goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Wireless LAN

Der aktuelle INFONEWS befasst sich mit Thema „Wireless LAN“. Mit einem vertieften Einblick in den Aufbau und die Geschichte von WLAN zeigen wir Ihnen, wo und wieso Wireless LAN beim Thema Sicherheit anspruchvoll ist.

Falls Sie Anregungen oder Ideen aus Ihrem eigenen IT-Alltag haben, nehmen wir diese gerne auf. Wir freuen uns auf ein Feedback von Ihnen.

Dies ist eine kostenlose Dienstleistung der GO OUT Production GmbH (www.goSecurity.ch/INFONEWS).

Inhaltsverzeichnis

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Einsatzgebiete von Wireless LAN

LAN in der Ethernet-Technik haben mittlerweile einen hohen Reifegrad bei verhältnismässig niedrigen Kosten erreicht. Heute wollen wir nahezu beliebige Kommunikationsdienste jederzeit unabhängig von unserem augenblicklichen Aufenthaltsort nutzen.

Wenn wir die Anwendungsfälle etwas differenzierter betrachten, können wir einige Mobile Einsatzgebiete unterscheiden:

- **Mitarbeiter wollen/müssen Laptops an wechselnden Orten einsetzen**
  Schreibtisch, Beratungsraum, Labor, bei Kunden
- **Kontakt zu mobilen Mitarbeitern und mobiler Technik**
  Servicetechniker, Transportsysteme ... (hier eher PDAs)
- **Mobile Nutzer untereinander**
  Beratungen ... Ad-Hoc-Networking
- **Bei schwierigen Verkabelungsverhältnissen**
  Denkmalschutz, Asbestprobleme, Brandschutz ...
- **Kurzzeitige Nutzungsfälle**
  Projekte, Messestände .....
- **Backup für Festnetz**
  Überbrückung von Ausfällen und Bautätigkeit
- **Variable Zahl von temporären Zugängen**
  Schulungen, Ausstellungen ...
- **Öffentliche "Hot-Spots"**
  Flughäfen, Hotels, Gaststätten, Stadtzentren ...
- **Community Networks**
  zur Versorgung der "Nachbarschaft"

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

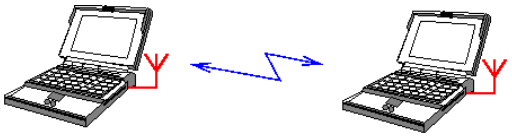
Telefon 052 320 91 20
Fax 052 320 91 21

2 Betriebsarten

Wireless LAN kann in drei unterschiedlichen Modi betrieben werden. Dabei handelt es sich um das P2P, BSS und ESS.

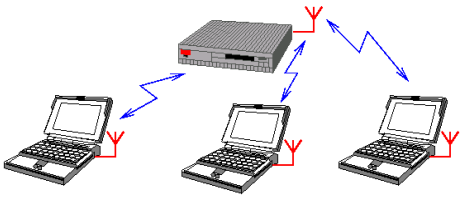
2.1.1 Peer-to-Peer (P2P)

Für Mobilstationen (MS) untereinander und wird auch "Independent Basic Service Set (IBSS)" oder auch "Ad-Hoc" genannt.



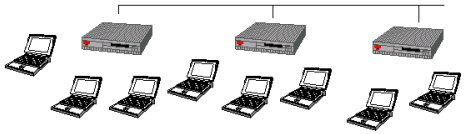
2.1.2 Basic Service Set (BSS)

Besteht aus mehreren Mobilen Geräten die mit einem Repeater, auch Access Point (AP) genannt, betrieben werden.



2.1.3 Extended Service Set (ESS)

Mehrere sich überlappende Basic Service Sets bilden ein Extended Service Set, innerhalb dessen sich der Anwender frei bewegen kann (Roaming).



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 Die Technik von Wireless LAN

Die folgenden Seiten behandeln vertieft die Technik von Wireless LAN. Mit diesem Wissen werden Sie anschliessend die einzelnen Gefahren besser verstehen können.

3.1 Kanalzugriff

Das Medium "Funk" ist in gewisser Hinsicht mit dem traditionellen Ethernet vergleichbar, bei dem mehrere Stationen um den Zugriff auf ein Medium (bzw. ein Frequenzband) konkurrieren. Bei Wireless LANs nach 802.11 werden folgende Verfahren zur Koordinierung des Medienzugriffs eingesetzt:

3.1.1 Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

Eine sendewillige Station prüft, ob das Medium (der Funkkanal) frei ist. Das vom Ethernet bekannte CSMA/CD ist nicht einsetzbar, weil eine Station während des Sendens kaum feststellen kann, ob eine weitere Station ebenfalls sendet.

3.1.2 Distributed Coordination Function (DCF)

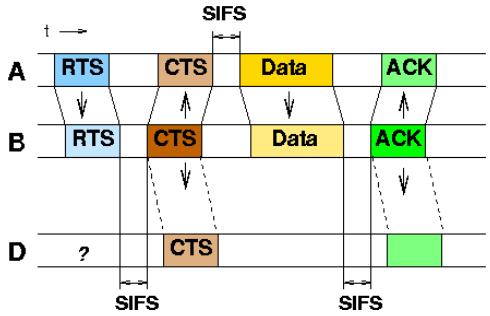
Eine absolute Vermeidung von Kollisionen ist nicht gegeben. Allerdings wird die Zeitspanne, in der Kollisionen vorkommen können, durch ein geschicktes Verfahren minimiert.

Wegen der endlichen Ausbreitungsgeschwindigkeit kann es natürlich trotzdem zu Kollisionen kommen, wenn zwei Stationen nahezu zum selben Zeitpunkt einen freien Kanal feststellen und zu senden beginnen. Kann durch ein ausbleibende Quittung (ACK) die Kollision erkannt werden. Eine Zufallskomponente bei der Zeit bis zum Wiederholversuch sorgt dafür, dass die beiden Stationen beim nächsten Mal (höchstwahrscheinlich) nicht wieder kollidieren.

Der eben beschriebene Mechanismus funktioniert allerdings nur dann korrekt, wenn alle Stationen alle anderen auch empfangen können. Mitunter wird das nicht gegeben sein, wenn zwischen bestimmten Stationen Hindernisse vorhanden sind. Wir bezeichnen dies als das Problem der hidden nodes.

Für diesen Fall gibt es den (optionalen) Mechanismus Request to send/Clear to send (RTS/CTS).

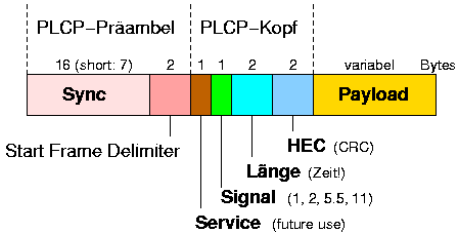
Den erreichten Effekt bezeichnet man als Virtual Carrier Sense. Eine Station D erfährt aus dem CTS von einer anderen Station zum Beispiel B, dass der Kanal durch A für eine gewisse Zeit belegt sein wird. (Siehe dazu die Grafik)



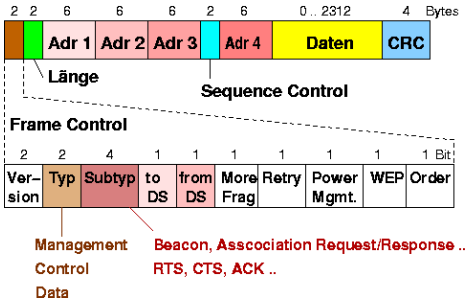
Optional ist eine Point Coordination Function (PCF), bei der die Zugriffskoordinierung durch den Access Point erfolgt.
Damit lassen sich beispielsweise definierte Teilbandbreiten vergeben (Stichwort "Multimedia" ...)

3.2 Rahmenstruktur

Hier sehen Sie die Rahmenstruktur des Physical Layer Convergence Protocol (PLCP):



192 Bits werden mit 1 Mbit/s übertragen, bei 802.11b ist eine kürzere Präambel zugelassen. In der Payload haben wir dann folgende Rahmenstruktur



Als Basic Service Set Identifier (BSSID) wird die MAC-Adresse des Wireless LAN -Interfaces des betreffenden AP verwendet.

Im Falle IBSS (Betrieb ohne AP) wird als BSSID eine 48-Bit-Zufallszahl verwendet. Die Stationen eines IBSS-Netzes erfahren diesen Wert, weil er von einem (dynamisch gewählten) Mitglied des Netzes zyklisch als Bakensendung (Beacon) verbreitet wird. Es gibt weiterhin eine für Broadcasts reservierte BSSID (alles 1-Bits).

3.3 Der Standard IEEE 802.11

Erste drahtlose lokale Netze gibt es seit etwa 1992. Bei den frühen Produkten musste man sich mit Bandbreiten deutlich unter 1 Mbit/s begnügen. Noch unangenehmer war die fehlende Standardisierung, nur Produkte eines Typs von einem (vielleicht kurzlebigen) Hersteller waren untereinander interoperabel.

Diese Situation verbesserte sich entscheidend mit der Verabschiedung des 802.11-Standards, der danach noch verschiedene Erweiterungen erfahren hat:

- 1997: IEEE 802.11
  1/2 Mbit/s
- 1999: IEEE 802.11b
  11 Mbit/s

Frequenzbereich:

- 2.4 - 2.4835 GHz
- Industrial, Scientific, and Medical (ISM)
- lizenzfreie Nutzung mit niedrigen Leistungen
- max 100 mW, praktisch 10 .. 30 mW

Übertragungsverfahren bei 802.11:

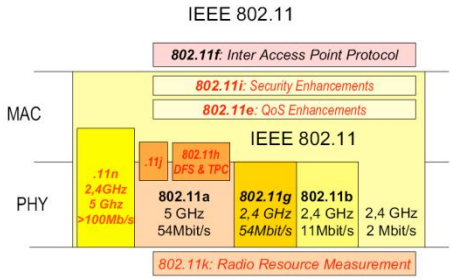
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
  (bei 802.11b wird nur noch DSSS verwendet)

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Mit 802.11a und b ist noch nicht das Ende der Entwicklung erreicht, vielmehr gibt es eine ganze Reihe weiterer Standards, die hier nur kurz genannt werden:

- HIPERLAN/2: bis 54 Mbit/s, 5,15-5,35 GHz
- Higher Performance Radio LAN (HIPERLAN), ETSI
- 802.11g: 22 ... 54 Mbit/s, 2,4 GHz, 30-50m (OFDM, aber verträglich zu 802.11b)
- 802.11e: MAC Enhancements (QoS ...)
- 802.11f: Inter-Access Point Protocols
- 802.11i: Security Enhancements
- 802.16: Wireless MAN, fixed Broadband Wireless Access (BWA), 2 ... 66 GHz



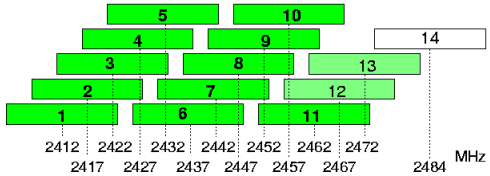
Da bei Wireless LANs mittlerweile DSSS-Verfahren die Hauptrolle spielen, werden wir uns diese nachfolgend näher ansehen.

3.3.1 Kanalaufteilung

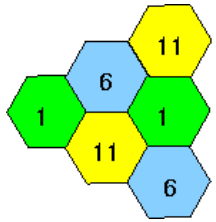
Oft werden mehrere Wireless LANs bzw. mehrere Zellen eines Wireless LAN mit überlappenden Funkbereichen betrieben. Hier ist es vorteilhaft, unterschiedliche Frequenzbereiche zu benutzen, um die gegenseitigen Beeinflussungen zu minimieren. Eine Separierung auf der logischen Ebene ("Netzname") ist zwar auch möglich, allerdings ohne eine Vervielfachung der Bandbreite.

Die Kanalaufteilung für DSSS hat folgende Merkmale:

- Kanalbreite je 22 MHz
- Kanäle sind überlappend!
- Europa (ETSI): 1 - 13
- U.S., Kanada: 1 - 11
- Japan: 14



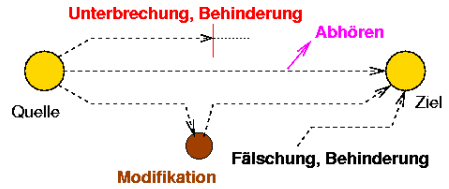
Es existieren also nur drei nichtüberlappende Kanäle. Im Idealfall wird man z.B. nur die Kanäle 1, 6 und 11 vergeben. Die Nachfolgende Grafik zeigt eine mögliche Einteilung der Funkzellen.



Praktische Funkzellen sind natürlich (leider) nicht wabenförmig, auch halten sich die Funkwellen nicht an eine exakte Grenze.

4 Mögliche Gefahren und Lösungsansätze

Mit welchen Problemen müssen wir beim Einsatz von Wireless LAN rechnen?

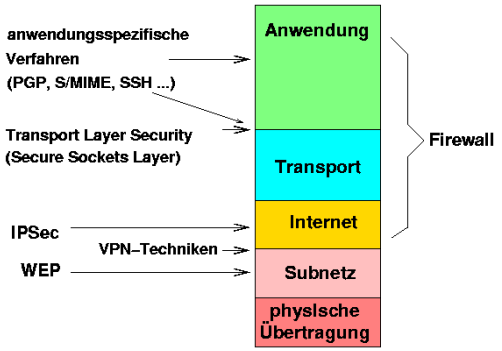


Wir sehen hier dieselben Gefährdungsklassen, die wir schon von drahtgebundenen Netzen kennen. Wie dort ist Sicherheit auch relativ und muss immer eine angemessene Wertigkeit gegenüber den oft konkurrierenden Merkmalen wie Nutzerfreundlichkeit oder Performanz erhalten.

Bei den Vorkehrungen zur Wireless LAN -Sicherheit werden wir diese Teilaspekte unterscheiden:

- Authentifizierung und Autorisierung
- Integrität
- Vertraulichkeit

Vorkehrungen zur Sicherheit können in ganz verschiedenen Schichten angeordnet werden. Damit wird klar, dass hier keineswegs nur Wireless LAN -spezifische Techniken eine Rolle spielen. Einige der Techniken sind alternativ, aber auch Kombinationen sind oft sinnvoll.



4.1 WEP

Funknetze sind offensichtlich leichter abzuhören oder zu beeinflussen als drahtgebundene Netze oder gar Lichtwellenleiter. In Anerkennung dieser Tatsache wurde als Bestandteil von 802.11 eine Technologie unter der Bezeichung Wired Equivalent Privacy (WEP) entwickelt.

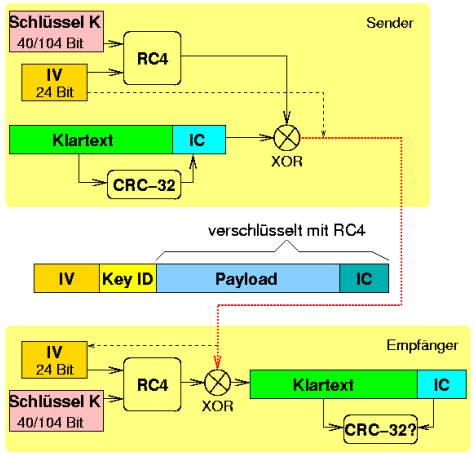
Diese soll ein Abhören der Funkübertragung verhindern oder zumindest erschweren. Ein sekundäres Ziel war die Realisierung einer Zugriffskontrolle auf das Wireless LAN. WEP soll etwa das Sicherheitsniveau eines Kabel-Ethernet erreichen.

Die Realisierung hat mehrere Elemente:

- Verschlüsselung mit Stream Cipher RC4
  den Partnern ist ein geheimer Schlüssel bekannt
- Integrity Check (IC) CRC-32 zur Integritätsprüfung
- 24 Bit Initialization Vector (IV)

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



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. (Siehe Anhang)

4.1.1 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

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

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 wieder verwendet, 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.

- 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.

- 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 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.

4.2 WPA

WPA ist ein Ausschnitt aus der gegenwärtigen Version 802.11i, welches Temporal Key Integrity Protocol (TKIP) und 802.1x einschliesst. Die Kombination dieser beiden Verfahren liefert dynamische Schlüsselverwaltung und gegenseitige Authentifizierung. Dinge, die in Wireless LAN dringend benötigt werden.

Wie mit WEP verwendet TKIP RC4 (RSA) um den Frame Body und jedes CRC eines 802.11 Frames vor der Über-

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

tragung verschlüsselt. Die Schwachstellen von WEP haben wenig mit dem RC4 Algorithmus alleine zu tun. Die Probleme liegen vielmehr bei der Schlüsselgenerierung und der Art der Verschlüsselung.

TKIP fügt folgende Stärken zu WEP hinzu.

- **48-Bit Initialisierungsvektor**. WEP generiert mit dem privaten Schlüssel und einem 24 Bit Initialvektor einen Schlüsselstrom, welcher gleich der Länge der 802.11 Frames ist. So kann es in stark frequentierten Netzen sein, dass sich die Pakete schon nach einer Stunde wiederholen. WPA mit TKIP verwendet daher einen Initialisierungsvektor von 48 Bit. So gelangt ein potentieller Hacker nicht an genug Packet, um den Strom zu entschlüsseln.

- **Paketweiser Aufbau und Verteilung**. WAP erzeugt automatisch und regelmässig einen neuen eindeutigen Schlüssel. So verwendet WPA einen einmaligen Schlüssel für jeden 802.11 Rahmen. So ist es praktisch unmöglich, den Schlüssel zu knacken.

- **Message Integrity Code**. Mit WPA wurde der Message Integrity Code (MIC) eingeführt. WEP führt eine 4-Byte Überprüfung durch (ICV). Der Empfänger berechnet ebenfalls ICV und vergleicht, ob die Pakete identisch sind. Obwohl WEP diese Pakete verschlüsselt, kann ein Hacker die Angaben verändern und ein aktualisiertes ICV einfügen. WPA löst dieses Problem durch einen 8-Byte langen MIC.

Für die Authentifizierung verwendet WPA eine Kombination aus offenem System und 802.1x Authentifizierung. Zuerst autorisiert sich der Client am Access Point. Anschliessend kann der Access Point eine Überprüfung mit RADIUS oder LDAP durchführen. Ebenfalls ist es möglich, WPA mit pre-shared keys zu betreiben. Dies macht vor allem bei Heimanwendern oder kleinen Firmen Sinn.

4.3 Authentifizierungsmechanismen

Eine Authentifizierung der Wireless LAN -Nutzer brauchen wir aus mehreren Gründen:

- nur festgelegte Nutzer/Nutzerklassen zulassen
- Ressourcenbegrenzung (Bandbreiten/Datenmengen)
- Abrechnung (Accounting)

Zur Identifikation eines Nutzers gibt es eine ganze Reihe unterschiedlicher Ansätze. Einige sind eher für kleine, selten wechselnde Nutzermengen geeignet; für grosse Nutzermengen sind nicht alle Verfahren praktikabel.

- **Kenntnis des Network Name, SSID, Extended Service Set IDentifier (ESSID)**
  Der Nutzer weist hier nur nach, dass er einen Netzidentifikator kennt. Wenn dies als "Netzpasswort" gehandhabt werden soll, ergeben sich dieselben logistischen Hürden wie bei der Verteilung geheimer WEP-Schlüssel.
  Ein offenes Netz akzeptiert Mobilstationen ohne Netzidentifikator. Für die Einschränkung auf Mobilstationen, die den SSID kennen, findet man mitunter die Bezeichnung "Closed Network" (das ist wohl etwas irreführend).

- **MAC-Adresse - 48 Bit**
  Hier wird im Grunde die Wireless LAN -Karte als "Authentifizierungstoken" verwendet, was sich

ganz gut mit der mancherorts praktizierten Ausleihe von Wireless LAN -Karten organisieren lässt.

Nachteilig ist der Organisationsaufwand für "fremde" Wireless LAN -Karten. Ausserdem ist eine MAC-Adresse kein Geheimnis, sie lässt sich leicht ermitteln. Weniger bekannt ist die Tatsache, dass sich in vielen Fällen auch beliebige MAC-Adressen einstellen lassen.

- **WEP-Authentifizierung - shared secret key**

- **VPN-Authentifizierung (PPTP, L2TP, IPSec ..)**
  Viele VPN-Technologien enthalten Vorkehrungen zur Authentifizierung gegenüber dem anderen Tunnelende, so etwas ist natürlich nutzbar.
  Hier greifen die Eigenschaften (aber auch potentiellen Schwachstellen) der verwendeten VPN-Technologie

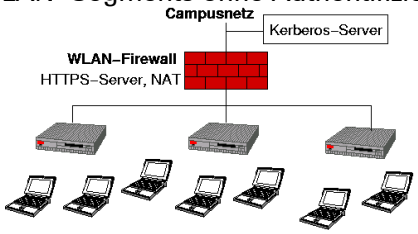
  IPSec
  Bei den ersten Standardentwürfen zu IPSec hatte man übrigens ähnliche Fehler gemacht wie bei WEP. Mittlerweile kann IPSec aber als einigermassen solide gelten lassen. Als Nachteil bleibt die meist nicht triviale und schwer auf Korrektheit zu prüfende Konfigurierung (vor allem in Endsystemen).

  Point-to-Point Tunneling Protocol (PPTP)
  Diese Variante ist im Windows-Umfeld recht verbreitet. Es gibt allerdings auch hier eine Reihe signifikanter und gern ausgenutzter Schwachstellen.

  Layer 2 Tunneling Protocol (L2TP)
  Hinter dieser Variante stehen IETF und grosse Routerhersteller.

- **End-zu-End-Verschlüsselung und -Authentifizierung**
  Nutzername/Passwort via HTTPS
  Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH)

  Die Nutzer müssen sich über eine Anwendung authentifizieren. Die Authentifizierungsinformationen (z.B. Nutzername und Passwort) müssen hinreichend sicher übertragen werden, was beispielsweise mit HTTP über SSL/TLS gegeben ist.
  Diese Lösung ist recht einfach durch Nutzer und Management zu handhaben. In Kauf zu nehmen sind die begrenzte Sicherheit der zeitlichen Kontinuität sowie die potentielle Nutzung des Wireless LAN -Segments ohne Authentifizierung.

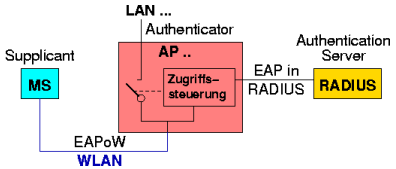


- **Port-based access control - IEEE802.1x**
  Das ist eine neue Entwicklung zur Authentifizierung von Netzzugängen. Im Fokus befinden sich nicht nur Wireless LAN -Zugänge, sondern z.B. auch Ethernet-Dosen mit mehr oder weniger öffentlichem Zugang.
  Diese Technik ist Teil der neuen IEEE-Sicherheitsarchitektur Robust Security Network

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

(RSN). Es wird das Extensible Authentication Protocol (EAP) verwendet, hier konkret EAP over Wireless (EAPoW).



Da EAP ursprünglich für drahtgebundene Netze vorgesehen war, fehlten spezielle Vorkehrungen zum kryptografischen Schutz der Authentifizierungsinformationen. Weiterhin hat sich der Authenticator nicht selbst ausgewiesen, so dass man mit einem "illegalen" AP/Authenticator die Authentifizierungsinformationen "einsammeln" kann.
Beide Probeme löst die Entwicklung EAP/TLS, wo mit Transport Layer Security (TLS) eine bewährte Technik zur Herstellung eines sicheren Kanals verwendet wird (bekannt von https ...).

Einige der Verfahren sind kombinierbar, was Schwachstellen kaschieren kann.
Problematisch ist oft die Erkennung der Kontinuität bzw. des Nutzungsendes für einen autorisierten Nutzer.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

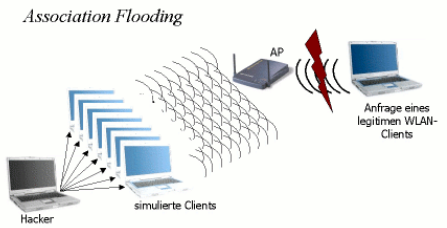
4.4 DoS-Angriffe auf WLANs

Die brutale Methode, ein Funknetz lahm zu legen, ist ein Störsender, der im Frequenzbereich sendet, den die WLAN-Standards definieren (2.4 GHz für 802.11b/g oder 5 GHz für 802.11a/h). Doch in Foren und Mailinglisten werden auch systematische Angriffe gegen Funknetze diskutiert, die sich Eigenheiten der WLAN-Protokolle zu Nutze machen und sich via Software ausführen lassen.

4.4.1 Association Flooding

Die gängigen Angriffsmethoden beruhen auf dem Fluten des Funknetzes mit speziellen Paketen, die das An- oder Abmelden von Systemen an der Basisstation vortäuschen. Da die Verwaltungsinformationen dabei auch bei eingeschalteter WEP-Verschlüsslung unverschlüsselt übertragen werden, kann ein Angreifer diese Pakete ohne großen Aufwand fälschen.

Der Anmeldevorgang besteht aus zwei Schritten: der Authentifizierung und dem Assoziieren. Zum Abmelden eines Clients vom Netz genügt ein einziges De-Authentication Paket. Heise Security hat die Anfälligkeit verschiedener Basisstationen gegen Angriffe mit Association, Authentication und De-Authentication Flooding untersucht.

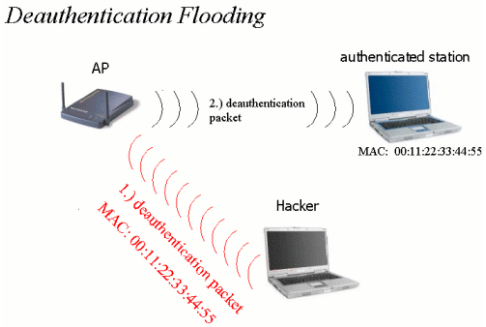


Association Flooding simuliert den parallelen Zugriff mehrerer WLAN-Clients. Vor allem ältere Access Points können nur circa 255 parallele Association-Anfragen von WLAN-Clients parallel bearbeiten. Dabei erhält jeder WLAN-Client eine eigene ID (AID). Aufgrund der gefälschten Anfragen stehen dem Access Point keine freien AIDs für legitime Clients mehr zur Verfügung; diese können keine Verbindung mehr aufbauen.

Die Authentication-Flooding-Attacke ähnelt dem Association Flooding, es wird jedoch eine große Anzahl von Authentication Frames gesendet, über die sich Clients beim Access Point anmelden. Einige Access Points verweigern daraufhin komplett ihren Dienst da sie nur eine begrenzte Anzahl von Anfragen pro Zeiteinheit bearbeiten können. Sie sind dann oft erst nach einer bis zu 15-minütigen Erholungsphase wieder erreichbar.

4.4.2 Deauthentication Flooding

Beim Deauthentication Flooding schickt der Angreifer einem Access Point ein Deauthentication-Paket mit der MAC-Adresse eines bereits authentifizierten WLAN-Clients. Daraufhin beendet der Access Point die Verbindung zum authentifizierten WLAN-Client, indem er ihm ebenfalls ein derartiges Paket sendet. Alternativ kann der Angreifer die gefälschten Pakete auch an den Client schicken -- dann eben mit der Abenderadresse der Basisstation. Und schließlich kann er mit gefälschten Broadcasts des Access Points sogar alle Clients im WLAN auf einmal abmelden.



Auch diese Attacke ist bei WLANs mit aktivierter WEP-Verschlüsselung möglich, da diese nicht zur Verifizierung von Deauthentication Management Frames herangezogen wird. Der Angreifer benötigt lediglich die SSID des WLAN, die BSSID des Access Point und die MAC-Adresse des vorgetäuschten Absenders. Diese Daten lassen sich jedoch mit herkömmlichen Sniffer-Tools einfach ermitteln, da sie auch bei aktivierter WEP-Verschlüsselung im Klartext übermittelt werden.

In einschlägigen Mailinglisten werden darüber hinaus bereits weitere DoS-Attacken diskutiert, die zum Beispiel verschiedene Management Frames des Extensible Authentification Protocol (RCF 2284, Bestandteil von WPA) missbrauchen. Demnächst ist also auch mit Angriffen via EAPoL ID-Flood, EAPoL Logoff-Flood und EAPoL Start-Flood zu rechnen.

4.5 Zum Angriff

Die drei Angriffe gegen herkömmliche WLANs lassen sich mit dem im Internet verfügbaren Tool void11 durchführen, das auf dem Host-AP-Treiber für Linux aufsetzt. In einem Test untersuchte heise Security das Verhalten aktueller 802.11b/g-Access Points der Hersteller USR, Belkin, Trust, Intel, 3COM, Lancom, T-Sinus und Apple.

Dabei stellte sich heraus, dass aktuelle Systeme gegen Association und Authentication Flooding weit gehend imun sind. Negativ fiel lediglich die Apple Basisstation AirPort Extreme auf. Sie war direkt nach Beginn der Attacken nicht mehr erreichbar.

Das Deauthentication Flooding funktionierte hingegen mit allen Basisstationen und Clients, da die momentan verwendeten IEEE-802.11-Standards keine Absicherungsmethoden vorsehen, die eine sichere Verifizierung der erhaltenen Meldungen ermöglichten. Wir konnten sowohl einzelne Clients gezielt abmelden oder durch Broadcasts alle Verbindungen kappen.So konnte ein einfaches Notebook mit WLAN-Karte beliebige Funknetze innerhalb der eigenen Reichweite außer Betrieb setzen.

Theoretisch lassen sich solche Angriffe durchaus auch automatisieren. Laut IDC werden 2004 etwa 50 Millionen Notebooks mit fest eingebauten WLAN-Chips verkauft. Sie stellen damit schon ein lohnendes Ziel für einen Wurm mit WLAN-Störfunktion dar. Bei nennenswerter Verbreitung könnte ein solcher WLAN-Störwurm gerade in Gebieten mit hoher Funknetzdichte beträchtlichen Schaden anrichten. Unabhängig von solch spekulativen Würmern zeigen unsere Tests: Garantierte Verfügbarkeit und WLAN schließen sich aus; wo es darauf ankommt, dass die Netzinfrastruktur auch tatsächlich verfügbar ist, sollte man eine Abhängigkeit von WLAN vermeiden.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 Anhang

5.1.1 Tools

Wireless Sniffers
http://www.personaltelco.net/index.cgi/WirelessSniffers

AirSnort
http://airsnort.shmoo.com/

Kismet
http://www.kismetwireless.net

"802.11b wireless network sniffer"
http://wellenreiter.sourceforge.net

Mognet
http://chocobospore.org/projects/mognet/

Netstumbler
http://www.netstumbler.com

5.1.2 Quellen

Uwe Hübner, Technische Universität Chemnitz
Maximilian Riegel, KNF Kongress
Jim Geier, Wireless-Nets, Ltd.
Roland Lenz, 2cool4u
Alain Girardet, Dominik Blunk, Zürcher Hochschule Winterthur
Heise Security
BSI, Bundesamt für Sicherheit in der Informationstechnik