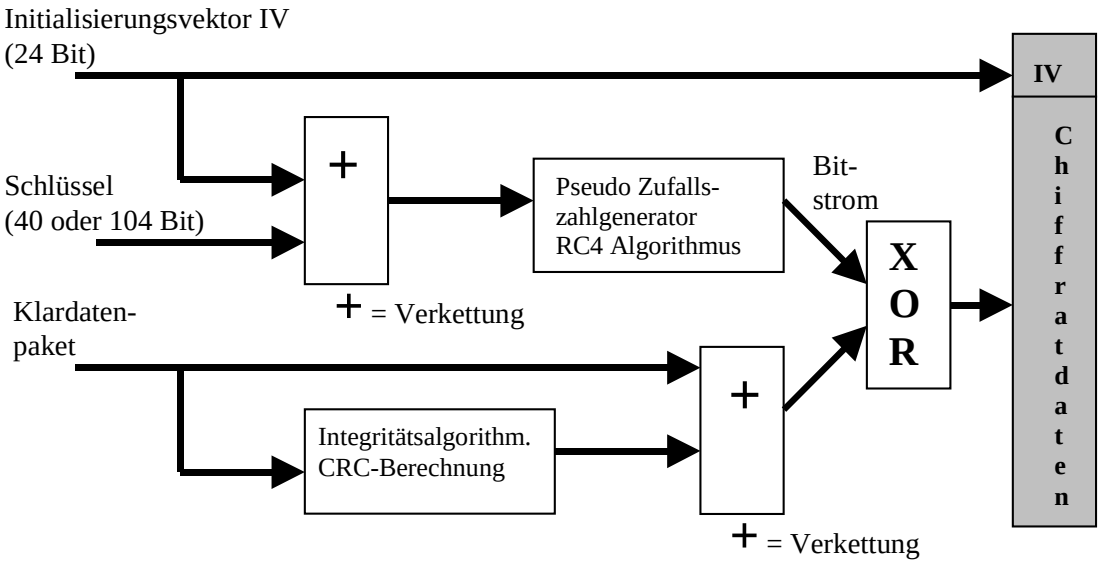


Abb. 4: Blockschaltbild von WEP

3 Sicherheitsprobleme

Die aktuellen standardkonformen Funk-LAN-Systeme bergen bzgl. der Sicherheit große Schwachstellen, die aktive wie passive Angriffe erlauben und damit zu einem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen können. Im Folgenden werden mögliche Sicherheitsprobleme beim Einsatz dieser Technologie exemplarisch aufgeführt.

3.1 Sicherheitskritische Grundeinstellung

Im Auslieferungszustand sind die Funk-LAN Komponenten häufig so konfiguriert, dass keine oder nur einige der zudem schwachen Sicherheitsmechanismen aktiviert sind.

3.2 SSID Broadcast

Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das Funk-LAN vor Unbefugten zu verstecken (so genanntes „Closed System“). Dieser Schutz wirkt gegen diverse frei verfügbare Tools wie z. B. Netstumbler, jedoch kann mittels Funk-LAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.

3.3 Manipulierbare MAC-Adressen

Jede Netzwerkkarte verfügt über eine eindeutige Hardwareadresse die sog. MAC-Adresse (Media Access Control-Adresse). Diese MAC-Adressen der Funk-Clients können relativ einfach abgehört und manipuliert werden, somit sind die in den Access-Points zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar.

3.4 Fehlendes Schlüsselmanagement

Schlüssel müssen in einem Funk-LAN „von Hand“ verteilt werden, d. h. in jedem Funk-LAN-Adapter (Client) und im Access-Point muss der gleiche statische Schlüssel eingetragen werden. Dies erfordert physischen Zugriff auf die Komponenten. Diese Art des „Schlüsselmanagements“ führt in der Praxis oft dazu, dass der geheime Schlüssel sehr selten oder überhaupt nicht gewechselt wird.

Die Offenbarung eines Schlüssels, z. B. durch Verlust eines Clients oder mittels frei verfügbarer Tools, kompromittiert das gesamte Funk-LAN. Der gemeinsame geheime Schlüssel eines Funk-LAN-Clients wird, je nach Hersteller, entweder auf der Funk-LAN-Karte oder auf der Festplatte des Client-Rechners gespeichert; einige Hersteller schreiben diese Informationen sogar offen in die Registry-Datei des Windows-Betriebssystems.

3.5 Schwachstellen in WEP

Das Ziel mittels WEP Vertraulichkeit, Integrität und Authentizität im Funk-LAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert; es existieren sogar frei verfügbare Tools für passive Angriffe.

Für eine detailliertere Betrachtung der Schwachstellen von WEP werden diese im nachfolgenden in zwei Kategorien eingeteilt.

3.5.1 Schwachstellen im Protokoll

Die Mechanismen zur Verschlüsselung, Integritätssicherung und Authentisierung des WEP-Protokolls besitzen folgende konkrete Schwachstellen:

- **Die Schlüssellänge von 40 Bit ist viel zu kurz.** Bei einem aufgezeichneten Chiffrat kann das Chiffrat selbst mit einem handelsüblichen PC innerhalb weniger Tage mit sämtlichen infrage kommenden Schlüsseln probe-entschlüsselt werden, um denjenigen Schlüssel herauszufinden, welcher „vernünftige“ Klardaten liefert. Bis zum nächsten Schlüsselwechsel, sofern dieser überhaupt vorgesehen ist, ist eine unberechtigte Teilnahme im Funk-LAN möglich. Eine Schlüssellänge von 104 Bit ist hingegen ausreichend, um sich auch vor versierteren Angreifern gegen ein Durchprobieren sämtlicher Schlüssel zu schützen.

- **Die Länge von 24 Bit des IV ist viel zu kurz.** Ein Stromchiffrier-Algorithmus kann nur dann sicher sein, wenn der generierte Bitstrom für je zwei Datenpakete unterschiedlich ist. Wird nämlich zweimal mit demselben Bitstrom verschlüsselt, lassen sich sowohl die beiden Datenpakete als auch der Bitstrom in vielen Fällen rekonstruieren. Da sich der Bitstrom aus dem Schlüssel und dem IV berechnet und der Schlüssel für längere Zeit als konstant angenommen werden kann, kann es ausreichend sein, zwei verschlüsselte Datenpakete mit demselben IV abzufangen, um diese zu entziffern. Mit 24 Bit sind maximal ca. 16,8 Mio. verschiedene IVs generierbar. Sofern der IV zufällig generiert wird, ist nach ca. 4000 Datenpaketen die erste Wiederholung eines IVs zu erwarten. Bei regem Datenverkehr zwischen Access-Point und den per Funk-LAN angeschlossenen Rechnern ist nach einigen Stunden Aufzeichnung zu erwarten, dass jeder IV mindestens ein Mal verwendet wurde und von dort ab der Funk-LAN-Verkehr mit hoher Verlässlichkeit mitgelesen werden kann. Die Problematik des zu kurzen IVs betrifft Schlüssellängen von 40 und 104 Bit gleichermaßen.
- **Datenpakete können gefälscht werden.** Der von der Stromchiffre generierte Bitstrom ist abhängig von dem verwendeten Schlüssel und dem IV. Gelangt ein Angreifer in den Besitz eines einzigen dieser generierten Bitströme, so ist er fortan in der Lage, bis zum nächsten Schlüsselwechsel beliebige Datenpakete zu fälschen, d. h. „korrekte“ Chiffrate zu erzeugen. Sind zu einem abgehörten Chiffrat die Klardaten bekannt, kann aus dem Chiffrat der generierte Bitstrom durch die einfache XOR-Struktur leicht berechnet werden. Wird anschließend der berechnete Bitstrom zum Chiffrieren wiederverwendet, haben diese Chiffrate zwar alle den gleichen IV - die mehrfache Verwendung eines IVs ist jedoch möglich, da der IV ausschließlich vom Sender festgelegt wird und somit der Angriff von den anderen Teilnehmern des Funk-LANs nicht bemerkt werden kann. Der Angreifer gelangt am einfachsten an einen Bitstrom, indem er eine Authentisierung mithört (s.u.).
- **Das Authentisierungsprotokoll kann gebrochen werden.** Wird von einem Angreifer ein vollständiges Authentisierungsprotokoll aufgezeichnet, kann er sich in Zukunft selbst authentisieren, ohne im Besitz des Schlüssels zu sein. Hierzu bildet er die XOR-Verknüpfung aus Challenge und Response. Mit dem so erhaltenen Bitstrom kann er zu einer gegebenen Challenge selbst die Response berechnen. Da für die Authentisierung und für die Verschlüsselung derselbe Schlüssel verwendet wird, können zudem mit dem errechneten Bitstrom Nachrichten gefälscht werden (s.o.).
- **Die Integritätssicherung ist wirkungslos.** Durch das Anfügen der CRC-Summe an die Datenpakete sollen sowohl zufällige als auch mutwillige Störungen auf dem Übertragungswege erkannt werden. Gegen zufällige Störungen hilft das: Fehler werden mit einer Wahrscheinlichkeit von lediglich 2^{-32} nicht erkannt. Werden hingegen gezielt Bits in den Chiffratdaten gestört, was wegen der einfachen XOR-Struktur des Stromchiffrier-Algorithmus die Störung der entsprechenden Bits im Klartext zufolge hat, kann die verschlüsselte CRC-Summe ebenfalls manipuliert werden, sodass die Störung beim Empfänger nicht erkannt wird. Grund hierfür ist die Linearität der CRC-Summe und die XOR-Struktur des Stromchiffrier-Algorithmus.

Es sei hier nochmals erwähnt, dass nur eine einseitige Authentisierung des Clients durchgeführt wird; Access-Point und Nutzer müssen sich nicht authentisieren.

Die hier beschriebenen Schwachpunkte des WEP-Protokolls sind bereits Grund genug, keine sensiblen Daten damit zu übertragen. Über die Schwächen des Protokolls und des Operationsmodus hinaus, existieren eklatante Designschwächen des Chiffrieralgorithmus RC4, die eine rein passive Angriffsmöglichkeit auf das WEP-Protokoll eröffnen.

3.5.2 Schwachstellen im RC4-Design

Seit 2001 sind Schwächen im RC4-Design bekannt, die mit statistischer Analyse ausgenutzt werden können [FMS01]. Mittels im Internet erhältlicher Tools sind mittlerweile auch weniger versierte Lauscher in der Lage, den Angriff auf das WEP-Protokoll durchzuführen.

Kurz beschrieben verläuft der Angriff wie folgt: Ein Angreifer muss lediglich eine bestimmte Anzahl von verschlüsselten Paketen mit den zugehörigen IVs sammeln, die mit ein und demselben Schlüssel, aber unterschiedlichen, geeigneten[1] IVs, verschlüsselt wurden. Hieraus lässt sich dann mit statistischen Methoden der komplette Schlüssel bestimmen.

Da die für einen Angreifer interessanten Pakete mit geeigneten IVs relativ selten sind, muss eine große Anzahl von Paketen passiv abgehört werden. Wie viele Pakete insgesamt notwendig sind, um den Angriff durchzuführen, hängt davon ab, wie die IVs gewählt werden. In den meisten Fällen wird ein einfacher Zähler (Little Endian) als IV verwendet. In diesem Fall schätzen Fluhrer, Mantin und Shamir [FMS01], dass ca. 4 Millionen Pakete abgehört werden müssen, um den Angriff durchführen zu können. Stubblefield, Ioannidis und Rubin [SIR01] stellen fest, dass in der Praxis durchschnittlich 5-6 Millionen Pakete notwendig sind. Die gleichen Autoren stellen in [SIR02] eine Verbesserung des Angriffs auf RC4 vor, sodass nur noch 1 Million Pakete notwendig sein sollen. Hierzu sind zurzeit (noch) keine öffentlich zugänglichen Tools bekannt.

Die für den Angriff benötigte Zeit ist nicht nur von der Anzahl der abzuhörenden Pakete abhängig, sondern im Wesentlichen auch von der durchschnittlichen Paketgröße der Nettoübertragungsrate und der Auslastung des Access-Points[2]. In den folgenden Tabellen findet sich eine Abschätzung, wie viel Zeit für den Angriff auf ein typisches System nach IEEE 802.11b benötigt wird. Für höhere Datenratenübertragungsraten, z. B. bei Systemen nach den Standards 802.11a und 802.11g, verringert sich die benötigte Zeit entsprechend.

Anzahl Pakete	**Paketgröße**		
	512 Byte	1024 Byte	2048 Byte
2.000.000	0,95 GB	1,91 GB	3,81 GB
4.000.000	1,91 GB	3,81 GB	7,63 GB
6.000.000	2,86 GB	5,72 GB	11,44 GB
8.000.000	3,81 GB	7,63 GB	15,26 GB

Tabelle 1: Benötigte Datenmenge in Abhängigkeit von der durchschnittlichen Paketgröße und der Anzahl der Pakete

[1] Interessant sind für den Angreifer dabei nur solche Pakete, die im ersten Byte des IVs einen Wert zwischen i=3 und i=15 und im zweiten Byte den Wert 255 haben; hiervon werden für jeden Wert i zwischen 3 und 15 ca. 60 IVs benötigt. Außerdem ist von den zugehörigen Chiffratdaten nur das erste Byte erforderlich. Da ein unverschlüsseltes Funk-LAN-Paket stets mit demselben Byte (nämlich hexadezimal AA) beginnt, kann aus dem ersten Chiffratbyte das erste Byte des RC4-Bitstroms ermittelt werden.

[2] Die durchschnittliche Paketgröße bestimmt sich zum einen durch die Nutzungsart des LANs (z.B. Surfen oder Down- bzw. Upload von großen Dateien) und zum anderen durch die Verbindungsqualität. Je schlechter die Verbindung zwischen dem Client und dem Access-Point ist, desto kleiner werden die übertragenen Pakete. Bezogen auf die Nettodaten der Funkschnittstelle (inkl. IP-Header) beträgt die maximale Paketgröße 2304 Byte und der maximale Durchsatz eines Access-Points liegt bei etwa 5 Mbit/s für 802.11b Systeme.

Datenmenge	Auslastung		
	5 Mbit/s	1 Mbit/s	0,1 Mbit/s
0,95 GB	25 min	2,11 h	21,11 h
1,91 GB	50 min	4,24 h	42,44 h
2,86 GB	1,27 h	6,36 h	2,65 Tage
3,81 GB	1,70 h	8,47 h	3,53 Tage
5,72 GB	2,54 h	12,71 h	5,30 Tage
7,63 GB	3,39 h	16,96 h	7,06 Tage
11,44 GB	5,08 h	25,42 h	10,59 Tage
15,26 GB	6,78 h	33,91 h	14,13 Tage

Tabelle 2: Benötigte Zeit in Abhängigkeit von der Datenmenge und der durchschnittlichen Auslastung des Access-Points für 802.11b Systeme

Beispiel: Gemäß Tabelle 1 und 2 sind beispielsweise bei einer durchschnittlichen Paketgröße von 1024 Byte und geschätzten 4 Millionen benötigten Paketen insgesamt 3,81 GB an abgehörten Daten notwendig, um den Angriff auf RC4 durchführen zu können. Bei einem Access-Point mit mittlerer Auslastung, also z. B. bei einer durchschnittlichen Auslastung von 1 Mbit/s benötigt der Angriff demnach ca. 8,4 Stunden.

Obwohl schon bei nur mäßiger durchschnittlicher Auslastung des Funk-LANs der Schlüssel in relativ kurzer Zeit ermittelt werden kann, ist ein regelmäßiger Schlüsselwechsel (so oft wie praktikabel) trotzdem sinnvoll. Dadurch wird ein Angreifer gezwungen, ständig neu den momentan gültigen Schlüssel zu ermitteln. Optimal wäre jedoch nur ein automatisierter Schlüsselwechsel.

3.6 Bedrohung der lokalen Daten

Auf den Client-Rechnern entstehen durch die Teilnahme eines Clients am Funk-LAN zusätzliche Bedrohungen für die lokalen Daten. Lokale Datei- bzw. Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung meist auch über das Funk-LAN Zugriffe auf diese Ressourcen. Ebenso sind bei eingeschaltetem Funk-LAN Angriffe auf den Rechner zu befürchten, die Schwachstellen des verwendeten Betriebssystems ausnutzen. Diese Gefahren bestehen insbesondere bei der Nutzung von Funk-LAN-Komponenten in öffentlichen Bereichen, in Hot Spots und in Ad-hoc-Netzwerken.

3.7 Unkontrollierte Ausbreitung der Funkwellen

Auch über die spezifizierte Reichweite von 10 - 150 Metern hinaus, breiten sich die Funkwellen der Funk-LAN-Komponenten aus und können je nach Umgebungsbedingungen und der Leistungsfähigkeit der verwendeten Empfangsgeräte empfangen werden. Dies bedeutet, dass auch über die Nutzreichweite der Funk-LANs hinaus eine konkrete Abhörgefahr besteht.

3.8 Bedrohung der Verfügbarkeit

Funk-LANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die Funk-LAN Kommunikation stören und im Extremfall den Betrieb des Funk-LANs verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z. B. Bluetooth Geräte, andere Funk-LANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras, etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff erfolgen. Darüber hinaus sind Denial-Of-Service-Angriffe auch möglich durch wiederholtes Senden bestimmter Steuer- und Managementsignale.

3.9 Erstellung von Bewegungsprofilen

Da die Hardwareadresse einer Funk-LAN-Karte, die sog. MAC-Adresse, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar.

Auf diese Weise können Bewegungsprofile über mobile Nutzer, die sich in öffentliche Hot Spots einbuchen, erstellt werden. Da die MAC-Adresse grundsätzlich unverschlüsselt übertragen wird, ist das Erstellen von Bewegungsprofilen keinesfalls nur den Betreibern der Hot Spots möglich. Prinzipiell kann jeder, der an geeigneten öffentlichen Plätzen eine Funk-LAN-Komponente installiert, die MAC-Adressen anderer Nutzer mitlesen.

Sendet der Nutzer zusätzlich personenbezogene Daten unverschlüsselt über das Funknetz, können auch diese mitgelesen und mit dem Bewegungsprofil zusammengeführt werden.

4 Maßnahmen

Zur Erhöhung der Sicherheit beim Einsatz von Funk-LAN-Komponenten sind - abhängig vom Einsatzszenario und dem Schutzbedarf der Informationen - mehrere Maßnahmen erforderlich. Die Maßnahmen sind in drei Kategorien unterteilt:

A. Konfiguration und Administration der Funkkomponenten
B. Zusätzliche technische Maßnahmen
C. Organisatorische Maßnahmen

4.1 Konfiguration und Administration der Funkkomponenten

Diese einfachen Basisschutzmaßnahmen an den Funkkomponenten des Funk-LANs sollten trotz bekannter Unzulänglichkeiten aktiviert werden, um Angriffe mit freiverfügbaren Tools abzuwehren.

A1: Basisschutzmaßnahmen aktivieren:

A1.1 Passwortvorgaben ändern

- Standard SSID ändern (am Access-Point und bei allen Clients): Die SSID sollte keine Rückschlüsse auf Firma oder Netzwerk zulassen.
- Standard Passwort zur Konfiguration des Access-Points ändern

A1.2 SSID Broadcast am Access-Point abschalten - falls technisch möglich -

A1.3 MAC Adress-Filterung am Access-Point einschalten - falls technisch möglich -

A1.4 WEP Verschlüsselung einschalten - falls möglich 128 Bit -

A1.5 In Verbindung mit der WEP Verschlüsselung ist - falls technisch möglich - die Authentisierungsmethode „Open“ zu wählen, da die Option „Shared Key“ zusätzliche Sicherheitsprobleme birgt (vgl. Kapitel Sicherheitsprobleme).

A2: WEP Schlüssel periodisch wechseln (vgl. Kapitel Sicherheitsprobleme)

Hinweis: WEP Schlüssel, SSIDs und Zugangspassworte sollten entsprechend anerkannter Passwortgestaltungsregeln (z. B. in [GSHB]) so gewählt werden, dass sie einen möglichst wirksamen Schutz gegen Angreifer bieten.

A3: Aufstellort und Antennencharakteristik des Access-Points optimieren

Aufstellort und Antennencharakteristik des Access-Points sollten so gewählt werden, dass möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Dabei ist zu beachten, dass sich die Funkwellen sowohl horizontal als auch vertikal ausbreiten.

A4: Sendeleistung am Access-Point optimieren

Die Sendeleistung am Access-Point sollte - falls technisch möglich - reduziert werden, damit nach Möglichkeit nur das gewünschte Gebiet funktechnisch versorgt wird. Hierbei ist zu beachten, dass zur Erzielung der maximalen Datenübertragungsrate ein bestimmtes Signal-Rauschverhältnis erforderlich ist.

A5: DHCP Server im Access-Point abschalten

Der DHCP (Dynamic Host Configuration Protocol) Server im Access-Point sollte - falls vorhanden und technisch möglich - abgeschaltet werden, d. h. es sollten statische IP Adressen vergeben und der zulässige IP-Adressraum sollte möglichst klein eingestellt werden. Der DHCP Server wird einem Eindringling andernfalls automatisch eine gültige IP-Adresse zuweisen.

A6: Firmware Upgrade durchführen

Die Firmware der Systemkomponenten sollte, wenn möglich, auf erweiterte Sicherheitsstandards aktualisiert werden. Diese Möglichkeit wird von vielen Herstellern angeboten. Dabei ist zu beachten, dass diese Sicherheitsmechanismen proprietäre Erweiterungen des Standards sind. Daher können nur Systemkomponenten mit der gleichen Erweiterung zusammen verwendet werden. Andernfalls werden die proprietären Sicherheitsmechanismen nicht aktiviert. Dies geschieht im Allgemeinen ohne den Benutzer hiervon in Kenntnis zu setzen.

A7: Frequenzkanäle überlappungsfrei einstellen

Beim Einsatz mehrerer Access-Points sind die benutzten Frequenzkanäle benachbarter Access-Points möglichst überlappungsfrei zu wählen (siehe Kapitel Funkschnittstelle).

A8: Funk-LAN-Komponenten nur bei Gebrauch einschalten

Bei Nichtbenutzung der Funk-LAN-Komponenten sollte deren Funktion deaktiviert werden. Dies gilt gleichermaßen für Access-Points und Clients, bei letzteren insbesondere auch für den Ad-Hoc-Modus.

A9: Konfiguration der Access-Points nur über sichere Kanäle

Die Konfiguration und Administration der Access-Points sollte nur über sichere Kanäle erfolgen, d. h. drahtgebundene Übertragungswege sind der Funkübertragung vorzuziehen und bei der Wahl der Management-Protokolle sind die als sicher geltenden Protokolle wie z. B. SSL/TLS oder SNMPv3 zu nutzen. Der physische Zugriff auf die Access-Points sollte nur autorisierten Personen möglich sein.

Zwischenfazit

Durch korrekte Konfiguration und Administration der Funkkomponenten des Funk-LANs können trotz bekannter Unzulänglichkeiten viele Angriffe abgewehrt werden, die mit freiverfügbaren Tools durchführbar sind. Dadurch wird Schutz gegen unbeabsichtigtes Einloggen in ein Funk-LAN und gegen Mithören des Funk-LAN-Datenverkehrs durch Gelegenheitslauscher erreicht. Die Verfügbarkeit des Systems kann mit diesen Maßnahmen ggf. geringfügig erhöht werden, bleibt aber dennoch leicht angreifbar.

Diese Maßnahmen reichen jedoch im Allgemeinen nicht aus zum Schutz von sensiblen Daten. Eine Ausnahme bildet ein Firmwareupgrade auf einen neuen Sicherheitsstandard wie WPA oder 802.11i (vgl. Kapitel Ausblick). In Behörden- und Firmennetzen mit einer größeren Anzahl von Benutzern sind darüber hinaus einige Maßnahmen (z. B. A1.3, A2, A5) nicht im erforderlichen Umfang praktikabel. In diesen Fällen sind weitere Maßnahmen erforderlich (siehe Maßnahmen B und C).

4.2 Zusätzliche technische Maßnahmen

Über den Standard 802.11 hinaus sind zur Erhöhung der Sicherheit folgende zusätzliche technische Maßnahmen erforderlich.

B1: Verwendung einer zusätzlichen Sicherheitslösung

Eine Sicherheitslösung hat zum Ziel, nur berechtige Clients und Access-Points in einem Virtual Private Network (VPN) miteinander kommunizieren zu lassen, sowie diese Kommunikation vertraulich und integritätsgeschützt zu halten. Daher sollte eine zusätzliche Sicherheitslösung die drei Bausteine Authentisierung, Verschlüsselung und Integritätssicherung sinnvoll miteinander kombinieren.

Hierzu wird hinter dem Access-Point jeder Liegenschaft ein VPN-Gateway installiert. Beim Verbindungsaufbau wird ein kryptographischer Tunnel (z. B. basierend auf dem Standard IPSEC oder SSL Version 3/TLS) zwischen dem Client und dem VPN-Gateway aufgebaut [SINA]. Da es sich bei IPSEC und SSL um Standards handelt, können alle marktgängigen Produkte, die diesen Standard erfüllen, verwendet werden. Mittlerweile gibt es Produkte, die die VPN-Funktionalität bereits im Access-Point integriert haben.

IEEE favorisiert die port-basierte Authentisierung nach dem Standard IEEE 802.1X, der auf dem Extensible Authentication Protocol (EAP, RFC2284) basiert. EAP stellt einen Rahmen für verschiedene Authentisierungsmethoden wie z. B. EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, etc. zur Verfügung. Beim Einsatz von 802.1X ist eine Authentisierungsmethode zu wählen, die tatsächlich eine gegenseitige Authentisierung durchführt (z. B. EAP-TLS). Weiterhin ist zu beachten: 802.1X bietet nur Authentisierung (und ggf. Schlüsselverteilung) und stellt daher keine integrierte Sicherheitslösung dar. 802.1X ist ohne passende Verschlüsselung / Integritätssicherung sogar unsicher [MA02]. Daher muss 802.1X zusammen mit z. B. TKIP / Michael verwendet werden, wie es in WPA bzw. 802.11i der Fall ist (vgl. Kapitel Ausblick).

Insgesamt bietet es sich an, eine Sicherheitslösung auf Basis von digitalen Zertifikaten und ggf. einer PKI-Infrastruktur zu nutzen. Dadurch wird zum einen das Schlüsselmanagement besser integriert und zum anderen können die Sperrlisten der PKI genutzt werden, um die Authentisierung zusätzlich abzusichern.

B2: Abschottung des drahtgebundenen Firmen-/Behördennetz durch Firewall und Intrusion Detection System

Das drahtgebundene Firmen-/Behördennetz sollte durch eine Firewall mit Intrusion Detection System (IDS) gegen die Access-Points des Funknetzes abgeschottet werden.

Mittlerweile sind neben leitungsgebundenen IDS auch spezielle funkbasierte IDS auf dem Markt verfügbar, die mit Funksensoren das Frequenzspektrum des Funk-LANs überwachen und sicherheitsrelevante Anomalien, wie z. B. falsche APs und unbekannte Clients, entdecken und melden. In bestimmten Szenarien ist der Einsatz solcher Systeme als Alternative bzw. Ergänzung zu leitungsgebundenen IDS empfehlenswert.

B3: Absicherung der Clients

Insbesondere bei mobilen Clients, die sich in verschiedene Funk-LANs einbuchen können, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z. B.: Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.[GSHB].

4.3 Organisatorische Maßnahmen

Diese nichttechnischen Maßnahmen dienen, in Kombination mit den Maßnahmen A und B, der Anhebung des Sicherheitsniveaus.

C1: Sicherheitsrichtlinien aufstellen

Für den Einsatz von Funk-LAN-Komponenten in Behörden und Unternehmen sollten individuelle Sicherheitsrichtlinien aufgestellt werden. Diese Funk-LAN spezifischen Sicherheitsrichtlinien sollten konform zum generellen Sicherheitskonzept der Behörde bzw. des Unternehmens sein und regelmäßig auf Aktualität überprüft und ggf. angepasst werden. Typische Punkte einer Funk-LAN Sicherheitsrichtlinie findet man z. B. in [NIST]. Nutzer der Funk-LANs sollten sensibilisiert werden für Gefährdungen sowie für Inhalte und Auswirkungen der Richtlinie.

C2: Einhaltung der Sicherheitsrichtlinien überprüfen

Die Einhaltung der Vorgaben sollte ständig kontrolliert werden. Mechanismen zur Überprüfung der Einhaltung sind z. B.:

- C2.1 Regelmäßige Kontrollen der Access-Points und Clients mittels Funk-LAN-Analysator und Netzwerk-Sniffer
- C2.2 Auswertung der Protokolldatei (Log) des Access-Points - falls technisch möglich - und Überprüfung der an einem Access-Point angemeldeten Clients

C3: Schutz personenbezogener Daten

Der Nutzer von öffentlichen Funk-Zugängen sollte sich versichern, dass der von ihm gewählte Hot-Spot-Anbieter (Wireless Internet Service Provider, WISP) datenschutzkonform mit den personenbezogenen Daten umgeht.

Das Erstellen von Bewegungsprofilen und die Analyse des Benutzerverhaltens über die Auswertung der MAC-Adresse des Netzwerkclients kann der Nutzer erschweren, falls er periodisch die MAC-Adresse ändert oder den Funk-LAN-Adapter regelmäßig austauscht.

4.4 Beispielszenarien zur Maßnahmenauswahl

Im Folgenden sind exemplarisch drei Beispielszenarien mit unterschiedlichem Schutzbedarf der über das Funk-LAN übertragenen Informationen dargestellt und die dazu empfohlenen Maßnahmen aufgeführt:

Beispielszenario 1:

Schutzbedarf der Informationen: gering

Empfohlene Maßnahmen: A1, A2, A3, A4, A5, A6, A7, A8, A9 und B3 und C1, C2

Beispielszenario 2:

Schutzbedarf der Informationen: mittel - hoch

Empfohlene Maßnahmen: A1, A2, A3, A4, A5, A6, A7, A8, A9 und B1, B2, B3 und C1, C2

Beispielszenario 3:

Schutzbedarf der Informationen: keine - hoch (öffentlicher Funk-Zugang „Hot Spot")

Empfohlene Maßnahmen: A8 und B3 und C1, C2, C3

In Hot Spots wird i.d.R. nach erfolgreicher Authentifizierung des Funk-Clients auf eine Verschlüsselung der Nutzdaten verzichtet. Für die Vertraulichkeit der übertragenen Daten ist der Benutzer selbst verantwortlich, d. h. er sollte für Internet-Transaktionen (z. B. Abfrage des E-Mail-Postfachs) immer eine mittels SSL gesicherte Verbindung wählen. Der Zugang zum Firmen-/Behörden oder Heimnetz sollte über ein VPN durchgeführt werden (siehe Maßnahme B1).

Über die hier aufgeführten Maßnahmen hinaus sind zum Schutz von sensiblen Informationen auf mobilen Endgeräten, Rechnern und in Netzwerken im Einzelfall ggf. weitere Maßnahmen notwendig. Entsprechende Maßnahmen und Informationen zur Erstellung von Sicherheitskonzepten für den mittleren Schutzbedarf findet man im IT-Grundschutzhandbuch des BSI [GSHB].

Es sei ausdrücklich erwähnt, dass auch nach Durchführung der hier genannten Maßnahmen die Bedrohung der Verfügbarkeit der Funk-LAN-Systeme durch Funk-Störquellen weiterhin existent ist.

5 Ausblick

Voraussichtlich Ende des Jahres 2003 wird nach Verabschiedung des neuen Standards 802.11i eine robustere Sicherheitsarchitektur für Funk-LANs nach IEEE 802.11 verfügbar sein. Diese neue Sicherheitsarchitektur wird sich in zwei Teile gliedern:

- Vertraulichkeit und Integrität

  Hier wird sowohl ein neues auf AES (Advanced Encryption Standard) basierendes Protokoll angeboten, als auch eine auf WEP basierende Kompatibilitätslösung, die TKIP (Temporal Key Integrity Protocol) genannt wird.

- Authentisierung und Schlüsselmanagement

  Diese Protokolle werden auf dem Standard IEEE 802.1X basieren.

Die Herstellervereinigung Wi-Fi-Alliance hat Ende 2002 bekannt gegeben, TKIP und 802.1X, basierend auf den Drafts von IEEE 802.11i, unter dem Namen Wi-Fi Protected Access (WPA) zu unterstützen. WPA stellt eine zu IEEE 802.11i aufwärtskompatible Zwischenlösung dar. Es soll demnächst möglich sein, Wi-Fi zertifizierte Funk-LAN-Komponenten durch Firmware-Update auf WPA aufzurüsten. Dabei ist 802.1X optional für die Benutzerauthentisierung und das Schlüsselmanagement bei großen Funk-LAN-Installationen vorgesehen, während kleinere Funk-LANs weiterhin mit manuell verteilten Schlüsseln arbeiten. TKIP verwendet weiterhin WEP, jedoch werden zur Behebung der gröbsten Schwächen sicherheitsrelevante Veränderungen eingeführt. Diese sind ein erweiterter Initialisierungsvektor IV, eine dynamische Schlüsselerzeugung pro Datenpaket und ein kryptographischer Message

Integrity Check (MIC), genannt „Michael“. Michael wird zusätzlich zum CRC zur Integritätssicherung eingesetzt.

Auch bei WPA sind bereits mögliche neue Schwachstellen bekannt geworden: Entdeckt der Access-Point einen aktiven Angriff in Form von gefälschten Paketen, werden alle Verbindungen getrennt und der Access-Point wird für eine Minute inaktiv. Durch diese Gegenmaßnahme kann ein Angreifer das drahtlose Netzwerk unbrauchbar machen, indem er einfach gefälschte Pakete sendet (Denial of Service Angriff). Da diese zusätzliche Gegenmaßnahme oft kritisiert wurde, wird sie möglicherweise aus dem endgültigen Standard wieder entfernt.

Eine weitere Schwachstelle von WPA ist der mögliche Kompatibilitätsbetrieb eines Access-Points, sowohl mit WPA als auch mit WEP. In diesem Kompatibilitätsbetrieb werden zwar prinzipiell alle WPA-fähigen Clients mit dem Access-Point über WPA kommunizieren, es gibt jedoch einige Einschränkungen: Zum einen werden Multicast- und Broadcast-Nachrichten grundsätzlich mit WEP verschlüsselt, zum anderen sind nicht-WPA-fähige Clients in der Regel auch nicht 802.1X kompatibel. Dadurch kann die Authentisierung und der dynamische Schlüsselwechsel umgangen werden.

Aus diesen Gründen sollte der Kompatibilitätsbetrieb möglichst nicht verwendet werden, d. h. wenn alle Clients auf WPA umgestellt wurden, sollte der Access-Point ebenfalls so konfiguriert werden, dass ausschließlich WPA Verbindungen akzeptiert werden.

Das Sicherheitsniveau von WPA ist - bei Kenntnis der genannten Schwachstellen und Berücksichtigung der o.g. Empfehlung - wesentlicher stärker einzustufen als das des Standards IEEE802.11.

6 Fazit

Die Sicherheitsmechanismen des Standards IEEE 802.11 (und damit auch von IEEE 802.11b, a, h und g) erfüllen nicht die Anforderungen für eine Nutzung in sensitiven Bereichen. Trotz der dargestellten Sicherheitsprobleme sollten jedoch die im Standard definierten elementaren Schutzmaßnahmen im Funk-LAN aktiviert werden.

Für höhere Sicherheitsanforderungen sind zusätzliche Maßnahmen über den Standard 802.11 hinaus dringend erforderlich. Zurzeit sind im Wesentlichen nur proprietäre Erweiterungen, die untereinander meist nicht kompatibel sind, sowie WPA verfügbar. Neue Vorgaben hierzu wird der zukünftige Standard 802.11i voraussichtlich zum Ende des Jahres 2003 liefern. Bis zur Einführung der neuen Sicherheitsarchitektur ist WPA als Zwischenlösung zu empfehlen.

Aufgrund der gravierenden Schwächen von WEP bleibt zu hoffen, dass zügig mit der Integration von WPA und insbesondere von 802.11i in die Produkte begonnen wird. Es bleibt abzuwarten, ob die Implementierung korrekt erfolgt und somit keine neuen Angriffsmöglichkeiten entstehen.

Die höchste Sicherheit bei der Anbindung eines Funk-Clients an ein Firmen-/ Behördennetz bietet gegenwärtig ein korrekt implementiertes VPN, z. B. auf IPSEC oder SSL Basis.

7 Literatur

[IEEE] IEEE 802 LAN/MAN Standards, http://standards.ieee.org/getieee802

[WIFI] WECA WiFi Homepage, http://www.wi-fi.com

[SINA] BSI Projekt „Sichere Inter-Netzwerk Architektur“, http://www.bsi.bund.de/fachthem/sina/index.htm

[GSHB] BSI IT-Grundschutzhandbuch, http://www.bsi.bund.de/gshb

[UNOFF] „The Unofficial 802.11 Security Web Page“, http://www.drizzle.com/~aboba/IEEE/

[BGW01] N. Borisov, I. Goldberg und D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In 7th Annual International Conference on Mobile Computing and Networking, 2001, ACM-Press 2001

[FMS01] S. Fluhrer, I. Mantin und A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. In Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Springer-Verlag, Seiten 1-24.

[SIR01] A. Stubblefield, J. Ioannidis und A. Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. AT&T Labs Technical Report 2001

[SIR02] A. Stubblefield, J. Ioannidis und A. Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In 9th Annual Symposium on Network and Distributed System Security, 2002, http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf

[MA02] A. Mishra und W.A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X Standard, Technical Report CS-TR-4328, Departement of Computer Science, University of Maryland, 2002

[WPA] WiFi Alliance Darstellung von WiFi Protected Access

http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

[NIST] National Institut of Standards and Technology, Wireless Network Security, 11/2002 http://cs-www.ncsl.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[REGTP] Regulierungsbehörde für Post und Telekommunikation; http://www.regtp.de, Vfg. Nr. 154 / 1999 und Vfg. Nr. 35 / 2002

8 Glossar

802.11 Funk-LAN Spezifikation des IEEE; Datenrate bis 2 Mbit/s; im 2,4 GHz ISM Band; FHSS und DSSS; auch Infrarot Spektrum Kommunikation vorgesehen

802.11a 802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 5 GHz Band; OFDM;

802.11b 802.11 Erweiterung; Datenrate bis 11 Mbit/s; im 2,4 GHz Band; hohe Marktdurchdringung, DSSS/CCK

802.11g 802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 2,4 GHz Band; OFDM und DSSS

802.11h Zukünftige 802.11a Anpassung, im Bereich der Sendeleistung und Frequenzmanagement, für den Einsatz in Europa; Datenrate bis 54 Mbit/s; im 5 GHz Band; OFDM

802.11i Zukünftige 802.11 Erweiterung mit zusätzlichen Sicherheitsmerkmalen

802.1X Spezifikation eines portbasierenden Authentisierungsmechanismus durch IEEE

AES Advanced Encryption Standard

BSS Basic Service Set

CCK Code Complementary Keying; Modulationsart bei DSSS

Client Jeder mit einem Funk-LAN-Adapter (Funk-LAN-Karte) ausgestattete Rechner, der von anderen Teilnehmern des Funk-Netzwerkes Dienste in Anspruch nimmt

CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; Zugriffsverfahren auf den Funkkanal bei 802.11
CRC	Cyclic Redundancy Check; Bitfehler Erkennungsverfahren
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum; Codemultiplex – Bandspreizverfahren
EAP	Extensible Authentication Protocol
EAP-MD5	EAP-Variante, die Passwörter zur einseitigen Authentisierung benutzt
EAP-TLS	EAP-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EAP-TTLS	EAP-Tunneled-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EIRP	Effective Isotropic Radiated Power, mittlere äquivalente isotrope Strahlungsleistung
ESS	Extended Service Set
ESSID	Extended Service Set Identity; „Netzwerkname“ des Funk-LANs
FHSS	Frequency Hopping Spread Spectrum; Frequenzsprung – Bandspreizverfahren
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISM-Frequenzband	Industrial-Scientific-Medical, lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können
LAN	Local Area Network; Lokales Netz
MAC	Media Access Control; Funkzugriffsprotokoll auf ISO Layer 2 Data Link; Es definiert Paket-Format, Paket-Adressierung und Fehlerdetektion.
MAC-Adresse	Seriennummer einer Netzkomponente, die durch den Hersteller vergeben wird
MIC	Message Integrity Check, kryptographischer Integritätsschutzmechanismus
Michael	Name des MIC, der bei WPA und TKIP Verwendung finden soll
OFDM	Orthogonal Frequency Divison Multiplex
PEAP	Protected EAP, EAP-Variante zur gegenseitigen Authentisierung
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service; Authentisierungs- und Überwachungsprotokoll auf Anwendungsebene für Authentisierung, Integritätsschutz und Accounting im Bereich Netzzugang
RC4	Stromchiffrierverfahren von Ron Rivest, "Rons Code"
RFC2284	Request for Comments 2284, „Extensible Authentication Protocol“
SINA	Sichere Inter-Netzwerk Architektur
SNMPv3	Simple Network Management Protocol Version 3

SSID	Service Set Identity; „Netzwerkname“ des Funk-LANs
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport-Layer Security
Verkettung	Aneinanderhängen von Bitfolgen
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance; Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11; umbenannt zu WiFi-Alliance
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; Marketing Begriff generiert durch WECA
WiFi-Alliance	Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11; früher WECA
WPA	WiFi Protected Access; Bezeichnung für über IEEE 802.11 hinaus gehende Sicherheitsmechanismen; generiert durch die WiFi-Alliance
WISP	Wireless Internet Service Provider
XOR	logische Verknüpfung "exklusiv oder"