Fachbereich 4: Informatik

Grundlagen und Einrichtung eines sicheren W-LANs

Studienarbeit
im Studiengang Informatik

vorgelegt von
Norman Budack

Betreuer:
Prof. Dr. Rüdiger Grimm
Institut für Wirtschafts- und Verwaltungsinformatik FB4

Anastasia Meletiadou
Institut für Wirtschafts- und Verwaltungsinformatik FB4

Koblenz, im März 2007

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Zusammenfassung

In dieser Arbeit geht es darum, einen Einblick in das Thema Wireless LAN zu vermitteln. Es werden zunächst einmal die gängigsten Standards und weitere wichtige Aspekte aus diesem Bereich vorgestellt. Das Hauptaugenmerk dieser Arbeit liegt jedoch darauf, wie die Kommunikation in Funknetzwerken sicherer gestaltet werden kann. Im Zuge dessen werden einige Mechanismen vorgestellt, mit denen es möglich ist, die Kommunikation zu verschlüsseln oder nur bestimmte Teilnehmer an der Kommunikation teilnehmen zu lassen. Mit diesen Mechanismen ist es dann möglich eine hohes Maß an Sicherheit in Funknetzwerken zu erreichen. Abschließend wird in einem Tutorial beschrieben, wie die zuvor vorgestellten Mechanismen eingerichtet und angewendet werden können.

2 Einleitung

2.1 Motivation

Seit es Netzwerke gibt, muss man sich Gedanken darüber machen wie Daten vor unerlaubtem Zugriff oder Missbrauch geschützt werden können. Bei kabelgebundenen LANs (Local Area Network), welche in aller Regel nicht öffentlich zugänglich sind, ist dieses Problem relativ klein, da ein Angreifer nur schwer Zugang zu dem verwendeten Medium (in diesem Falle ein Kabel) erlangen kann. Dieses ist jedoch notwendig um Daten abfangen und auswerten zu können. Bei öffentlich genutzten Netzwerken wie etwa dem Internet sieht die Sache schon etwas anders aus, da sich jeder Angreifer sehr einfach Zugang zum verwendeten Medium und damit dem Netzwerk verschaffen kann. Dieses Problem ist jedoch nicht Thema dieser Arbeit und wird somit nicht weiter behandelt.
Bei Funknetzwerken ist das Problem Datenschutz jedoch ein sehr großes, da alle Daten, egal für wen sie bestimmt sind, über den kompletten Empfangsbereich ausgesendet werden und somit in diesem Bereich von jedermann empfangen werden können. Da seit der Einführung von Funknetzwerken, die Preise für benötigte Hardware sehr stark gesunken sind, haben sich Funknetzwerke immer weiter verbreitet und sie in immer mehr Bereichen Einklang gefunden haben. Heute ist die benötigte Hardware so günstig und trotzdem leistungsfähig geworden, sodass in sehr viel privaten Haushalten und kleinen Unternehmen die ein Netzwerk besitzen, dieses entweder komplett oder zumindest in Teilen aus einen Funknetzwerk besteht. Die Tatsache das heute nahezu jedes neue Notebook über eine integrierte Funknetzwerkkarte verfügt und die Absatzzahlen von Notebooks stetig wachsen, führt ebenso dazu, dass sowohl Privatleute als auch kleine Unternehmen immer mehr auf Funknetzwerke setzen. Somit werden auch immer mehr sicherheitsrelevante Daten wie Passwörter, Bankverbindungen, und so weiter über drahtlos Netzwerke transportiert. Alle diese Aspekte führen dazu, dass sich die Industrie sehr viele Gedanken über Privatsphäre in Funknetzwerken gemacht hat. Welche Verfahren und Standards dabei entstanden sind, welche Vor- Nachteile sie bieten und wie sie angewendet werden, wird in dieser Arbeit dargestellt.

2.2 Was ist ein Wireless-LAN

Ein Wireless LAN ist ein drahtloses Netzwerk, welches eine Verbindung von zwei oder mehr Endgeräten wie z.B. Computer, PDA oder Notebook, innerhalb eines bestimmten Areals darstellt. Ähnlich wie ein kabelgebundenes Netzwerk (beispielsweise Ethernet) dient es der Kommunikation zwischen mehreren, möglicherweise unterschiedlichen, Endgeräten. Bei kabelgebundenen Netzwerken, wird wie der Name schon sagt, ein Kabel als Übertragungsmedium genutzt. Bei einem Funknetzwerk hingegen gibt es kein Kabel, sondern die Luft dient als Übertragungsmedium und die Daten werden mittels Funkwellen übertragen. Bei einem kabelgebundenen Netzwerk ist die Reichweite des Netzwerkes dadurch begrenzt, wie lang die jeweiligen Kabel sind. Bei einem Funknetzwerk hingegen hängt die Reichweite von vielen Faktoren ab. Zum einen spielt die Umgebung eine große Rolle. In Gebäuden ist die Reichweite sehr viel geringer als im Freien. Weiter hängt die Reichweite von den verwendeten Netzwerkkomponenten und deren Sende-/Empfangsleistung ab. In nahe zu allen Ländern existieren gesetzliche Regelungen was die Maximale Sende-/Empfangsleistung von Funknetzwerkkomponenten betrifft. Da die Hersteller jedoch in der Lage sind deutlich stärkere Antennen zu produzieren, ist eine derartige Regelung zwingend notwendig damit ein Funknetzwerk nicht zu einem gesundheitsgefährdenden Instrument wird[Rec04]. Als letztes Kriterium muss man den Betriebsmodus betrachten, denn IEEE 802.11 Funknetzwerke, welche die für diese Arbeit relevaten Netzwerke sind, bieten ähnlich wie bei kabelgebundenen Netzwerken die Möglichkeiten eine direkte Verbindung zwischen zwei oder mehr Endgeräten herzustellen, dieser Modus wird Ad-Hoc-Mode genannt. In der Praxis hat sich gezeigt das der Ad-Hoc-Mode nur sehr selten genutzt wird. Haupteinsatzgebiet für Ad-Hoc Netzwerke ist der spontane Austausch von Daten zwischen mehreren Endgeräten.[Rad04] Ein Grund für die geringe Verbreitung von Ad-Hoc Netzwerken ist das Fehlen eines Verwaltungsorgans und somit die fehlende Unterstützung von nahezu allen bekannten Sicherheitsmechanismen. Zudem kann die Reichweite eines Ad-Hoc Netzwerkes nur über die Sende-/Empfangsleistung der verwendeten Geräte beeinflusst werden.
Der zweite Betriebsmodus wird Infrastructure-Mode genannt. In ihm werden Verbindungen von Endgeräten über einen Access Point abgewickelt. Dieser Access Point übernimmt die Funktion eines Hubs oder Switches in einem Kabelnetzwerk. Ein Access Point dient letztendlich als Verwaltungsorgan des Netzwerkes. Da sich alle Clients bei ihm anmelden müssen ist ein Access Point in der Lage Sicherungsmechanismen zur Verfügung zu stellen. Manche Access Points sind nicht nur in der Lage die Kommunikation zwischen mehreren Teilnehmern des Drahtlosnetzwerkes zu steuern, sondern sie bilden auch eine Brücke zwischen drahtlosem Netzwerk und einem kabelgebundenen Netzwerk. Solche Access Points können unter anderem auch eine Brücke zwischen Drahtlosnetzwerk und Internet herstellen[Rec04]. Das bedeutet, jeder authentifizierte Client im Drahtlosnetzwerk hat Zugriff auf das Internet. Damit die Reichweite eines Funknetzes unabhängig von der Sende-/Empfangsleistung der verwendeten Geräte erweitert werden kann, bietet der Infrastructure-Mode noch die Möglichkeit mehrere Access Points zu verwenden. Jeder Access Point versorgt dabei ein gewisses Areal und bildet dabei eine Funkzelle. Wenn mehrere Funk-

zellen eines Netzwerkes so angelegt werden, dass ihre Grenzen sich überschneiden, so kann sich ein Client frei zwischen allen Zellen hin und her bewegen ohne dabei die Verbindung zum Netzwerk zu verlieren. Die Verbindung der einzelnen Access Points untereinander kann in diesem Falle entweder ebenfalls drahtlos erfolgen oder sie können auch über ein Kabelnetzwerk mit einander verbunden werden[BSI05].

3 Grundlagen

3.1 Vor- und Nachteile von Funknetzwerken im Vergleich zu kabelgebundenen Netzwerken

Funknetzwerke bieten einige Vorteile gegenüber kabelgebundenen Varianten. Leider bringen sie jedoch auch den einen oder anderen Nachteil mit sich. Welche Vor- und Nachteile das sind, wird in diesem Kapitel kurz erläutert.Als die wichtigsten Vorteile müssen folgende Aspekte genannt werden.
Zunächst ist der Aufbau eines Funknetzwerkes, gerade für kleine Unternehmen, teils deutlich günstiger als der Aufbau eines Kabelnetzwerkes. Bei drahtlosen Netzwerken müssen nur Netzwerkkarten und Access Points gekauft und aufgestellt werden. Wenn man jedoch ein kabelgebundenes Netzwerk aufbauen will, müssen neben den eben erwähnten Netzwerkkomponenten noch Kabel gekauft und vor allem verlegt werden. Die Kosten für eine solche Kabelverlegung können teilweise sehr immens sein. Wenn etwa ein Netzwerk in einem Altbau aufgebaut werden soll und dieser vielleicht sogar unter Denkmalschutz steht, müssen sehr viele Vorschriften und Auflagen bezüglich Brandschutz, Denkmalschutz beachtet werden. Dies treibt die Kosten für ein Netzwerk recht schnell in ungeahnte Bereiche. Ebenso können mit drahtlosen Verbindungen sehr leicht und kostengünstig mehrere Gebäude miteinander verbunden werden [Rec04].
Ein weiterer sehr großer Vorteil ist der sehr leichte Aufbau eines Netzwerkes oder die Erweiterung eines bereits bestehenden Netzwerkes. Zum Aufbau oder der Erweiterung müssen mehr oder weniger nur Access Points aufgestellt werden und dann entsprechend konfiguriert werden und schon ist es autorisierten Personen möglich das Netzwerk zu verwenden. Bei Konferenzen, Seminaren oder beliebigen anderen spontan zeitlich befristeten Treffen bieten Drahtlosnetzwerke, in Verbindung mit Notebooks oder PDAs (Personal Digital Assistant), den Teilnehmer sehr einfach die Möglichkeit Daten untereinander auszutauschen, oder auf das Internet beziehungsweise ihre E-Mails zuzugreifen. Dies bedeutet deutlich gesteigerten Komfort und vielleicht sogar eine bessere Arbeitseffizienz[Rec04]. Ein weiterer Vorteil von drahtlosen Netzwerken ist der sehr einfache Aufbau von sogenannten Hotspots. Hotspots sind Areale in denen ein Anbieter ein öffentliches Drahtlosnetzwerk für jedermann zur Verfügung stellt, somit können Personen, die sich in diesem Areal befinden und über ein Notebook, oder ein anderes W-Lan fähiges Endgerät verfügen, dieses Netzwerk nutzen und darüber Zugang zum Internet erlangen. Diese Hotspots können je nach Betreiber von jedermann kostenlos oder gegen Gebühr verwendet werden. Möglich ist auch, dass der Betreiber nur bestimmen Benutzern den Zugang zu seinem Hotspot erlaubt. Heutzutage sind Hotspots noch nicht flächendeckend verfügbar, jedoch sind sie in immer mehr Flughäfen, Bahnhöfen, Restaurants, Parks, Hotels, Universitäten und diversen öffentlichen Plätzen zu finden
[Rec04] [Rad04].
Gegenüber den vielen Vorteilen haben Funknetzwerke im Wesentlichen zwei große Nachteile gegenüber Kabelnetzwerken.
Erstens können sie von der reinen Performance, jedenfalls bis heute, nicht

mit Kabelnetzwerken mithalten. Die verschiedenen offiziellen Standards von Funknetzwerken bieten heutzutage maximale Bruttoübertragungsraten von 11-54Mbps. Da der Overhead bei Funknetzwerken jedoch sehr groß ist, liegt die Nettoübertragungsrate deutlich niedriger und es werden reale Übertragungsraten von maximal 6-24Mbps erreicht[Rec04]. Im Vergleich dazu bieten Kabelnetzwerke deutlich mehr. Der sehr weit verbreitete Fast-Ethernet Standard bietet bis zu 100Mbps Bruttoübertragungsrate. Die aktuelle Entwicklung geht jedoch von Fast-Ethernet weg hin zu Gigabit-Ethernet, welches sogar bis zu 1Gbps Übertragungsrate zur Verfügung stellt. Da in kabelgebundenen Netzwerken die Overheads relativ klein sind, unterscheidet sich die Nettoübertragungsrate hier sehr viel weniger von der Bruttoübertragungsrate als bei Drahtlosnetzwerke.[Rec04].
Als zweiten Nachteil von Drahtlosnetzwerken muss die Sicherheit der Datenübertragung genannt werden. Bei Kabelnetzwerken ist das verwendete Medium physikalisch begrenzt und somit das Netzwerk vor Angriffen relativ gut geschützt. Wenn ein Angreifen Daten abfangen will, muss er sich zunächst Zugang zum Übertragungsmedium, in diesem Fall einem Netzwerkkabel, verschaffen. Da Kabel sehr oft in Wänden oder Decken verlegt sind, sind sie ziemlich gut gegen solche Attacken geschützt. Bei Drahtlosnetzwerken sieht dies leider ganz anders aus. Denn hier kommt die Luft als Medium zum Einsatz und da diese für jedermann frei zugänglich ist und alle Daten im kompletten Empfangsbereich ausgestrahlt werden, kann ein Angreifer sehr einfach Daten abfangen.[Rec04] Damit die Privatsphäre der Netzwerknutzer jedoch weiter gewahrt bleibt, hat sich die Industrie einige Sicherheitsmechanismen ausgedacht. Welche das sind, wird ausführlich in den Kapiteln 4 und 5 vorgestellt.

Zusammenfassend kann man sagen, dass Funknetzwerke sehr viel Komfort und Flexibilität bieten. Sie sind sehr schnell einsetzbar und erweiterbar und können an nahe zu jedem Ort flexibel eingesetzt werden. Gleichzeitig bieten sie fast alle Leistungsmerkmale eines Kabelnetzwerkes, kosten aber in der Anschaffung und dem Aufbau teils deutlich weniger. Gegen die Verwendung eines Funknetzwerkes sprechen nur die niedrigere Performance und die geringere Sicherheit.

3.2 OSI-Referenzmodell

Das OSI-Referenzmodell (Open System Interconnection Refference Model) wurde Ende der siebziger Jahre des letzten Jahrhunderts von der International Organization for Standardization (ISO) entwickelt um die Verbindung und den Datenaustausch zwischen Endgeräten in einem offenen Netzwerk zu regeln und zu standardisieren. Es handelt sich dabei um ein abstraktes Schichten basiertes Modell welches keine genauen Vorgaben macht, sondern nur die Ideen liefert. Seit seiner Einführung wird es immer wieder herangezogen um das Design eines Netzwerkprotokolls zu entwickeln und zu verstehen. Das OSI-Modell ist aus 7 übereinander angeordneten Schichten aufgebaut (siehe Abbildung 1). Jede Schicht ist dabei für einen bestimmten Teil der Kommunikation zuständig. Es beginnt bei physikalischen Parametern wie Kabelspezifikationen und endet bei der Bereitstellung von unterschiedlichsten Diensten wie beispielsweise

E-Mail oder Internet. Alle Schichten bis auf die ganz oben liegende Anwendungsschicht, liefern der nächst höheren Schicht Informationen, die diese zum Abarbeiten ihrer Aufgaben benötigt. Alle Schichten im OSI-Referenzmodell sind so gewählt und aufgebaut, dass folgende Kriterien erfüllt sind: (in Anlehnung an [Rad04])

- möglichst wenige Schichten
- Schichten sind so definiert, dass möglichst wenig Informationen zwischen den Schichten ausgetauscht werden müssen
- die Aufgabe einer jeden Schicht ist durch ihr Protokoll klar definiert
- innerhalb einer Schicht herrscht Homogenität
- zwischen zwei Schichten herrscht Heterogenität
- eine neue Schicht beschreibt den Wechsel in ein neues Abstraktionsniveau im Bezug auf Syntax, Semantik oder Datenbehandlung
- jede Schicht sollte nur die nächst höhere bzw. nächst niedrigere Stufe beeinflussen
- jede Schicht benutzt nur Dienste und Informationen der nächst niedrigeren Schicht

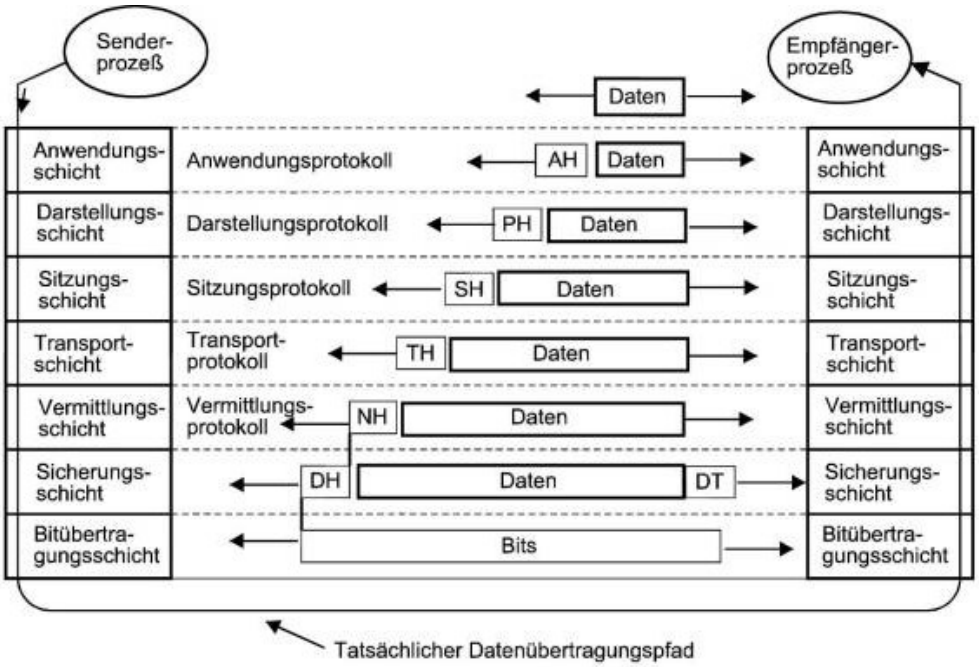

Abbildung 1: OSI Schichtenmodell [OSI1]

Der Vorteil des OSI-Modells oder jedes anderen Schichten Modells liegt darin, dass es für eine Schicht keine Rolle spielt, wie alle anderen Schichten realisiert sind, sondern für jede Schicht nur die ihr übergebenen Daten

entscheidend sind. Diese Tatsache macht es sehr einfach die Kommunikationsprotokolle eines kabelgebundenen Netzwerkes auf ein drahtloses Netzwerk zu adaptieren. Da der Hauptunterschied zwischen kabelgebunden und drahtlos nur in der Wahl des Mediums liegt, müssen für eine solche Adaption nur die untersten beiden Schichten, welche sich mit den Physikalischen Grundlagen der Verbindung befassen, erneuert werden. Für diese Aufgabe hat das Institute of Electrical and Electronics Engineers (IEEE) den Standard IEEE 802.11, auch Wi-Fi (Wireless-Fidelity) genannt, entworfen und verabschiedet. Dieser regelt hauptsächlich die Kommunikation auf den untersten beiden Schichten des OSI-Modells [Rec04]. Genauere Beschreibungen der einzelnen Schichten des OSI-Modells finden sich beispielsweise in [Rec04].

3.3 IEEE 802.11

Der Standard IEEE 802.11 implementiert die beiden untersten Schichten, Physical Layer und Data Link Layer, des OSI-Referenzmodells bei drahtlos Netzwerken. Im ursprünglichen IEEE 802.11 Standard wird der Data Link Layer durch eine MAC-Schicht repräsentiert. Der Physical Layer des OSI-Models wird hingegen durch drei unterschiedliche Verfahren beschrieben [Rec04]. Eines dieser Verfahren beschreibt wie Daten per Infrarotverbindung übertragen werden können. Da diese Methode wurde in der Praxis jedoch nie nennenswert angewendet wurde, wird hier nicht weiter darauf eingengen.
Die anderen beiden Protokolle sind Spreizspektrumverfahren, in denen ein schmalbandiges Funksignal in ein breitbandiges Funksignal umgewandelt wird und somit unempfindlicher gegen Störungen mittels Radiowellen übertragen werden kann. Die beiden Methoden heißen FHSS (Frequency-Hopping-Spread-Spectrum) DSSS (Direct-Sequence-Spread-Spectrum) [Rec04]. Die Radiowellenübertragung nutzt in beiden Fällen das ISM-Band (Industrial, Scientific, Medical), welches Frequenzen von 2,400Ghz bis 2,485Ghz nutzt. Dieses Frequenzband darf weltweit für alle industriellen, wissenschaftlichen und medizinischen Zwecke lizenzfrei genutzt werden. Die Tatsache das IEEE 802.11 im ISM-Band arbeitet bietet den großen Vorteil, dass keine Lizenzgebühren für die Nutzung gezahlt werden müssen. Die Tatsache, dass es frei genutzt werden darf führt jedoch auch zu folgendem großen Nachteil: Da es auch für diverse andere Bereiche verwendet wird, kann es immer wieder zu Interferenzen zwischen verschiedenen System kommen und somit kann auch die Übertragungsqualität unter diesen Interferenzen leiden [Rad04].
In IEEE 802.11 sollten sowohl das DSSS-Verfahren als auch das FHSS-Verfahren mit einer maximal Übertragungsrate von 1-2Mbit/sec auftrumpfen. [Rec04]
Außer den soeben vorgestellten Übertragungsverfahren, spezifiziert IEEE 802.11 neben mehreren für diese Arbeit irrelevanten Punkte noch folgende wichtigen Funktionen. Zum einen werden mehrere Sicherheitsmechanismen spezifiziert, welche in Kapitel 4 näher beschrieben werden. Darüber hinaus sind zudem noch Powermanagement und Roaming Funktionen sowie der sogenannte Beacon Frame spezifiziert. Die Punkte Powermanagement und Roaming spielen eine große Rolle, da IEEE802.11 hauptsächlich auf mobile Geräte abzielt und somit sehr flexibel und sparsam gearbeitet werden muss [Rad04]. Powermana-

gement bedeutet in diesem Zusammenhang, dass sich Netzwerkclients schlafen legen können um Energie zu sparen, ohne dass an sie adressierte Pakete verloren gehen. Roaming beschreibt eine ähnliche Funktion wie sie bei allen Mobiltelefonen Anwendung findet. Es sorgt dafür, dass sich ein Client zwischen verschiedenen Funkzellen beliebig hin und her bewegen kann, ohne das die Verbindung zum Netzwerk dabei getrennt wird. Der Beacon Frame spezifiziert ein Informationspaket, welches periodisch vom Access Point ausgesendet wird. Er enthält Information, welche für eine reibungslose Kommunikation zwingend erforderlich sind[Rec04]. Abbildung 2 zeigt, welche Parameter dies sind.

Information	Größe (in bytes)	Bedeutung
Timestamp	8	Uhrzeit des Senders zur Synchronisation der Uhren aller Stationen in einer Zelle
Beacon-Intervall	2	Zeitdauer zwischen dem Aussenden von zwei Beacon. Zusammen mit dem Timestamp können alle Stationen die Startzeit des nächstens Beacon(Target Beacon Transmission Time - TBTT) errechen. Dadurch kann auch das Ausbleiben eines Beacons erkannt werden
Capability	8	Zelleninformationen: Betriebsmodus, Verschlüsselung, CFP-unterstützung
Address	6	Adresse der Zelle, entspricht der MAC-Adresse des Access Points
Data Rate	3 - 8	Übertragungsrate
FH Parameter	7	Wahl des Übertragungskanals
CF Parameter	8	Informationen über evt. Implementierte CFP
TIM	4	Steuerung der Stromsparmodi

Abbildung 2: Beacon Frame (in Anlehnung an [Sik01])

3.3.1 Folgestandards

Seit der Verabschiedung von IEEE 802.11 wurden mehrere Folgestandards in diesem von IEEE beschlossen. Die bis heute wichtigsten davon sind:

IEEE 802.11a Dieser Standard wurde im Jahr 1999 verabschiedet. Der Standard nutz nun nicht mehr das ISM-Frequenzband sondern nutzt Frequenzen im Bereich von 5,4Ghz. Weiter wird ein neues Funkübertragungsverfahren, OFDM (Orthogonal Frequency Division Multiplexing) verwendet. Größter Vorteil von IEEE 802.11a ist die deutlich höhere Übertragungsrate von bis zu 54Mbit/sec. Weiterhin wird das 5,4Ghz Frequenzband deutlich weniger genutzt als das ISM-Band was dafür sorgt, dass es zu weniger Störungen kommt[Rec04]. Aber auch hier kann es unter anderem zu Interferenzen zum Beispiel mit Radar-System kommen. Zudem ist die Reichweite auf Grund von höheren Maximal erlaubten Sende-/Empfangsleistungen besser als bei Geräten die im ISM-Band arbeiten. Leider sind jedoch Geräte welche im 5,4Ghz Bereich arbeiten, teurer als ISM-Geräte. Weiter unterliegt das 5,4Ghz Frequenzband stärkeren gesetzlichen Regulationen. Diese Gründe und die Tatsache das in IEEE 802.11a keine Ad-Hoc Netzwerke spezifiziert sind, führte dazu, dass sich dieser Standard nie durchsetzen konnte [Rad04].

IEEE 802.11b Ebenfalls im Jahr 1999 wurde der Standard IEEE 802.11b ratifiziert. Er arbeitet wie sein Vorgänger IEEE 802.11 im ISM-Band. Den Entwicklern gelang es hierbei die Maximale Übertragungsrate auf 11Mbps aufzustocken und gleichzeitig den Overhead zu minimieren [Rec04]. Der Hauptvorteil von IEEE 802.11b gegenüber IEEE 802.11a liegt in den geringeren Kosten für Endgeräte. Dies führte dazu, dass sich dieser Standard nach [Wiki1] sehr weit verbreitet hat und immer noch weit verbreitet ist.

IEEE 802.11g 2003 wurde der IEEE 802.11g Standard vorgestellt. Er ist eine Weiterentwicklung des IEEE 802.11b Standards und nutzt somit weiterhin das ISM-Frequenzband. Die Maximale Übertragungsrate liegt nun jedoch bei 54Mbps. Er bietet letztendlich alle Vorteile des 802.11b Standards nur das die Datenrate deutlich verbessert werden konnte. Geräte welche im 802.11g Standard arbeiten sind voll kompatibel zu IEEE 802.11b Geräten, jedoch arbeiten sie dann nicht mit voller Geschwindigkeit [Rad04]. Laut [Wiki1] ist IEEE 802.11g aktuell der am weitest verbreitetste Standard.

Neben den oben aufgeführten Standards sind seit 1997 noch etliche weitere Standards vorgestellt worden. Manche von ihnen wurde nie wirklich verwendet, andere wurden von Herstellen von Netzwerkgeräten weiterentwickelt und wurden nie von IEEE als Standard anerkannt und einige wenige befinden sich heute immer noch in der Entwicklungsphase. Da diese Standards jedoch für den Verlauf dieser Arbeit nicht relevant sind, wird auf diese nicht näher eingegangen.

3.4 Was bedeutet Sicherheit

Damit man von Sicherheit in Netzwerken, insbesondere Funknetzwerken, sprechen kann, muss zunächst einmal geklärt werden was Sicherheit genau bedeutet. Letztendlich kann man den Begriff Sicherheit in folgende Unterbegriffe aufteilen [Rad04].

Vertraulichkeit Vertraulichkeit in Netzwerken bedeutet, dass gesendete Daten nur von den Personen gelesen und verwendet werden können für die sie auch bestimmt waren. Da jedoch gerade bei Funknetzwerken nicht sichergestellt werden kann, dass Angreifer die Daten nicht abhören können, muss man Methoden entwickeln um die Daten zu verschlüsseln und somit die Vertraulichkeit der Daten zu wahren.

Identität/Authentizität Identität beschreibt die Tatsache das Sender und Empfänger sich gegenseitig eindeutig Identifizieren und somit eine Kommunikation mit anderen Parteien ausgeschlossen werden kann. Diese Authentifizierung findet in den meisten Fällen durch Passwörter statt. Da Passwörter jedoch geheim bleiben müssen, kommen auch hier Verschlüsselungsmechanismen zum Einsatz um die Vertraulichkeit der Daten zu sichern.

Integrität Unter Integrität wird verstanden, dass die gesendeten Daten nicht verfälscht wurden. Das bedeutet der Empfänger kann davon ausgehen, dass die Daten Originale sind und nicht von dritten Personen verfälscht wurden. Die Integrität von Daten kann an Hand von Checksummen gewährleistet werden. Diese Checksummen werden vor der Übertragung vom Sender erstellt und an die Daten angehangen. Der Empfänger kann diese Summe nach Erhalt der Daten auch berechnen und mit der erhaltenen Summe vergleichen.

Autorisierung Autorisierung bedeutet das einzelnen Clients gewisse Rechte zugeteilt werden. Wenn sich also ein Client in einem Netzwerk anmeldet, darf er unter Umständen nicht alle zur Verfügung stehenden Services nutzen. Damit diese Einschränkungen ausgeführt werden können existieren Autorisierungsmechanismen.

Verfügbarkeit Neben den oben aufgeführten Aspekten spielt die uneingeschränkte Verfügbarkeit aller Netzwerkressourcen eine weitere großen Rolle. Verfügbarkeit bedeutet, dass alle Ressourcen jederzeit fehlerfrei funktionieren und für alle autorisierten Person unabhängig von irgendwelchen Störungen erreichbar sind. Störungen können in diesem Fall neben physikalischen Störungen auch unerlaubte Eingriffe von außerhalb bedeuten.

Zur Sicherung all diese Aspekte wurden im Laufe der letzten Jahre etliche Methoden entwickelt. Die wichtigsten von ihnen werden im weiteren Verlauf dieser Arbeit genauer erläutert und miteinander verglichen. Später wird auch deutlich, dass der Aufwand, welcher betrieben werden sollte oder muss, um Daten zu schützen, sehr davon abhängt was für Daten transferiert werden. Wenn es beispielsweise nur darum geht das eigene Verhalten beim Surfen oder private Kommunikation zu schützen, muss wesentlich weniger Aufwand zum Schutz dieser Daten betrieben werden, als wenn beispielsweise Kontoinformationen, Kreditkarteninformationen oder Identitätsinformationen übertragen werden sollen.

4 In IEEE 802.11 standardisierte Sicherungsmechanismen

In diesem Kapitel werden die Sicherungsmechanismen, welche im IEEE 802.11 Standard definiert sind, vorgestellt und deren Schwachstellen aufgezeigt. Da IEEE 802.11b bzw. IEEE 802.11g die aktuell mit Abstand am weitest verbreitetsten Standards sind [Wiki1] und diese nur eine Weiterentwicklung des IEEE 802.11 Standards sind, sind die im Folgenden vorgestellten Methoden auch die am häufigsten verwendeten Sicherungsmechanismen.

4.1 Netzwerkname

Jedes Wireless LAN besitzt einen Namen. Dieser ist notwendig um das Netzwerk zu identifizieren und sich am richtigen Netzwerk anmelden zu können. Der Name wird im IEEE 802.11 Standard SSID (Service Set Identifier) genannt. Wenn sich ein Client in einem Wireless LAN anmelden möchte, muss er dessen SSID kennen. Diese zwingende Kenntnis der SSID bildet den ersten Sicherungsmechanismus. Denn neben der Möglichkeit die SSID zu broadcasten und somit jedem Client im Empfangsbereich verfügbar zu machen, bieten Access Points die Möglichkeit die SSID nicht öffentlich zu machen. Somit muss jeder Client der sich im Netzwerk anmelden will die SSID kennen[BSI03].

4.2 Benutzerauthentifizierung

Der IEEE 802.11 Standard bietet zwei Möglichkeiten der Benutzerauthentifizierung: Open System und Shared Key.
Open System ist ein sehr einfaches Verfahren, welches zudem keine Sicherheitsaspekte bietet. Da während der Authentifizierung keine Identitätsprüfung des Clients stattfindet, kann sich bei einem Netzwerk mit Open System Authentifizierung jeder Client anmelden und das Netzwerk verwenden. Die Open System Authentifizierung läuft in folgenden zwei Schritten ab [Rec04]. Zunächst sendet ein Client eine Authentifizierungsanfrage an das Netzwerk welches in diesem Fall von einem oder mehreren Access Point repräsentiert wird. Der Access Point antwortet dem Client und gewährt den Zugang zum Netzwerk. Die Antwort des Access Points kann Statusinformationen über das Netzwerk beinhalten. Für eine Authentifizierung mit dem Open System Verfahren ist es notwendig das der Client die Netzwerk SSID kennt.
Das Shared Key Verfahren ist etwas anspruchsvoller als das Open System Verfahren. Da es jedoch nur bestimmten Clients den Zugang zum Netzwerk gestattet, soll es mehr Schutz bieten. Die Basis der Shared Key Authentifizierung bildet das WEP Verfahren(Wired Equivalent Privacy) und dessen WEP-Keys (siehe Kapitel 4.3). Die Authentifizierung geschieht bei Shared Key in vier Schritten. Zunächst stellt ein Client eine Anfrage an das Netzwerk. Diese Anfrage landet in der Regel bei einem Access Point und wird von diesem mit einem Challenge-Response beantwortet. Die Challenge besteht üblicherweise aus einem 128bit langen, zufällig generierten, Klartext. Im dritten Schritt verschlüsselt der Client den soeben erhalten Klartext mit Hilfe des beidseitig

bekannten, aber geheimen, WEP-Keys und sendet die so verschlüsselte Nachricht wieder zurück zum Access Point. Der Access Point muss die erhaltene Nachricht nun nur noch entschlüsseln und mit der ursprünglichen Nachricht vergleichen. Sollten beiden Nachrichten identisch sein, so wird davon ausgegangen, dass der Client die Berechtigung besitzt dem Netzwerk beizutreten. Folglich wird der Client authentifiziert und im Netzwerk angemeldet [Rec04].

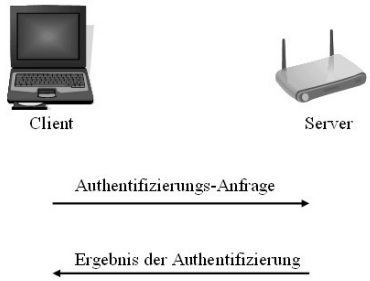

Abbildung 3: Open System

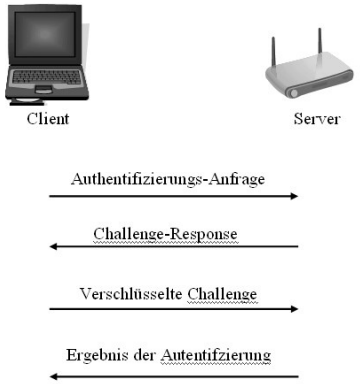

Abbildung 4: Shared Key

4.3 WEP-Verschlüsselung

Eine WEP Verschlüsselung dient zum einen der Authentifizierung eines Clients mit Hilfe des Shared Key Verfahrens (siehe Kapitel 4.2) und zum andern der Verschlüsselung aller transferierten Daten. WEP nutzt den RC4 Algorithmus [BSI05] welcher 1987 von RSA-Security Inc. entwickelt wurde. Als Basis für die Verschlüsselung werden in der Regel einer bis vier WEP-Keys abwechselnd verwendet. Diese Schlüssel müssen allen Netzwerkteilnehmern bekannt sein, sind ansonsten aber geheim.
IEEE 802.11 spezifiziert zwei Verschlüsselungsgrade; entweder WEP64 oder WEP128. WEP64 erklärt sich daher, dass ein 40bit langer Schlüssel und ein 24bit langer Initialisierungsvektor verwendet wird. Bei WEP128 bleibt der Initialisierungsvektor nach wie vor 24bit lang, die Schlüssellänge hingegen wächst auf 104bit. Die Verschlüsselung läuft in beiden Fällen wie folgt ab: (vergleiche Abbildung 5) Der Initialisierungsvektor bildet zusammen mit dem Schlüssel die Eingabe für den RC4 Algorithmus, welcher aus ihnen einen Schlüsselstrom erzeugt. Von den zu verschlüsselnden Daten wird mittels CRC-32 Verfahren eine Prüfsumme oder Integrity Check Value (ICV) erstellt. Dieser Wert wird an die Klartextnachricht angehangen. Die daraus entstandene Nachricht wird nun mit dem zuvor berechneten Schlüsselstrom XOR-Verknüpft, was letztendlich zur verschlüsselten Nachricht führt. Da der Initialisierungsvektor vor jeder Übertragung zufällig erzeugt wird und der Empfänger die Nachricht ohne den Initialisierungsvektor nicht entschlüsseln kann, muss dieser ebenfalls dem Empfänger übermittelt werden. Diese Übermittlung geschieht indem er einfach an die verschlüsselte Nachricht angehangen wird.

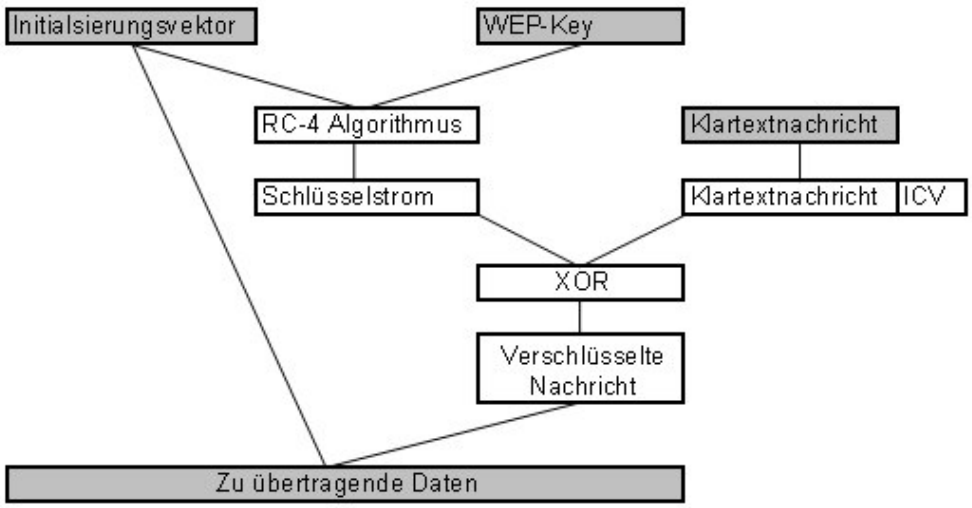

Abbildung 5: WEP-Verschlüsselung

4.4 MAC-Filter

Der letzte Sicherungsmechanismus den IEEE 802.11 bietet, ist es den Zugang zu Drahtlosnetzwerken mittels eines MAC-Adressenfilters zu regulieren.
MAC-Adresse (Media Access Control-Adresse) sind 48bit lange hexadezimal Werte. Jedes Netzwerkgerät weltweit bekommt eine solche Adresse fest und unveränderbar vom Hersteller zugewiesen. Diese Hex-Werte werden eindeutig vergeben, das bedeutet, es existieren keine zwei Geräte mit der gleichen MAC-Adresse [Rad04]. Dieser Verfahren ermöglicht nun eine recht einfache aber wirkungsvolle Identifizierung eines Clients. Somit kann der Zugang zu einem Netzwerk darüber reguliert werden, dass alle MAC-Adressen, denen der Zugang zum Netzwerk gestattet werden soll, dem Access Point in einer Liste zur Verfügung gestellt werden. Diese Liste kann entweder im internen Speicher des Access Points gespeichert werden oder ihm mittels des RADIUS Protokolls (Remote Dial-In User Authentification Service) von einem zentralen Server bereitgestellt werden. Die Bereitstellung von einem Server ist gerade dann von Vorteil wenn es mehrere Access Points in einem Netzwerk gibt. Jeder Access Point kann anhand dieser Liste entscheiden ob ein Client auf das Netzwerk zugreifen darf oder nicht [Rec04].

4.5 Schwachstellenanalyse der IEEE 802.11 Sicherungsmaßnahmen

SSID Kann nicht als Sicherungsmechanismus im eigentlichen Sinne betrachtet werden, da sie keinen nennenswerten Zuwachs an Sicherheit bringt. Dies liegt daran, dass auch bei deaktiviertem SSID Broadcast die SSID mittels geeigneter Tools (siehe Kapitel 6.1) auslesbar bleibt. Sie muss mehr als notwendige Identifikation gesehen werden, welche nur dazu genutzt werden kann ein Netzwerk auf den ersten Blick unsichtbar erscheinen zu lassen. Trotzdem sollte der Broadcast möglichst deaktiviert werden um

einem Angreifer möglichst wenig Angriffsfläche zu bieten.

Benutzerauthentifizierung Es hat sich gezeigt, dass das eigentliche sicherere Shared Key Verfahren leider nicht mehr Sicherheit bietet als das Open System Verfahren. Es ist sogar so, dass bei einer Shared Key Authentification bereits während der Authentifizierung ungewollt Informationen über den verwendeten WEP-Key offen gelegt werden [BSI05]. Dadurch ist es möglich, dass sich ein Angreifer im Netzwerk anmelden kann ohne den WEP-Key zu kennen [Rad04]. Als Konsequenz daraus ergibt sich, dass besser auf eine Shared Key Authentifizierung verzichtet werden sollte.

WEP-Verschlüsselung Auch die WEP-Verschlüsselung bietet keinen ausreichenden Schutz und kann sehr schnell geknackt werden. Sollte sogar nur eine WEP64 Verschlüsselung verwendet werden, so ist mit heutigen Computern selbst durch Bruteforce Attakten innerhalb kurzer Zeit möglich den Key zu erlangen [?].
Bei WEP128 ist Bruteforce nicht mehr die erste Wahl. In diesem Fall wird ein Schwachpunkt des verwendeten RC-4 Algorithmus ausgenutzt. Die Schwachstelle des RC-4 Algorithmus liegt darin, das die Verschlüsselung nur solange sicher ist, solange kein Schlüsselstrom zweimal verwendet wurde[RSA01]. Da zur Generierung des Schlüsselstroms nur der Initialisierungsvektor und der WEP-Key verwendet werden und der WEP-Key als statisch angesehen werden kann, reicht es also aus, wenn ein Initialisierungsvektor wiederholt verwendet wird. Dieses ist jedoch auf Grund der geringen Länge von 24bit schon nach ca. 16 Millionen Paketen zwingend notwendig [BSI03]. Es kann jedoch auch schon viel früher dazu kommen, dass ein Initialisierungsvektor erneut verwendet wird, da es kein festgelegtes System gibt wie sich Initialisierungsvektoren von Paket zu Paket verändern. Tools, welche für einen solchen Angriff verwendet werden können, werden im Kapitel 6.4 genauer vorgestellt.

MAC-Filter Das Prinzip Clients an Hand ihrer MAC-Adresse zu authentifizieren, funktioniert problemlos. Leider wird die MAC-Adresse des Senders jedoch bei jedem Paket im Klartext mit übermittelt. Dies geshieht unabhängig davon, ob WEP aktiviert oder deaktiviert ist. Somit kann also ein Angreifer relativ leicht an gültige MAC-Adressen kommen und diese dann nutzen um sich am Netzwerk anzumelden [Rec04]. Die dazu notwendigen Tools werden in Kapitel 6.3 genauer beschrieben

4.6 Fazit

Ein großer Vorteil aller in diesem Kapitel vorgestellten Maßnahmen ist, dass sie alle uneingeschränkt mit jedem IEEE 802.11 Gerät verwendet werden können und sehr leicht zu verwenden sind. Da heutzutage die 802.11 Geräte nahezu eine Monopolstellung haben, ist dieses sehr praktisch und anwenderfreundlich. Leider bieten die Mechanismen jedoch bei weitem nicht die Sicherheit, die sich ihre Erfinder erhofft hatten und die notwendig ist um von sicherer

Kommunikation sprechen zu können. Wie im letzten Kapitel gezeigt, können alle Mechanismen relativ leicht umgangen werden. Somit ist es nicht zu empfehlen, ein Netzwerk nur mit den vorgestellten Sicherheitsmechanismen zu schützen[BSI05]. Dieses hat auch die Industrie erkannt und neue, bessere Sicherheitsmechanismen entwickelt. Welche das sind, wird im nächsten Kapitel genauer beschrieben.

5 weitere Sicherheitsmechanismen

Neben den im letzte Kapitel vorgestellten Sicherheitsmechanismen nach dem IEEE 802.11 Standard existieren noch diverse andere Methoden über Funknetzwerkverbindungen sicherer zu machen. Welche Methoden es gibt, wie sie funktionieren und welche Vor- und Nachteile sie bieten wird in diesem Kapitel näher erläutert.

5.1 Temporäre Lösungen

Die beiden folgenden Sicherheitsmechanismen bilden beide eine Weiterentwicklung des in IEEE 802.11 spezifizierten WEP-Verschlüsselungsverfahrens. Sie sind beide proprietär und nicht von IEEE oder anderen Organisationen standardisiert. Somit können sie nicht als langfristige Problemlösung dienen, sondern nur als Übergangslösungen bis bessere Standards verabschiedet sind und auch die notwendige Verbreitung haben. In Kapitel 4.5 wurde gezeigt, dass das Hauptproblem der WEP-Verschlüsselung im Schlüsselstrom und somit letztendlich der Erzeugung des Initialisierungsvektor liegt. Hier versuchen die beiden Verfahren WEPPlus und Fast Packet Keying Abhilfe zu schaffen. Beide Verfahren sind proprietär und sind nicht von IEEE als Standard angenommen.

5.1.1 WEPPlus

WEPplus ist ein von Agere entwickelter Zusatz zur WEP-Verschlüsselung der dafür sorgt, dass keine schwachen Initialisierungsvektoren mehr verwendet werden. In der Praxis hat sich gezeigt, dass nicht der RC4 Algorithmus die Sicherheitslücke darstellt, sondern dass der Initialisierungsvektor das eigentliche Problem darstellt. Wie in Kapitel 4.5 beschrieben, ist die Verschlüsselung solange sicher, solange keine Pakete mit ein und demselben Initialisierungsvektor verschlüsselt und übertragen wird. Dieser wird bei WEP vor jeder Übertragung eines Paketes neu erstellt und auch nur für diese Übertragung verwendet. Leider kommt es nach einer gewissen Anzahl von gesendeten Paket dazu, dass sich die Initialisierungsvektoren wiederholen und sich dem Angreifer somit eine gute Angriffsmöglichkeit bietet. WEPplus sorgt dafür das solche schwachen Initialisierungsvektoren nicht mehr verwendet werden [Rad04].

5.1.2 Fast Packet Keying

Ähnlich wie WEPplus versucht auch Fast Packet Keying, die Erstellung, der für den RC4 Algorithmus notwendigen Initialisierungsvektoren zu verbessern und die Verschlüsselung somit sicherer zu machen. Der große Unterschied zwischen WEPplus und Fast Packet Keying liegt darin, dass bei WEPplus nach wie vor alle Netzteilnehmer den gleichen Schlüsselstrom nutzen. Bei Fast Packet Keying geht man dazu über das jeder Teilnehmer einen eigenen Schlüsselstrom zum Übertragung verwendet. Bei diesem Verfahren wird für jedes gesendete Datenpaket in schneller Abfolge verschiedene RC-4 Schlüsselströme generiert [RSA01]. Damit eine solche Generierung möglich ist, ist es notwendig, dass sich Sender und Empfänger einen gemeinsamen 128bit langen Schlüssel teilen.

Dieser Schlüssel wird Temporal Key(TK) bezeichnet. Aus diesem TK und der Mac-Adresse des Senders wird nun ein senderspezifischer Schlüssel berechnet. Dieser Schlüssel wird nun zusammen mit einem 16bit langen Initialisierungsvektor, welcher für jeweils nur einmal verwendet wird, dazu genutzt, den eigentlichen RC-4 Schlüsselstrom bestehend aus 24bit Initialisierungsvektor und 104bit Schlüssel zu berechnen[Gol01].

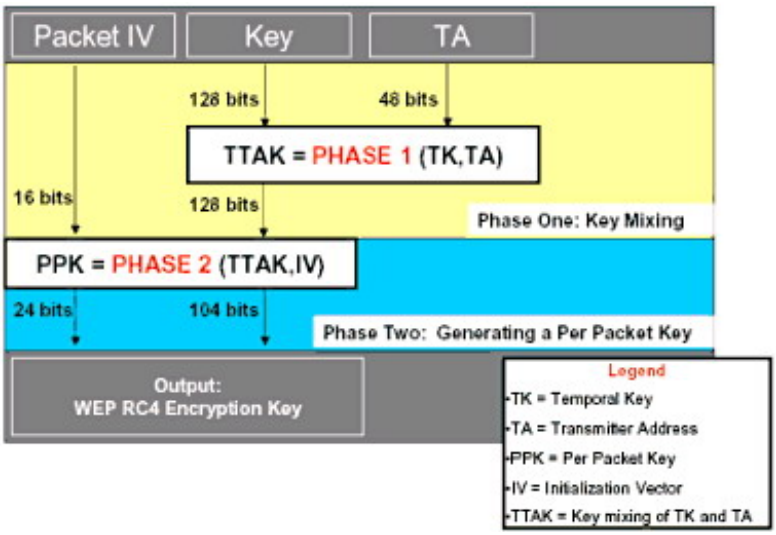

Abbildung 6: Schlüsselerzeugung bei Fast Packet Keying [Gol01]

Auch dieses Verfahren soll angeblich per Softwareupdate auf allen IEEE 802.11b/g Netzwerkgeräten verwendet werden können. Ob Hersteller von solchen Geräten dieses Verfahren jedoch annehmen und unterstützen, steht ihnen auf Grund der fehlenden Standardisierung weiterhin frei. Durch die Verwendung der sogenanneten Temporal-Key-Hash-Technique, welche ein Teil der Ergebnisse zwischenspeichert, soll es in der Praxis zu keinen nennenswerten Performanceeinbußen bei der Erzeugung der Schlüsselströme kommen [Gol01]. Wie Kapitel 5.2.1 beschrieben wurde die Idee von Fast Packet Keying von IEEE für den zukünftigen IEEE 802.11i Standard aufgenommen und weiter verwendet.

5.2 IEEE 802.11i

Nachdem bekannt wurde, dass die Verschlüsselungsverfahren in IEEE 802.11 teilweise doch deutliche Sicherheitslücken beinhalten, versuchte IEEE einen neuen Standard namens IEEE 802.11i (später auch WPA2 genannt) zu etablieren. Dieser sollte neue Sicherungsmechanismen beinhalten und die Kommunikation in Drahtlosnetzwerken somit deutlich sicherer machen. Da man jedoch schon vor der endgültigen Ratifizierung von IEEE 802.11i im Juni 2004 einen deutlichen Handlungsbedarf im Bereich Verschlüsselung gesehen hat, nahm IEEE einen Teil des IEEE 802.11i Standards vorweg und veröffentlichte im April 2003 den Pseudostandard WPA (Wi-Fi protected Access)[Rec04]. Dieser Standard sollte die WEP-Verschlüsselung ersetzen und somit den gestiegenen

Sicherheitsanforderungen genügen. Welche Funktionen und Verfahren in WPA verwendet werden, wird im nächsten Abschnitt beschrieben.

5.2.1 WPA

Der Pseudostandard WPA basiert auf der gleichen Architektur wie WEP und es wird auch weiterhin eine RC-4 Verschlüsselung verwendet. Jedoch kommen bei WPA folgende Verfahren zum Einsatz um die Sicherheitslücken von WEP zu schließen.

- TKIP
  Das TKIP Verfahren(Temporal Key Integrity Protocol) versucht das Hauptproblem von WEP zu lösen. Diese besteht darin, dass der verwendete Schlüssel statisch ist. Hier greift TKIP ein und verwendet ein ähnliches Verfahren wie Fast Packet Keying (sieht Kapitel 5.1.2) um kontinuierlich neue Schlüssel zu erzeugen und zu verwenden.[Rad04] Ein Schlüssel wird immer nur für 10kb Daten verwendet, danach wird er durch einen anderen ersetzt.
  Anders als Fast Packet Keying verwendet TKIP allerdings 48bit lange Initialisierungsvektoren, welche aus zwei Teilen bestehen. Der erste Teil ist 16bit lang und wir vor jeder Übertragung um eins hochgezählt. An Hand dieses Wertes ist es dem Empfänger möglich festzustellen, ob er eine Paket bereits erhalten hat oder dieses noch aussteht.

- MIC
  MIC steht für (Message Integrity Check) und stellt eine Alternative zum CRC Verfahren,welches bei WEP-Verschlüsselungen verwendet wird, dar. CRC ist inzwischen mittels man-in-the-middle Attacken sehr leicht zu knacken und zu beeinflussen[Rad04]. Das MIC Verfahren nummeriert alle WEP-Frames fortlaufen durch. Dadurch ist es möglich, Frames, welche nicht in der richtigen Reihenfolge eintreffen, zu verwerfen. Weiter wird auch bei MIC eine Prüfsumme der zu übertragenden Daten erstellt. Diese Prüfsumme ist jedoch gegen das systematische Vertauschen von Bits in einem WEP-Paket (Bit Flipping) resistent[Rec04]. In Verbindung mit TKIP kann man durch die Verwendung von MIC Daten wesentlich sicherer und besser auf Integrität testen.

5.3 Der eigentliche IEEE 802.11i Standard

Für den Standard 802.11i wurden von IEEE mehrere Verbesserungen gegenüber den alten Standards geplant. Zum einen sollte der komplette WEP Algorithmus durch einen neues Verfahren WPA ersetzt werden. Wie dieses Verfahren arbeitet und welche Vorteile es mit sich bringt wurden bereits im letzten Kapitel gezeigt. In diesem Kapitel geht es darum, welche Verfahren noch in IEEE 802.11i enthalten sind und welche Vorteile diese bieten.
Zum einen wurde der zuvor verwendete Verschlüsselungsalgorithmus RC-4 durch den neuen AES (Advanced Encryption Standard) ersetzt. Zudem wird der Authentifizierungsstandard IEEE 802.1x angewendet.

5.3.1 AES-Verschlüsselung

AES ist ein symmetrisches Verschlüsselungssystem, welches im Oktober 2000 vom National Institute of Standards and Technology (NIST) standardisiert wurde. Symmetrisch bedeutet, dass zur Verschlüsselung und zur Entschlüsselung der gleiche Schlüssel verwendet wird. Das AES Verfahren ist frei zugänglich und kann kostenfrei verwendet werden. Dies geschieht bis heute auch bei etlichen Verfahren wie SSH, IPSec, PGP [Rad04].
Bis heute ist außer Bruteforce kein Angriff bekannt, mit dem eine AES Verschlüsselung geknackt werden kann. Bruteforce führt jedoch bei Schlüssellängen von 128bit nicht in annehmbarer Zeit zum Erfolg. Nachteilig ist aber, dass man für die Verwendung einiger Veränderungen auf der Hardwareseite vornehmen muss. Somit kann nicht garantiert werden das IEEE 802.11b/g Geräte auch mit dem Standard IEEE 802.11i arbeiten können [Rad04].

5.3.2 IEEE 802.1x und EAP

Wie bereits erwähnt, sollte im IEEE 802.11i Standard auch ein neues Verfahren zur Benutzerauthentifizierung verwendet werden. Man entschied sich für den 2001 entstanden Standard IEEE 802.1x. Dieser Standard wurde nicht explizit für Funknetzwerke entwickelt, sondern stellte eine Methode dar, wie man in beliebigen Netzwerken Benutzer authentifizieren kann[Rad04]. Für diese Authentifizierung wird ein zentraler RADIUS (Remote Authentification Dial-In User Service) Server verwendet. Entwickelt wurde das RADIUS Protokoll um Benutzer, welche sich in das Internet oder andere Netzwerke einwählen wollen, zu authentifizieren. Es ermöglicht die Authentifizierung, Autorisierung und Accounting von einzelnen Clients und wird daher auch als AAA-Protokoll bezeichnet [Rec04].
Der große Vorteil ist, dass nicht jeder Einwahlpunkt, im Falle eines Funknetzwerkes ein Access Point, die Authentifizierung selber durchführen muss, sondern dass die Authentifizierung zentral auf dem RADIUS Server stattfindet. Damit dies möglich ist, muss sich ein Client versuchen, sich an einem Access Point anzumelden. Da dieser die Anfrage selber nicht bearbeiten kann, leitet er die Anfrage an den zentralen RADIUS Server weiter. Der RADIUS Server kann nun an Hand von Benutzerdatenbanken feststellen, ob und wenn ja, welche bereitgestellten Services ein Client nutzen darf. Das Ergebnis der Authentifizieren wird nun an den Access Points zurück gesendet, damit dieser dem Client den Zugang zum Netzwerk erteilen kann oder eben nicht. Ob Pakete, die den Access Point erreichen, zur Authentifizierung verwendet werden sollen oder als Nutzlast angesehen werden sollen, wird dadurch entschieden, dass ein Access Point die physikalische Verbindung vom LAN in einen kontrollierten und einen unkontrollierten logischen Port aufteilt. Der unkontrollierte Port ist immer offen und dient nur der Übermittlung von Identifikationsanfragen und Antworten. Der kontrollierte Port ist immer blockiert und wird nur bei erfolgreicher Authentifizierung geöffnet. Über ihn findet dann die eigentliche Kommunikation statt [Rec04].
Da es für eine fehlerfreie Authentifizierung notwendig ist, dass die übertragenen Daten nicht verfälscht werden, kommt für die Kommunikation zwischen

Client und Access Point und zwischen Access Point und RADIUS Server das EAP (Extensible Authentification Protocol) zum Einsatz. Auch dieses Verfahren wird nicht nur bei Funknetzwerken eingesetzt, sondern kommt auch bei PPP(Point-to-Point Protocol) und Ethernet Verbindungen zum Einsatz. (Im folgenden wird allerdings nur auf die Verwendung im Drahtlosnetzwerk eingegangen)
Für die Verwendung in Funknetzwerken wurden EAPoW(EAP over WLAN)Pakete spezifiziert, welche genau ein EAP-Paket in einem IEEE 802.11 Paket kapseln [Rec04]. Das EAP Protokoll spezifiziert wie Authentifizierungsnachrichten zu formatieren und zu interpretieren sind und wie der Datenaustausch zwischen den drei Parteien einer Authentifizieren stattfindet. Nicht spezifiziert wird jedoch der konkrete Authentifizierungsmechanismus. Dieser kann variabel gewählt werden und die für ihn notwendigen Daten in einem EAP-Paket verpackt werden.
Inzwischen wurden mehr als 40 EAP-Verfahren, das heißt Authentifizierungsmethoden, die das EAP-Framework nutzen, entwickelt. Einige von ihnen sind für die Authentifizierung in Funknetzen nicht geeignet, da diese nur Benutzernamen und Passwort erfordern, welche im Klartext übermittelt werden und somit sehr leicht abhörbar sind. Andere nutzen verschiedene Arten von Zertifikaten um die Authentifizierung durchzuführen und bieten daher mehr Schutz[Rad04].
Da alle diese Verfahren das EAP-Framework nutzen, läuft der Nachrichtenaustausch und somit die Authentifizierung zwischen den beteiligten Parteien immer wie folgt ab [Ott04]. (Vergleiche Abbildung 7)

- Zunächst muss allen Parteien bekannt sein welche EAP-Methode genau verwendet werden soll. Dies wird in Drahtlosnetzwerken mittels RSNIE (Robust Secure Network Information Element) gemacht. Diese RSNIEs werden von einem Access Point im Beacon Frame gebroadcastet .

- Access Points broadcasten regelmäßig Identifikationsanfragen. Sollte ein Client eine solche Anfrage empfangen, sendet dieser eine EAP-Response an den Access Point und teilt ihm somit seine Identität mit. Sollte zum Zeitpunkt der gewünschten Identifizierung keine Anfrage eingehen, kann ein Client auch eine EAPoW-Start Nachricht aussenden und somit die Identifikationsaufforderung bei allen in Reichweite befindlichen Access Points anfordern.

- Der Access Point filtert das EAP-Paket nun aus dem EAPoW Paket heraus und leitet es an den RADIUS Server weiter.

- Der Server leitet die eigentliche Authentifizierung ein und sendet dem Client, wieder über den Access Point, eine entsprechend der gewählten EAP-Methode passende Zugangs-Challenge und wartet dann auf Antwort vom Client.

- Sollte der Client korrekt geantwortet haben, so sendet der Server eine RADIUS-Accepted Nachricht an den Access Point worauf dieser dem Client den kontrollierten Port öffnet. Wenn die Antwort falsch ist, wird

eine RADIUS-Rejected Nachricht an den Access Point gesendet und dieser öffnet den kontrollierten Port nicht. Hiermit ist die Authentifikation abgeschlossen

- Wenn eine authentifizierte Verbindung getrennt werden soll, wird vom Client eine EAPOL-Logoff Nachricht gesendet und die Verbindung somit getrennt.

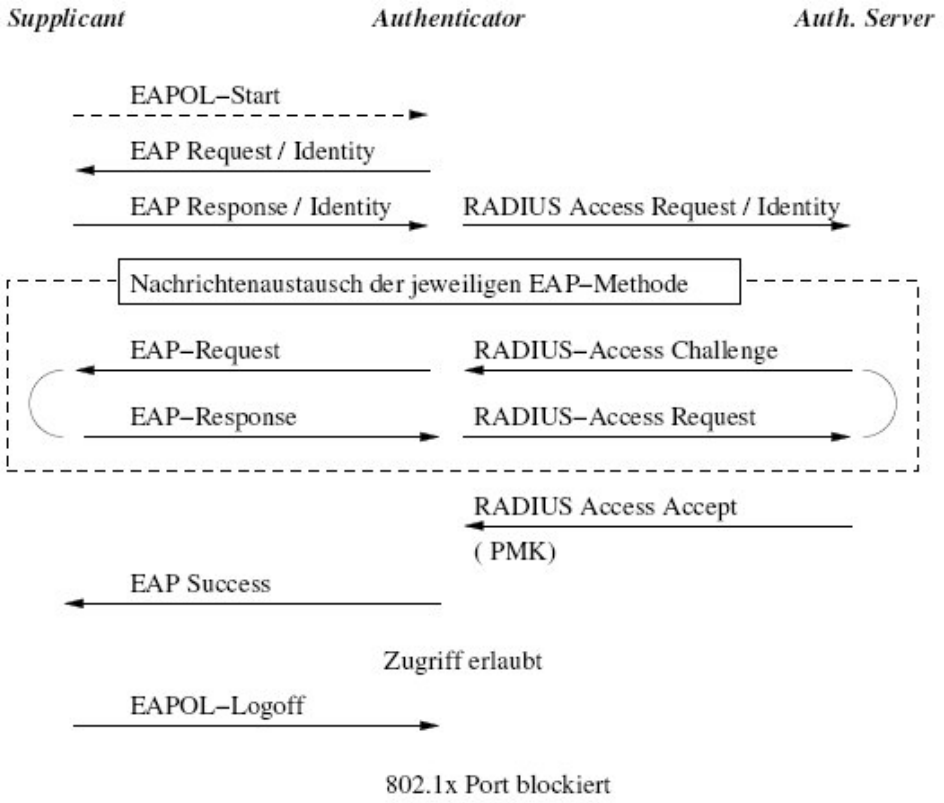

Abbildung 7: Authentifizierung mittels EAP [Ott04]

Obwohl der Client nun authentifiziert ist, können noch keine Daten übertragen werden. Dazu ist es erst notwendig, dass Client und Access Point noch Schlüssel für das TKIP Protokoll erhalten. Da alle Pakete, die während der Authentifizierung zwischen Client und Server ausgetauscht wurden, verschlüsselt sind und somit nur vom Client oder vom Server gelesen werden können, ist der Access Point nicht in der Lage die TKIP-Schlüssel selbst zu berechnen und benötigt somit Hilfe vom RADIUS Server. Dieser berechnet die Schlüssel und stellt sie dem Access Point zur Verfügung. Der Client hingegen kann diese anhand der RADIUS-Accepted Nachricht selber berechnen [Ott04].
Wenn nun Client und Access Point über die Schlüssel verfügen, kann die sichere Kommunikation beginnen[Rad04].

5.4 Virtual Private Network

Ein VPN (Virtual Private Network) bezeichnet einen Verbindung zwischen zwei Computern oder Netzwerken über ein weiteres Netzwerk. Dieses Netzwerk wird als Medium verwendet und kann sowohl ein Funknetzwerk als auch das Internet oder jede beliebige Art von Netzwerk sein. Der Sinn eines VPN liegt darin, sicher Daten zwischen zwei Punkten zu übertragen ohne dabei auf eine private und sichere Verbindung angewiesen zu sein. Erreicht wird dies in dem ein Tunnel zwischen den beiden Kommunikationspartnern aufgebaut wird. Dieser Tunnel bezeichnet eine Ende zu Ende Verbindung, welche im Optimalfall verschlüsselt ist[BSI03]. Theoretisch kann man ein VPN auch ohne Verschlüsselung des Tunnels realisieren. Da dies jedoch für den Schutz von Daten in Funknetzen keinen Sinn macht, wird darauf nicht weiter eingegangen.
VPN Verbindungen stellen eine sehr starke und gute Möglichkeit dar Funknetzwerke zu schützen. Mit Hilfe von verschiedenen Verschlüsselungsverfahren, auch Tunnelverfahren genannt, ist möglich den Grad der Sicherheit nahezu beliebig zu wählen[Rad04]. Welche Tunnelverfahren es gibt, wie sie funktionieren und welche Vorteile sie bieten, wird im nächsten Abschnitt genauer beschrieben.

5.4.1 Tunnelverfahren

Tunnelprotokolle werden dazu eingesetzt um sensible Daten über unsichere Netzwerke zu transportieren. Die zu übertragenden Daten werden hierzu verschlüsselt und in eigenen Datenpaketen von der Umwelt abgekapselt. Diese Datenpakete können dann praktisch gefahrlos über jeden beliebigen Datenweg transportiert werden. Neben der Kapselung von Daten muss ein Tunnelprotokoll zudem noch die Entkapselung und den Transport der Daten realisieren. Solange ein ausreichend sicheres Verschlüsselungsverfahren verwendet wird und nur Sender und Empfänger über die entsprechenden Schlüssel verfügen, ist eine VPN-Verbindung nahezu abhörsicher.[Rad04] Im folgenden werden die am häufigsten verwendeten Tunnelprotokolle kurz vorgestellt.

PPTP (Point-to-Point Tunneling-Protocol) PPTP ist ein Tunnelverfahren, welches von einem Herstellerkonsortium um Ascend Communications, Microsoft, 3Com und diverse andere, als Erweiterung des PPP(Point-to-Point Protocol)entwickelt wurde. Das PPTP Protokoll arbeitet in der zweiten Schicht des OSI-Modells und bietet dem Anwender die Möglichkeiten IP- IPX- und NetBEUI-Pakete verschlüsselt über unsichere Netzwerke zu transportieren . Neben der Verschlüsselung bietet PPTP auch noch Punkt-Punkt-Sicherheit und Benutzerauthentifizierung. Bei der Authentifizierung stehen entweder das CHAP Verfahren(Challenge Handshake Protocol) oder das PAP Verfahren (Password Authentication Protocol) zur Verfügung. Bei der Verschlüsselung kann neben den bereits bekannten Verfahren RC-4 und AES auch auf das DES Verfahren(Data Encryption Standard) zurückgegriffen werden [Rec04]. Obwohl bei PPTP in der Vergangenheit immer wieder diverse Sicherheitslücken entdeckt wurden und PPTP somit heutzutage nicht mehr zu den sichersten Tunnelverfahren zählt [Rad04] [Rec04], ist es immer noch sehr weit

verbreitet. Dies liegt inbesondere daran, dass es nach wie vor standardmäßig in Windows integriert ist.
PPTP bietet für den Transport alltäglicher Daten mehr als genug Sicherheit. Für Daten mit höchster Sensibilität sollte jedoch ein anderes Verfahren genutzt werden.

L2F (Layer-to-Forward) Dieses Protokoll wurde von Cisco Systems entwickelt und arbeitet genauso wie PPTP im Data-Link-Layer des OSI-Modells. Für Funknetzwerkwerkverbindungen kann dieses Protokoll jedoch nicht verwendet werden, da es nur bei sogenannten erzwungenen Tunnels verwendet werden kann. Erzwungen Tunnels, sind Tunells bei denen der User selber nicht wählen kann ob er einen Tunnel verwenden möchte und wenn ja, wann er diesen etablieren bzw. wieder schließen möchte[Rad04].

L2TP (Layer-to-Tunneling-Protocol) Das L2TP Verfahren ist eine Weiterentwicklung der beiden vorherigen Verfahren und vereint die Vorteile beider Verfahren in sich. Der Hauptunterschied zu den beiden Vorgängern liegt darin, dass es nicht mehr in der zweiten OSI-Schicht arbeitet, sondern in der dritten. In der Praxis hat dieses Verfahren das alte PPTP Verfahren inzwischen teilweise abgelöst. Ein wichtiger Grund dafür liegt in der Variabilität bei den zu verschlüsselnden Protokollen. PPTP ist nur in der Lage IP- IPX- und NetBEUI-Pakete zu übertragen. L2TP kann neben diesen noch mit X.25, Frame Relay oder ATM Paketen verwendet werden. Zudem bietet L2TP die Möglichkeit einen Tunnel nicht nur zwischen zwei Parteien zu etablieren, sondern diesen beliebig vielen Clients zugänglich zu machen ohne dabei die Sicherheit der Verbindung zu vernachlässigen [Rad04].
Leider gilt auch dieses Verfahren aktuell nicht mehr als zeitgemäß und sollte nicht für hoch sensible Daten verwendet werden [Rec04].

IPsec (IP Security) Dieses Protokoll wurde 1998 entwickelt um die Sicherheitslücken des IP-Protokolls zu schließen. Es dient somit dazu IP-Verbindungen zu tunneln. Letztendlich stellt das IPsec Protokoll ein Framework zur Verfügung mit dessen Hilfe es möglich ist, die Sicherheit einer IP-Verbindung zu gewährleisten. Sicherheit bedeutet bei IPsec: Daten Verschlüsselung, Authentifizierung einzelner Pakete als auch Benutzer zudem bietet IPsec noch eine Schlüsselmanagement Option und Punkt-zu-Punkt Sicherheit. IPsec schränkt aber keines dieser Hauptziele soweit ein, dass ein bestimmtes Verfahren verwendet werden muss. Es ist vielmehr sehr flexibel was die Einbindung und Verwendung neuer Protokolle angeht. Beispielsweise kann man zur Datenverschlüsselung nahe zu alle gängigen Verschlüsselungssysteme wie DES , IDEA (International Data Encryption Algorithm), Blowfish und AES verwenden. Das verwendete Verfahren ist dabei ausschlaggebend für die erreichte Sicherheit [BSI05]. Zur Authentifizierung können ebenfalls mehrere Verfahren verwendet werden. Beispielsweise kann das AH Verfahren (Authentification Header) verwendet werden, welches die Pakete nur mit digitale Signaturen versieht

und somit für die Verwendung im Funknetzwerken nicht geeignet ist. Es kann aber auch das ESP Verfahren (Encapsulating Security Payload) verwendet werden, welches auf Grund von digitalen Signaturen und Datenverschlüsselung wesentlich besser geeignet ist [Rad04]. Nach [BSI05] bietet IPSec in absehbarer Zeit den besten Schutz ohne dabei die Kompatibilität zu vernachlässigen

6 Analysewerkzeuge

In folgenden Kapitel werden Programme vorzustellt, mit deren Hilfe es möglich ist Schwachstellen im Netzwerk aufzudecken und sichtbar zu machen. Letztendlich können all diese Programme jedoch nicht nur dazu genutzt werden ein Netzwerk zu analysieren und es dann sicherer zu machen, sondern sie bilden auch die Basiswerkzeugen für Angreifer. Einem einigermaßen versierten, mit dem notwendigen Equipment und ausreichend Zeit ausgestatteten Angreifer, ist es mit Hilfe der folgenden Programme ein Leichtes, Netzwerke, die nur über geringe Sicherungsmaßnahmen verfügen zu manipulieren oder für seine Zwecke zu nutzen.
Die im folgenden beschriebenen Werkzeuge können nach [Rad04] grob in vier Kategorien eingeteilt werden.

- Scanner
- Sniffer
- Spoofer
- Wep-Crack

Welche Funktionen die einzelnen Kategorien übernehmen und welche Programme es gibt, wird im Weiteren gezeigt.

6.1 Scanner

Programme, welche in der Kategorie Scanner angesiedelt sind, helfen dabei generelle Information über Funknetzwerke zu erlangen. Mit ihnen ist es somit möglich über alle in Reichweite befindliche Netzwerke Informationen wie beispielsweise SSID, Signalstärke -qualitäten und Mac-Adresse des Senders zu erlangen.

Netstumbler

Netstumbler ist ein Windowstool, welches als Freeware zum Download [1] bereit steht. Es kann mit jeder Funknetzwerkkarte verwendet werden und ist sehr einfach zu bedienen. Dem User werden sehr schnell und einfach folgende Daten aller Netzwerke in Reichweite offen gelegt.

- SSID, auch wenn die SSID nicht gebroadcastet wird
- Signalstärke und Signalqualität
- Status der Verschlüsselung
- Mac-Adresse des Senders

[1] http://www.netstumbler.com/ (20.01.2007)

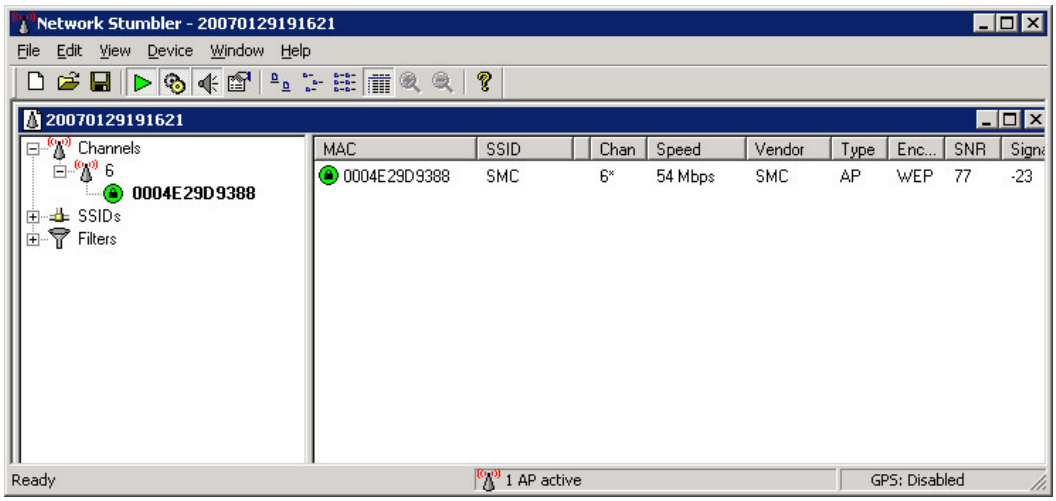

Abbildung 8: Grafische Oberfläche von Netstumbler

Alle diese Informationen erlangt Netstumbler indem es ein Paket an die Access-Points in Reichweite sendet, worauf diese antworten. In dieser Antwort findet sich unter anderem der Beacon-Frame des IEEE802.11 Protokolls. Wie bereits gezeigt, stehen in diesem alle Informationen die Netstumbler anbieten kann.
Da Netstumbler selber aktiv Pakete versendet, wird es auch als aktiver Scanner bezeichnet. Diese Tatsache, führt jedoch zu dem Nachteil, dass es von Netzwerkbetreibern aufgespürt werden kann [Rad04].

Kismet

Kismet ist ein Linux Opensource Projekt, welches kostenlos heruntergeladen werden kann.[2] Kismet bietet alle Funktionen von Netstumbler, ist allerdings etwas komplizierter zu bedienen und daher nicht unbedingt für Laien geeignet. Großer Vorteil von Kismet ist, dass es passiv arbeitet und somit nicht von Netzwerkbetreibern aufgespürt werden kann. Damit Kismet funktioniert, ist es jedoch notwendig eine Netzwerkkarte zu besitzen, welche im Monitormode betrieben werden kann. Monitormode bedeutet, dass die Netzwerkkarte selbst nicht am Netzwerkverkehr teilnimmt, sondern sie fängt alle Pakete in Reichweite ab, und kann somit alle Daten abhören und verwenden. Dies geschieht unabhängig davon, für welches Netzwerkgerät die Pakete ursprünglich bestimmt waren. Neben der Tatsache, dass es nicht aufgespürt werden kann, ist Kismet außerdem in der Lage die Verwendung von beispielsweise Netstumbler aufzuspüren[Rad04].
Besonders erwähnenswert ist die Tatsache, dass Kismet herausfinden kann ob ein Access-Point mit den herstellerspezifischen Einstellungen konfiguriert ist. Sollte dies der Fall sein, so stellt Kismet den Access-Point gesondert da und bietet dem Angreifer nun die Basis um einen solchen Access-Point zu hacken und dann zu manipulieren. Daher ist es extrem wichtig, den werksseitig eingestellten Zugang zum Konfigurationsmenü sofort zu ändern.

[2] http://www.kismetwireless.net/ (03.03.2007)

6.2 Sniffer

Sniffer dienen dazu, den kompletten Netzwerkverkehr aufzuzeichnen und darzustellen. Dabei ist es unwichtig um welche Art von Netzwerk es sich handelt. Im wesentlichen gibt es zwei weit verbreitete, kostenlose Programme: Wireshark (ehemals Etherreal) und Ettercap. Neben dieses existieren auch professionelle und kommerzielle Tools [Rec04]. Beispielsweise bieten die Firmen Network General [3] und WildPackets [4] solche Professionelle Systeme an. Auf Grund fehlender Lizenzen konnte jedoch keines dieser Programme getestet werden.

Wireshark

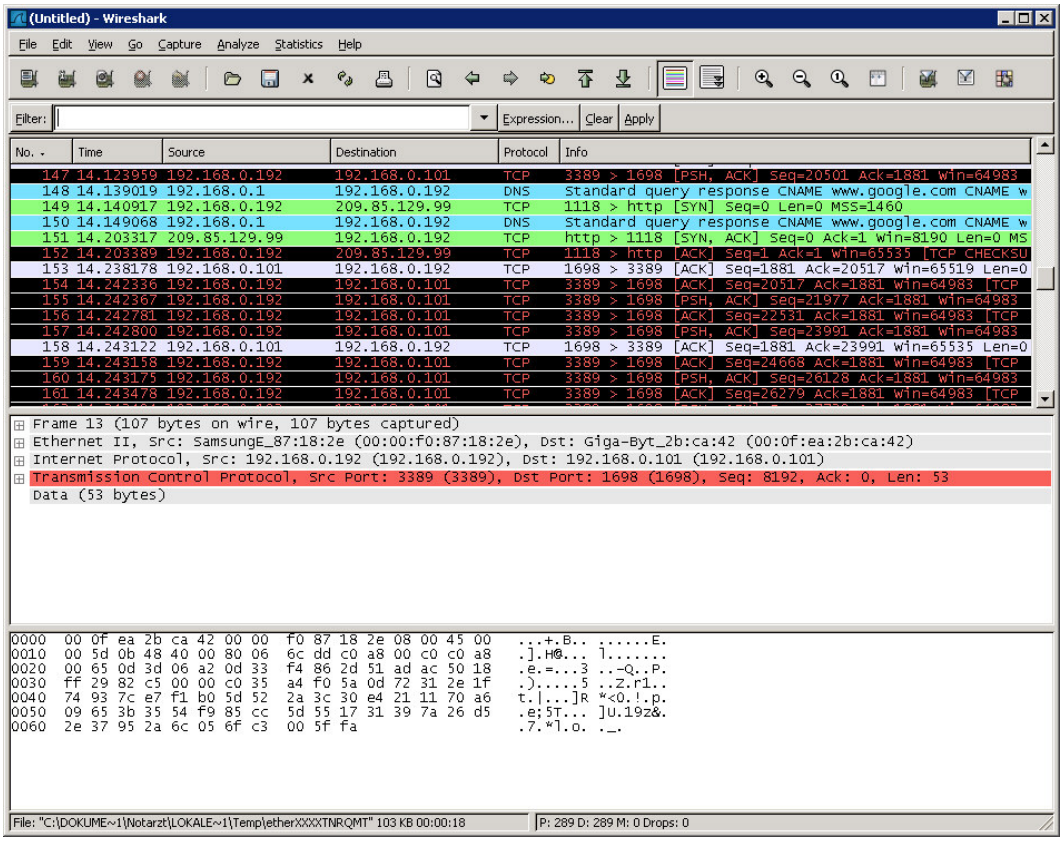

Abbildung 9: Grafische Oberfläche von Wireshark

Wireshark ist ein Opensource Projekt, welches sowohl für Linux als auch für Windows kostenlos zum Download [5] bereit steht. Wireshark ist aus dem Programm Etherreal [6] entstanden und führt dessen Funktionen fort. Aktuell steht sowohl eine Etherreal Version, welche wahrscheinlich jedoch nicht weiterentwickelt wird, als auch eine Wireshark Version zum Download bereit. Wireshark bietet dem Anwender die Möglichkeit den kompletten Netzwerkverkehr

[3] http://www.networkgeneral.com/ (10.03.2007)
[4] http://www.wildpackets.com/ (11.03.2007)
[5] http://www.wireshark.org/ (10.01.2007)
[6] http://www.ethereal.com/ (10.01.2007)

aufzuzeichnen und gegebenenfalls in einer Datei zu speichern. Verschlüsselte Übertragungen können zwar aufgezeichnet werden, jedoch nur die bereits verschlüsselten Pakete. Sobald Pakete aufgezeichnet wurden, können diese mittels diverser Filter sortiert und durchsucht werden. Somit ist es relativ einfach gesuchte Daten zu finden. Da einige Passworte, beispielsweise bei FTP Servern oder POP3 Servern, im Klartext übertragen werden können diese Passwörter mit Hilfe von Wireshark direkt ausgelesen werden.
Für die Analyse von W-Lans sehr wichtig ist, dass Wireshark im Monitor Mode betrieben werden kann und somit mit Hilfe von passenden Netzwerkkarten alle empfangenen Pakete aufgezeichnet werden können [Rad04].

Ettercap

Ettercap ist ebenfalls Opensource und steht auch für diverse Betriebssysteme kostenlos zur Verfügung [7]. Ettercap bietet nahezu den gleichen Funktionsumfang wie Wireshark. Ettercap bietet außerdem explizit die Möglichkeit Benutzerdaten von sehr vielen gängigen Netzwerkprotokollen wie, HTTP, FTP, POP, SSH1, ICQ, MySQL, NNTP, X11, NAPSTER, IRC, IMAP 4 und diversen anderen zu sammeln. Neben den vielfältigen Aufzeichnungsfunktionen bietet Ettercap noch die Möglichkeit selbst Pakete zu versenden und Verbindungen zwischen anderen Clients zu beenden. Somit kann Ettercap dazu verwendet werden Man-in-the-Middle Attakten vorzubereiten [Rad04].
Durch das Scannen des Netzwerkes können zudem Informationen über Typ, offene Ports, Betriebssysteme und Serverdienste von allen angeschlossenen Hosts erlangt werden. Nach [Wiki2] wird Ettercap auf Grund der gerade gezeigten Funktionen von vielen Firmen als sehr gefährlich eingestuft.

6.3 Spoofer

Zur Kategorie Spoofer gehören Programme mit deren Hilfe die Identität eines Netzwerkclients verändert werden können. Diese Täuschung kann sich auf diverse Punkte (Beispiele: IP-, ARP-,DNS-, MAC-Spoofing)beziehen. Im folgenden geht es jedoch nur darum, die MAC-Adresse eines Clients zu verändern. Es wird also nur MAC-Spoofing betrachtet.

SMAC

SMAC ist ein Freeware Tool, welches für viele Windows Versionen kostenlos zum Download [8] bereit steht. Es dient dazu die MAC-Adressen beliebiger Netzwerkgeräte anzuzeigen und zu verändern. Diese Veränderungen werden sofort wirksam und sind somit sehr leicht durchzuführen. SMAC ist, wie alle anderen MAC-Spoofer auch, nicht in der Lage die MAC-Adresse permanent zu ändern. Sie wird nur von der Software überschrieben und wird bei jedem Neustart wieder auf den ursprünglichen Wert zurückgesetzt. SMAC kann dazu verwendet werden, den MAC-Filter eines Netzwerkes zu testen oder auch um diesen zu umgehen.

[7] http://ettercap.sourceforge.net/ (11.01.2007)
[8] http://www.klcconsulting.net/smac/ (16.01.2007)

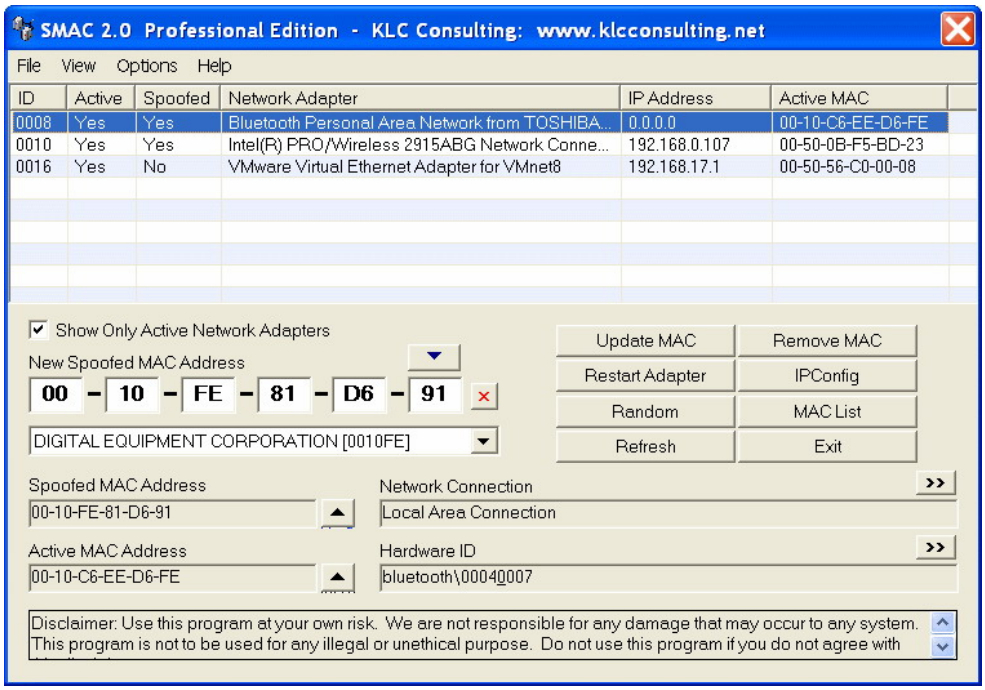

Abbildung 10: Grafische Oberfläche von SMAC

6.4 WEP-Crack

Die im folgenden beschriebenen Programme dienen alleine dem Zweck, den WEP-Key eines Netzwerkes zu berechnen. Dazu ist es notwendig „interessante“ Pakete zu analysieren. Solche Pakete sind Pakete, bei denen die Struktur Rückschlüsse auf den Schlüssel zulässt. Solche Pakete haben beispielsweise den Wert 255 im zweiten Byte stehen [BSI05].

AirSnort

AirSnort ist ein kostenloses Tool mit dessen Hilfe der WEP-Key in IEEE 802.11 Netzwerken errechnet werden kann. Es steht kostenlos für diverse Plattformen zur Verfügung [9]. Voraussetzung für die Verwendung von AirSnort ist eine Netzwerkkarte, welche im Monitormode und mit speziellen Treibern betrieben werden kann [10]. Um einen WEP-Key zu berechnen, hört AirSnort den kompletten Netzwerkverkehr ab und kann nach einer ausreichend großen Anzahl an empfangenen Paketen den WEP-Schlüssel berechnen. Zur Berechnung sind ca. 5-6 Millionen Pakete notwendig. Wie lange es dauert 5-6 Millionen Pakete zu sammeln hängt zum einen davon ab, welcher Netzwerkstandard verwendet wird und wie groß die einzelnen Pakete sind. Die Größe der Pakete hängt im Wesentlichen von der aktuellen Anwendung und der Verbindungsqualität ab. Je schlechter diese ist, desto kleiner werden die Pakete. Weiter ist es sehr entscheidend, wie stark das Netzwerk ausgelastet wird. Sollte ein Netzwerk nur

[9] http://airsnort.shmoo.com/ (16.01.2007)

[10] Liste der unterstützen Netzwerkkarten: http://www.tectic.de/articles/airsnort.pdf (15.01.2007)

sehr wenig verwendet werden, so dauert es wesentlich länger den WEP-Key zu berechnen, als wenn permanent Daten über das Netzwerk transportiert werden. Wie lang die Berechnung ungefähr dauert, ist in den Abbildungen 11 12 zu erkennen [BSI03].

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

Abbildung 11: Benötigte Zeit in Abhängigkeit von der Datenmenge und der durchschnittlichen Netzwerkauslastung [BSI03]

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

Abbildung 12: Datenmenge im Abhängigkeit zur durchschnittlichen Paketgröße und der Anzahl der Pakete [BSI03]

Neue Verfahren zur Berechnung des WEP-Keys

Neben den passiven Verfahren den WEP-Key zu errechnen, existieren in der Zwischenzeit Verfahren mit denen es in deutlich kürzerer Zeit möglich ist den WEP-Key zu knacken. Tools, welche diese Verfahren implementieren benötigen inzwischen nur noch ungefähr 100MB Traffic um den Schlüssel zu berechnen . Außerdem existieren auch Verfahren und Tools die aktiv dazu beitragen, Netzwerktraffic mittels Re-Injection zu erzeugen und so noch schneller an den Schlüssel zu gelangen [BSI05].
Ein Tool, welches diese neuen Verfahren implementiert, ist AirCrack. Es kann

kostenlos runtergeladen [11] werden und läuft am besten unter Linux. Unter Windows ist mit eingeschränktem Funktionsumfang lauffähig, jedoch läuft auch Aircrack nur mit bestimmten Netzwerkkarten [12]. Aircrack ist nicht nur ein Programm sondern eine komplette Sammlung, mit deren Hilfe es möglich ist, alle IEEE 802.11 Sicherheitsmechanismen von Grund auf zu testen. Letztendlich, übernimmt Aircrack dabei die Funktionen aller in diesem Kapitel vorgestellten Gruppen von Analysewerkzeugen.
Erwähnenswert ist die Tatsache, dass AirCrack sogar in der Lage ist WPA verschlüsselte Netzwerke anzugreifen. Dies ist bis dato jedoch nur per Bruteforce möglich und liefert somit bei geschickt gewähltem Schlüssel in absehbarer Zeit kein verwertbares Ergebnis [Wiki3].

6.5 Zusammenfassung der Analysewerkzeuge

Neben den gezeigten Programmen existieren noch viele weitere Programme mit deren Hilfe Netzwerke analysiert und angegriffen werden können. Da diese jedoch entweder nicht sonderlich bekannt sind, kostenpflichtig sind oder im Funktionsumfang sehr den gezeigten Programmen ähneln, werden sie hier nicht alle aufgezählt und vorgestellt. Sehr wichtig zu erkennen ist, dass es durch die Verwendung von einem oder mehrerer der vorgestellten Programme relativ leicht möglich ist, die ursprünglichen Sicherheitsmechanismen von IEEE 802.11 zu umgehen. Besonders WEP bietet bei einem Angriff mit dem richtigen Werkzeug nur sehr wenig Schutz und ist in kürzester Zeit umgangen.
Es ist also dringend zu empfehlen auf neuere Verschlüsselungen zurückzugreifen. Sollte auf WPA zurückgegriffen werden, ist es sehr wichtig, dass ein guter Schlüssel verwendet wird, welcher einigermaßen resistent gegen Wörterbuch und Bruteforce Attacken ist [BSI05].

[11] http://freshmeat.net/projects/aircrack/ (21.02.2007)
[12] http://www.tuto-fr.com/tutoriaux/en-carte-wifi-crack-wep-usb-pci-pcmcia.php (21.02.2007)

7 Einrichten eines sicheren W-Lans

Wie bereits gezeigt, ist ein Wireless LAN von Hause aus eher unsicher, das bedeutet, es müssen einige Einstellungen am W-LAN vorgenommen werden, damit dieses dem gewünschten Sicherheitsstandard entspricht.
Die dazu notwendigen Einstellungen müssen teilweise am verwendeten Router und teilweise auch an allen Clients vorgenommen werden. Welche Mechanismen es gibt und wie sicher sie sind, wurde bereits gezeigt. In diesem Kapitel geht es nun darum, zu zeigen, wie die Mechanismen eingerichtet und verwendet werden. Zunächst wird gezeigt, welche Einstellungen am Router vorgenommen werden müssen. Im zweiten Teil geht es dann um die Einrichtung der verwendeten Clients.

7.1 Routerseite

Für diese Anleitung wurde ein Linksys WRT54GL-DE Router [13] verwendet. Somit können die im weiteren gezeigten Schritte in einigen Details bei anderen Routern anders aussehen oder eventuell nur bedingt oder gar nicht zu Verfügung stehen. Vorteil des verwendeten Linksys Routers ist, dass er über eine freie Firmware verfügt und somit mit diversen modifizierten Firmwares verwendet werden kann. Die wichtigsten Firmwares sind: Free-WRT [14], OpenWRT[15], HyperWRT[16], Alchemy/Talismen[17] und DD-WRT[18]. Da jede Firmware einen unterschiedlichen Funktionsumfang bereit stellt, muss man bei der Wahl einer Firmware darauf achten, dass sie alle benötigten Funktionen zur Verfügung stellt. Da in dieser Arbeit das Hauptaugenmerk auf der sicheren Kommunikation über W-LAN liegt und in Kapitel 5.4 gezeigt wurde, dass VPN-Verbindungen ein sehr hohes Maß an Sicherheit bieten, sollte die Firmware die Möglichkeit bieten einen VPN-Server auf dem Router laufen zu lassen. Somit können dann VPN-Tunnel zwischen Clients und dem Router aufgebaut werden. Zudem sollten natürlich auch Maßnahmen wie WPA, WPA2, MAC-Filter weiterhin zu Verfügung stehen. Die letztgenannten Funktionen werden von allen verfügbaren Firmwares unterstützt. Auf Grund des vorhandenen VPN-Serveres und der umfangreichen Dokumentation [19] fiel die Wahl auf DD-WRT.

7.1.1 Vorbereitungen vor dem Flashen

Bevor damit begonnen werden kann den Router zu flashen, muss erst einmal die gewünschte Firmware heruntergeladen werden. Die gewählt DD-WRT Software kann kostenlos auf der Herstellerhomepage heruntergeladen werden. Sie steht dem User in verschieden Versionen zur Verfügung. [20] Ziel ist es, den Router

[13] www.linksys.com/de/ (02.02.2007)
[14] http://www.freewrt.org (10.12.2006)
[15] http://www.openwrt.org (10.12.2006)
[16] http://www.hyperwrt.org (10.12.2006)
[17] http://www.sveasoft.com/ (10.12.2006)
[18] http://www.dd-wrt.com (10.12.2006)
[19] http://www.dd-wrt.com/wiki/index.php/Main_Page (16.03.2007)
[20] http://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F (18.03.2007)

mit der VPN-Version zu betreiben. Somit muss diese Version heruntergeladen werden. Zudem ist es aber auch notwendig die Standard Version runterzuladen. Warum dieses notwendig ist, wird im nächsten Abschnitt beschrieben. Damit man eine neue Firmware auf den Router flashen kann, muss dieser in den Auslieferungszustand zurückversetzt werden. Dies geschieht indem man die Reset-Taste auf der Rückseite des Gerätes für 30 Ssekunden gedrückt hält. Weiterhin sollte nur noch ein Client, nämlich der, von dem geflasht werden soll, mit dem Router verbunden sein. Außerdem sollte der Router auch vom Internet getrennt werden.

7.1.2 Flashen der Firmware

Da der Router vor dem Flashen mit der original Linksys Software versehen ist, und diese als Update maximal 3MB große Images erlaubt, die gewünschte Version DD-WRT-VPN jedoch größer ist, muss man zunächst ein Zwischenschritt machen und die Standardversion von DD-WRT auf den Router flashen. Erst danach kann man dann eine beliebig große Firmware auf dem Router installieren. Der Router ist bereits auf die Werkseinstellungen zurückgesetzt, somit kann man mit dem Flashen beginnen. Dazu ruft man das Web-Konfigurationsmenü unter der Routeradresse(http://192.168.1.1) auf. Dies geschieht indem man in einem beliebigen Web-Browser (am besten jedoch Internet Explorer) die Routeradresse eingibt und sich mit dem Standardbenutzerdaten anmeldet. In dem nun erscheinenden Menü findet man unter *Administration* die Option *Firmwareupdate*. In diesem Unterpunkt kann man nun die zu flashende Datei, hier die Standardversion von DD-WRT, auf der Festplatte angeben und dann auf *Firmwareupdate* klicken. Danach wird die neue Software installiert. Nach erfolgreichen Flashen startet der Router automatisch neu. Während dieses Vorganges, welcher mehrere Minuten dauern kann, darf man den Router nicht Ausschalten oder Neustarten. Nach dem Neustart kann man das neue Konfigurationsmenü der DD-WRT Software zum ersten man benutzen.
Da bis jetzt nur die Standardversion von DD-WRT installiert ist, wird die Software direkt auf die VPN-Version geupdatet. Dieser Schritt läuft im Prinzip genauso ab wie der erste Updatevorgang. Man setzt den Router auf die Werkseinstellungen zurück, und kann danach im Webkonfigurationsmenü unter *Administration -> Firmware Update* den Updatevorgang starten. Hierzu gibt man nun die zuvor heruntergeladene Datei der VPN-Version an und klickt auf Update.

Genau wie beim ersten Mal arbeitet der Router wieder einige Minuten und darf während dessen nicht ausgeschaltet oder neu gestartet werden. Wenn auch dieses Update erfolgreich ausgeführt ist, startet der Router erneut neu. Ab jetzt ist die gewünschte Software installiert und alle Optionen können eingerichtet und verwendet werden.

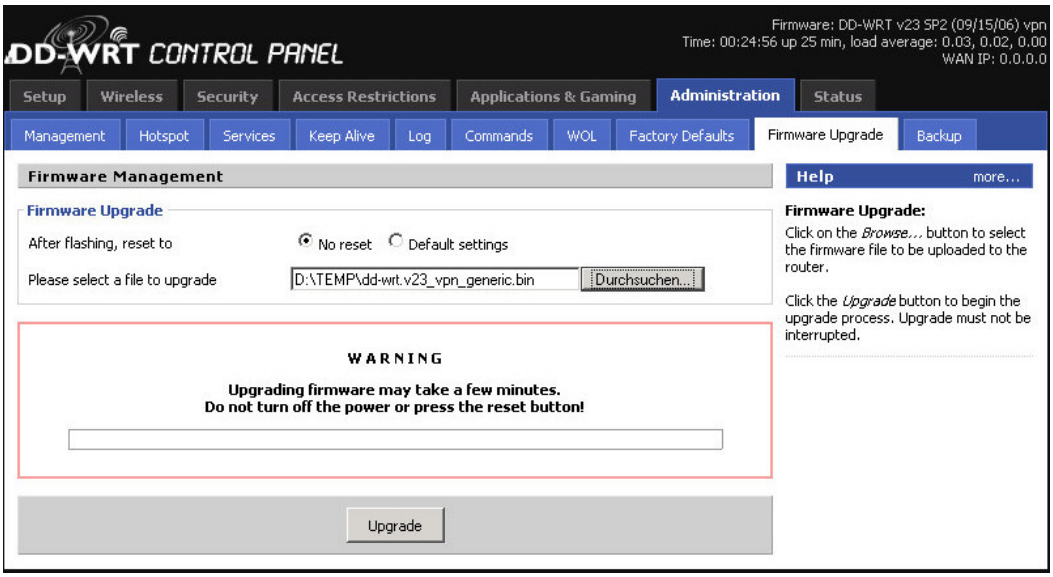

Abbildung 13: DD-WRT Webinterface - Firmwareupdate

7.1.3 Einstellen des Routers

Neben den bereits vorgestellten Sicherungsmechanismen, sollten noch weitere Punkte beachtet werden, damit ein Netzwerk als sicher eingestuft werden kann. Damit ein Router richtig arbeiten kann, müssen natürlich noch weitere Parameter für Internetverbindung, Firewall und so weiter eingeben werden. Diese Punkte werden hier jedoch nicht weiter erläutert.

Grundlegende Sicherheits-Einstellungen

Die wichtigsten Einstellungen findet man im Menüpunkt *Administration-> Management*.

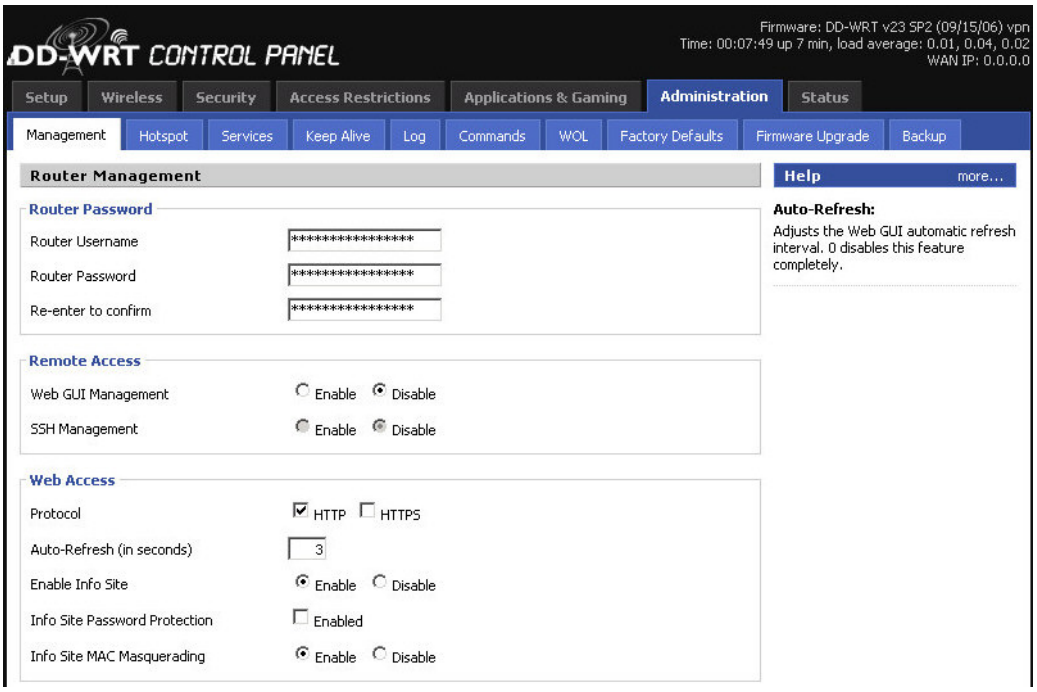

Abbildung 14: Webinterface - Router Management

- Benutzername und Passwort ändern
  Unter dem Punkt *Router-Passwort* kann der voreingestellte Benutzer geändert werden. Dies ist sehr wichtig, da es wie in Kapitel 6.1 gezeigt, Programme gibt, die feststellen können ob noch die werkseitig eingestellten Benutzerdaten verwendet werden. Diese Änderung stellt somit eine notwendige Maßnahme dar, damit der Router vor Angriffen und Manipulationsversuchen geschützt ist. Wie sichere Passwörter aussehen, wird hier nicht näher erläutert, jedoch sollten sie möglichst lang und möglichst zufällig sein.

- Webzugriff
  Unter *Webzugriff* wird der Zugang zum Webkonfigurationsmenü geregelt. Es ist sinnvoll nur https (HyperText Transfer Protocol Secure) Verbindungen zuzulassen, da diese Verbindungen verschlüsselt sind und somit ein höheres Maß an Sicherheit bieten. Weiterhin ist es sinnvoll die Info-Seite zu deaktivieren damit keine, möglicherweise kritischen Daten, ungewollt für Angreifer ersichtlich sind. Außerdem sollte allen W-LAN Client der Zugang zum Konfigurationsmenü versperrt werden. Dies geschieht im Menüpunkt *W-LAN -> Erweiterte Einstellungen*. Sobald die Option *Wireless GUI Access* deaktiviert ist, dürfen Clients, welche per W-LAN mit dem Router verbunden sind, nicht mehr auf das Konfigurationsmenü zugreifen.

- Remote Konfiguration
  Im Punkt *Remote Konfiguration* kann man einstellen, ob und wenn ja, wie der Router von außerhalb konfiguriert werden darf. Es ist ratsam die komplette Remotekonfiguration zu deaktivieren und Angreifern so keine Möglichkeit zu bieten von außen Schaden anzurichten.

- IP des Routers ändern / DHCP deaktivieren

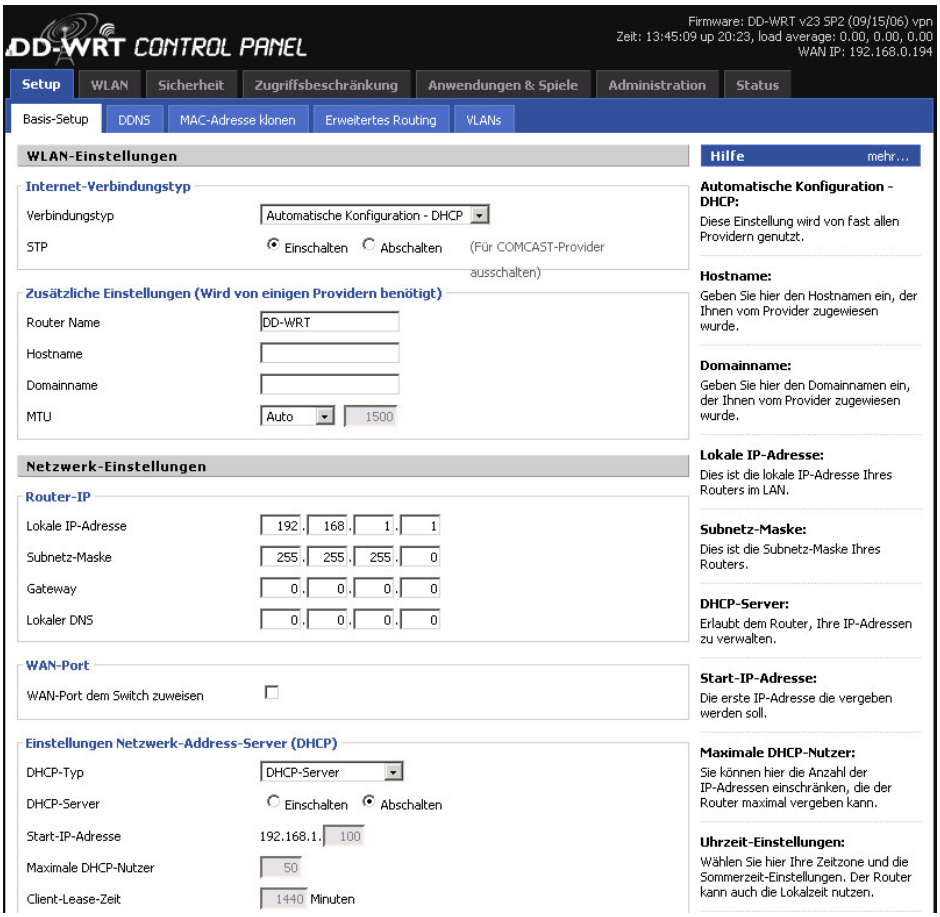

Abbildung 15: Webinterface - Netzwerkbasiseinstellungen

Die IP des Routers wird im Menüpunkt *Setup-> Basis Setup* unter dem Punkt *Router-IP* eingestellt. Die IP sollte geändert werden, damit es Angreifer nicht so leicht gemacht wird, den Router zu manipulieren. Um Komplikationen zu vermeiden, sollte jedoch weiterhin eine IP aus der IP Range 192.168.xxx.xxx gewählt werden. Alle verbundenen Clients müssen später ebenfalls eine IP aus der gleichen Range wie der Router zugewiesen bekommen (entweder manuell oder per DHCP). Weiter ist es sehr sinnvoll den im Router integrierten DHCP (Dynamic Host Configuration Protocol) Server zu deaktivieren. Dieser Server dient dazu jedem angemeldeten Client automatisch eine IP, die richtige Subnetzmaske und den benötigten Gateway zuzuweisen. Die DHCP Optionen finden

sich ebenfalls in Menü *Setup -> Basis Setup* unter dem Punkt *Einstellungen Netzwerk-Address-Server (DHCP)*. Wenn dieser deaktiviert ist, werden Clients die sich am Router anmelden keine IPs, Subnetz-Masken und der Standard Gateway mehr automatisch zugewiesen. Diese Werte müssen nun manuell an jedem Client eingestellt werden. Das Deaktivieren des DHCP Servers bedeutet einen etwas höheren Konfigurations- und Wartungsaufwand, da jeder Client mit einer eindeutigen, noch nicht verwendeten IP versehen werden muss. Andererseits wird es Angreifer allerdings auch deutlich erschwert eine gültige IP Adresse zu bekommen und dann an der Netzwerkkommunikation Teil zu nehmen.

W-LAN Sicherungsmechanismen

Nachdem nun alle Grundlegenden Einstellungen am Router vorgenommen sind, kann damit begonnen werden das W-LAN einzurichten. Die dazu notwendigen Einstellungen finden sich im Menüpunkt *WLAN*.

- Basiseinstellungen

Abbildung 16: Webinterface - W-LAN Basiseinstellungen

Im Unterpunkt *Basis-Einstellungen* gibt es die Möglichkeit einige generelle Einstellungen zu bearbeiten. Zum einen kann man den W-LAN Modus sowie Kanal- und Netzwerkmodus wählen. Weitaus wichtiger ist jedoch die Möglichkeit hier die SSID zu ändern und deren Broadcast zu verhindern. Wie bereits gezeigt, sollte man nicht die Standard SSID verwenden sondern eine neue, welche keine Rückschlüsse auf den Betreiber oder den Zweck des Netzwerkes lässt. Zudem sollte auch der SSID Broadcast deaktiviert werden. Während der Einrichtung des Netzwerkes ist es jedoch ratsam den SSID-Broadcast aktiviert zu lassen und diesen erst zu deaktivieren nachdem das Netzwerk komplett eingerichtet wurde.

- W-Lan Sicherheit

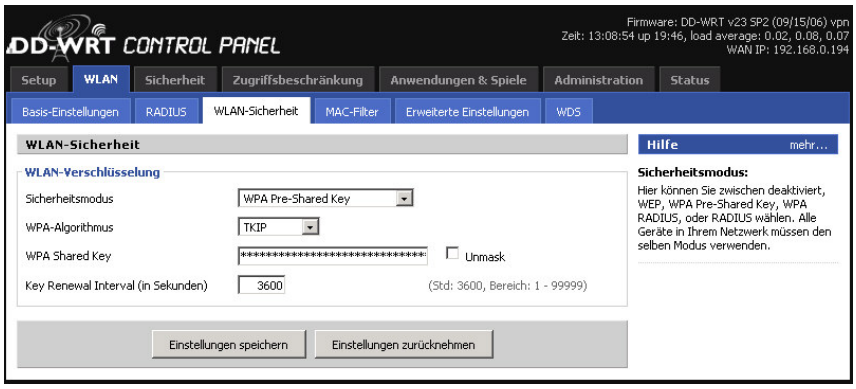

Abbildung 17: Webinterface - W-LAN Sicherheitseinstellungen

Im Unterpunkt *W-LAN Sicherheit* wird eingestellt welches Verschlüsselungsverfahren verwendet werden soll. Weiter kann noch der verwendete Schlüssel eingeben werden. Wie bereits gezeigt, sollte möglichst WPA oder gar WPA2 verwendet werden. Hier wird nun WPA2 Pre Shared Key gewählt. Beim Verschlüsselungsverfahren wird bestenfalls AES verwendet, aus Kompatiblitätsgründen kann jedoch auch auch TKIP + AES verwendet werden. In diesem Falle wird AES verwendet, sobald es vom Client unterstützt wird. Anderenfalls wird TKIP verwendet. Als letztes muss nun noch ein Schlüssel eingegeben werden.
Bei WPA und WPA2 darf dieser zwischen 8 und 63 ASCII Zeichen lang sein. Auch dieser Schlüssel sollte clever und sicher gewählt werden. Da im weiteren Verlauf jeder Client den zuvor eingestellten Schlüssel kennen muss, ist es ratsam den Schlüssel in einer Datei (.txt, .doc, ...) zu speichern und die Datei mittels CD, Diskette, USB-Stick allen Clients zur Verfügung zu stellen. Es ist allerdings darauf zu achten dass der Schlüssel nur während der Konfigurationsphase ungeschützt in einer Datei gespeichert bleibt und nach Abschluss der Einrichtung wieder gelöscht wird.

- Mac-Filter

Abbildung 18: Webinterface - W-LAN Mac-Filter

Im Unterpunkt *Mac-Filter* kann nur noch der Mac-Filter aktiviert werden. Dieser Filter bietet entweder die Möglichkeit Mac-Adressen anzugeben, denen der Zugang verweigert oder gewährt wird. Da es in den meisten Netzwerken relativ wenige zugelassen Clients gibt, ist es wesentlich sinnvoller die Adressen anzugeben denen der Zugang nicht verweigert werden soll. Dazu wird die Option *WLAN-MAC-Adressen, die auf das Netzwerk zugreifen dürfen* aktiviert. Mit einem Klick auf *Mac-Filter Liste editieren* öffnet sich ein neues Fenster indem die Mac-Liste editiert werden kann.

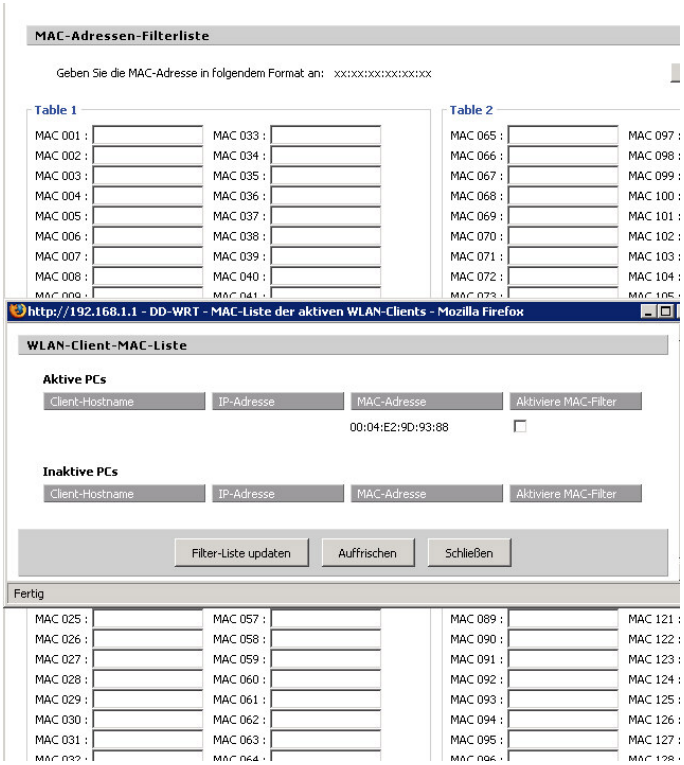

Abbildung 19: Webinterface - Mac Filterliste

Hier gibt es entweder die Möglichkeit die Adressen manuell per Hand einzugeben (Mac-Adresse eines Clients rausfinden siehe Kapitel 7.2.1) oder alternativ können die Mac-Adressen aller, oder beliebig vieler, am Netzwerk angemeldeten Clients automatisch in die Liste übernommen werden. Dies geschieht durch klicken auf *Mac-Liste W-LAN Clients*.
Im sich nun öffnenden Fenster werden alle angemeldeten Clients angezeigt und können durch setzen eines Häkchens und anschließendem klicken auf *Filterliste updaten* in die Liste aufgenommen werden. Da die automatische Option wesentlich leichter ist, dazu jedoch die Clients bereits mit dem Netzwerk verbunden sein müssen, empfiehlt es sich den Mac-Filter erst zu konfigurieren, nachdem alle Clients fertig konfiguriert sind. Weiterhin bleibt es jederzeit möglich neue Clients manuell in die Liste aufzunehmen oder auch Clients aus der Liste zu entfernen.

Virtual Private Network

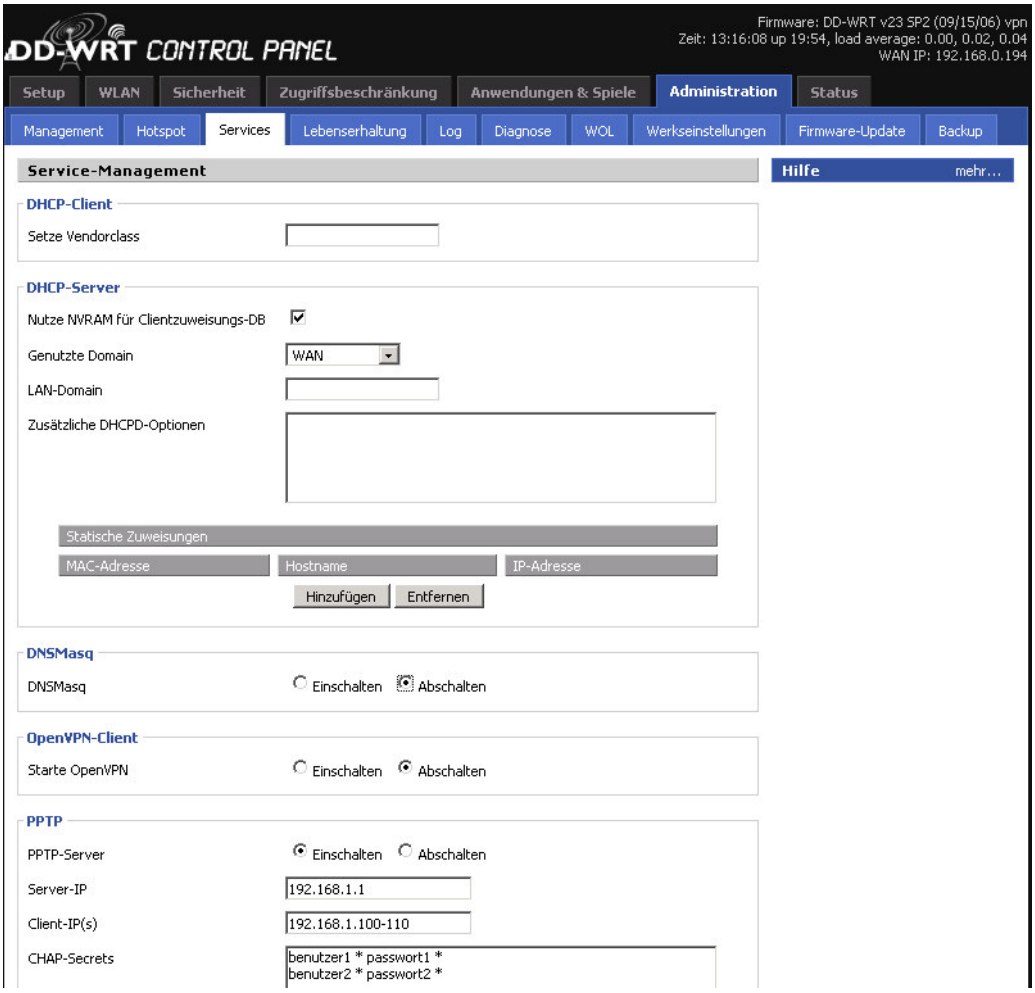

Abbildung 20: Webinterface - VPN Server

Damit Verbindungen zwischen Router und Clients per VPN getunnelt, und somit verschlüsselt, werden können, muss der VPN Server gestartet werden und Benutzerkonten für diesen eingerichtet werden. Unter *Administration -> Services* findet sich der Punkt PPTP. Hier kann der VPN Server konfiguriert werden. Dazu muss eine Server IP eingeben werden, welche Sinnvollerweise die gleiche ist wie die IP des Routers selber. Außerdem müssen Client-IPs, also IPs welche angemeldeten Clients zugewiesen werden, angeben werden. Diese IPs sollten in der gleichen Range liegen wie der Router. Benutzer und Passwörter müssen im Eingabefeld *CHAP-Secrets* eingegeben werden. Dabei ist es wichtig, dass nur ein Eintrag pro Zeile eingeben wird und Benutzerkonten mit folgender Syntax eingeben werden:

```
benutzer1 * passwort1 *
benutzer2 * passwort2 *
```

Bis auf den Mac-Filter, welcher erst später eingeschaltet wird, ist der Router nun komplett eingerichtet und kann so verwendet werden. Jetzt können die Clients konfiguriert und mit dem Router verbunden werden. Welche Schritte dazu notwendig sind, wird im nächsten Kapitel gezeigt.

7.2 Clientseite

Alle Schritte die im folgenden gezeigt werden, gelten fürs Clients auf denen Microsoft Windows XP-Professional SP2[21] als Betriebssystem installiert ist. Bei Clients auf denen ein anderes Betriebssystem läuft, können die einzelnen Schritte mehr oder weniger von den gezeigten abweichen.

7.2.1 Mac Adresse des eigenen Rechners rausfinden

Wie bereits in Kapitel 4.4 gezeigt, sind MAC-Adressen weltweit eindeutig und jedes Netzwerkgerät besitzt eine solche. Bei vielen Laptops oder anderen Netzwerkgeräten ist es inzwischen üblich, dass die MAC-Adresse(n) außen auf dem Gerät angebracht ist. Dies ist eine Möglichkeit um die Mac-Adresse rauszufinden.
Darüberhinaus gibt es aber noch die Möglichkeit die Adresse von Windows anzeigen zu lassen. Durch Eingabe von *cmd* unter *Start -> Ausführen* und anschließendes klicken auf *OK*, öffnet sich die Eingabeaufforderung von Windows. Hier muss nun *ipconfig/all* eingeben werden.

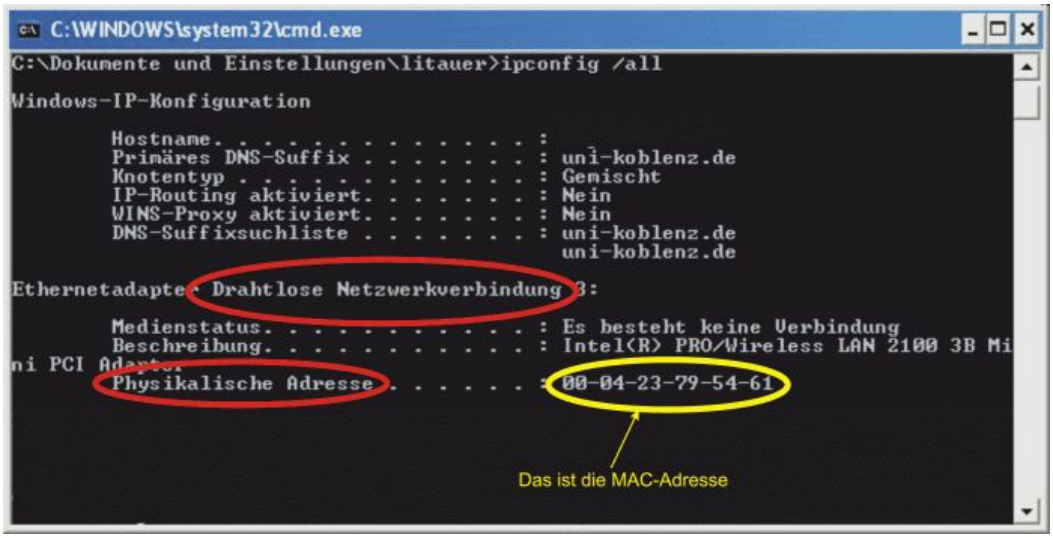

Abbildung 21: Anzeige von Netzwerkparametern [Uni]

Dadurch werden die Parameter aller sich im Rechner befindlichen Netzwerkgeräte angezeigt. Unter *Physikalische Adresse* findet sich die Mac-Adresse der

[21] http://www.microsoft.com/germany/windows/products/windowsxp/default.mspx (18.03.2007)

jeweiligen Netzwerkkarte. In vielen Rechnern befinden sich mehrere Netzwerkkarten, daher muss darauf geachtet werden, dass unter der richtigen Netzwerkkarte geschaut wird.

7.2.2 Einstellen einer IP Adresse

Wie bereits gezeigt, ist der DHCP Server des Routers deaktiviert, das bedeutet, ein Client bekommt keine IP zugewiesen, sondern muss manuell mit einer gültigen IP konfiguriert werden. Die Einstellungen finden sich unter *Start -> Einstellungen -> Netzwerkverbindungen.*

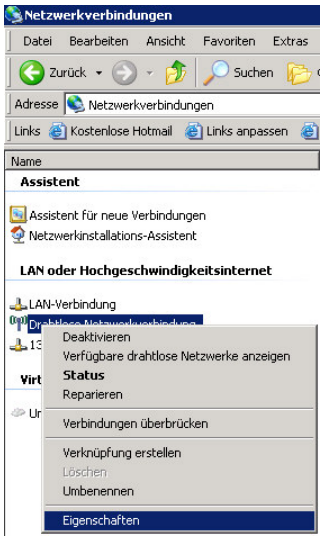

Abbildung 22: Eigenschaften von Drahtlose Netzwerkverbindung aufrufen

Durch einen Rechtsklick auf *Drahtlose Netzwerkverbindung* und anschließendes klicken auf *Eigenschaften*, öffnet sich das Dialogfeld *Eigenschaften von Drahtlose Netzwerkverbindung*

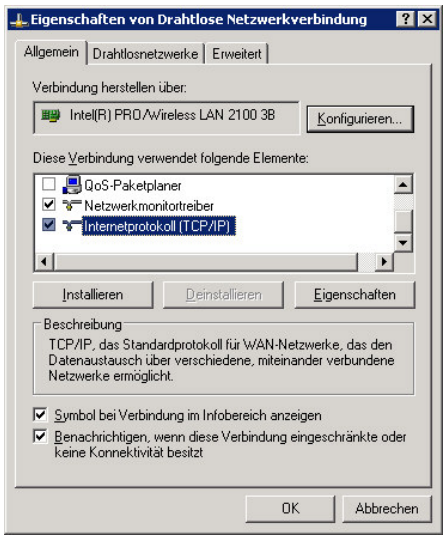

Abbildung 23: Eigenschaften von Drahtlose Netzwerkverbindung

Durch einen Doppelklick auf den Button *Internetprotokoll (TCP/IP)* unter *Diese Verbindung verwendet folgende Elemente* öffnet sich das Dialogfeld in dem die IP Adresse eingeben werden muss.

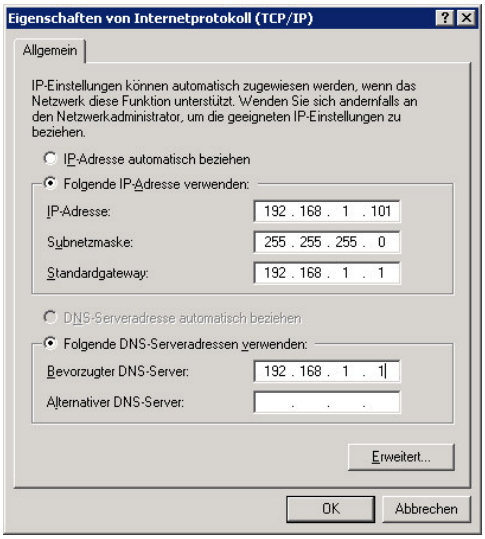

Abbildung 24: IP Adresse einer Netzwerkkarte einstellen

Damit diese gültig ist, muss sie aus derselben Range sein wie die IP des Routers. Die Subnetzmaske muss mit der Subnetzmaske des Routers übereinstimmen, wird aber automatisch eingestellt. Zudem muss sowohl bei *Standardgateway* als auch bei *Bevorzugter DNS-Server* die IP des Routers eingetragen werden.

7.2.3 Verbinden mit dem Netzwerk

Zunächst einmal muss das gewünschte Netzwerk gefunden werden, damit eine Verbindung zu diesem hergestellt werden kann. Das gewünschte Dialogfeld findet sich unter *Start -> Einstellungen -> Netzwerkverbindungen -> Drahtlose Netzwerkverbindung.*

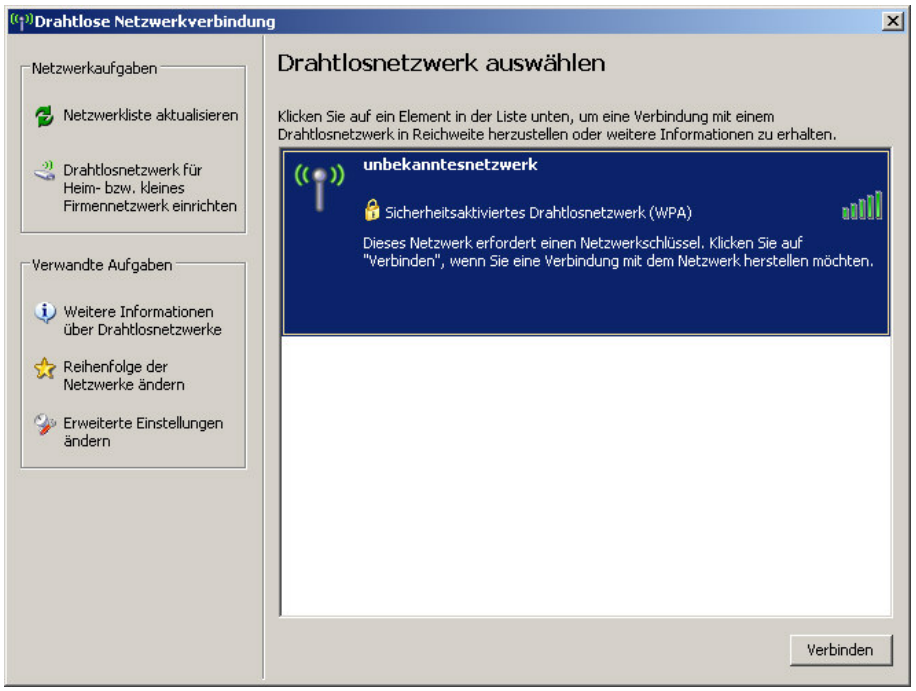

Abbildung 25: Dialogfenster Drahtlose Netzwerkverbindung

In diesem Dialogfeld werden alle verfügbaren und mit aktiviertem SSID Broadcast versehenen Netzwerke angezeigt. Ab jetzt unterscheiden sich die weiteren Schritte je nach dem ob die SSID gebroadcastet wird, oder nicht.

Aktivierter SSID Broadcast Durch klicken auf das gewünschte Netzwerk versucht sich der Client mit dem Netzwerk zu verbinden. Sollte das Netzwerk wie empfohlen, zuvor mit einer Verschlüsselung konfiguriert worden sein, so erscheint nun ein neues Eingabefenster in dem der zuvor festgelegte und im Router eingestellte Schlüssel eingeben werden muss. Durch einen weiteren Klick auf *Verbinden*, wird die Verbindung zum Netzwerk endgültig hergestellt.

Deaktivierter SSID Broadcast Da die SSID des Netzwerkes nicht gebroadcastet wird, wird das Netzwerk von Windows nicht angezeigt. Somit muss es manuell eingerichtet werden. Dies geschieht durch klicken auf *Erweiterte Einstellungen ändern*. Daraufhin öffnet sich das Dialogfeld *Eigenschaften von Drahtlose Netzwerkverbindung*(siehe Abbildung 23) in dem es einen Reiter *Drahtlosnetzwerke* gibt.

Unter *Bevorzugte Netzwerke* können die bisher verwendeten Netzwerke eingesehen und konfiguriert werden. Außerdem können neue Netzwerke

hinzugefügt werden. Dies geschieht durch klicken auf *Hinzufügen*.
Im dem sich nun öffnenden Fenster müssen alle relevanten Parameter wie SSID, Verschlüsselung und Schlüssel eingegeben werden. Durch klicken auf *OK* wird das Netzwerk gespeichert und kann ab sofort verwendet werden.

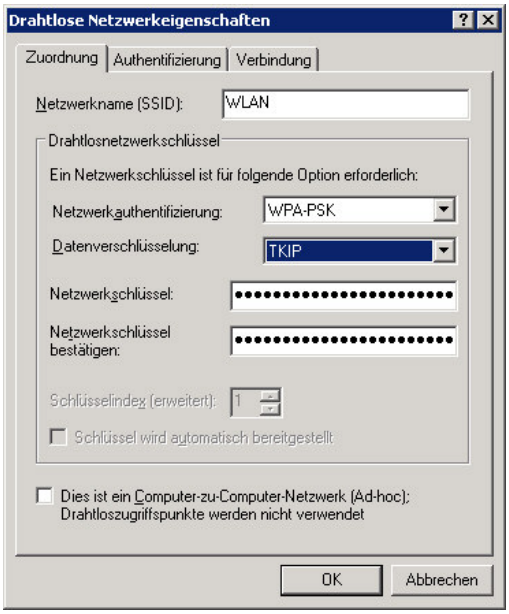

Abbildung 26: W-LAN mit deaktiviertem SSID Broadcast hinzufügen

Ab diesem Moment sind die Clients fertig konfiguriert. Beim Router müssen nur noch der MAC-Filter aktiviert und der SSID-Broadcast deaktiviert werden. Wenn auch diese Punkte erledigt sind, ist die Einrichtung eines sicheren W-LANs beendet und das Netzwerk kann verwendet werden.

8 Fazit

W-LANs finden aktuell immer mehr Zuspruch und werden nicht zuletzt auf Grund der in Kapitel 3.1 genannten Vorteile von immer mehr Privatpersonen sowie Firmen eingesetzt. Dies führt unweigerlich dazu, dass sensible Daten über Funkverbindungen transferiert werden. Leider sind diese Funknetzwerke von Haus aus nicht annähernd so sicher wie kabelgebundene Netzwerke.

Genau deshalb wurden im IEEE 802.11 Standard einige Mechanismen zum Schutz der Daten und des Netzwerkes eingeplant. Welche das sind wurde bereits in Kapitel 4 gezeigt. Vorteil dieser Mechanismen ist, dass sie uneingeschränkt auf jedem IEEE 802.11 Gerät in sehr kurzer Zeit eingrichtet und verwendet werden können. Leider entsprechen die Mechanismen nicht mehr dem aktuellen Stand der Technik und können somit dem Anwender auch keinen ausreichenden Schutz vor Angriffen bieten[BSI05]. Mit Hilfe der in Kapitel 6 vorgestellten Programme ist es relativ leicht möglich alle IEEE 802.11 Sicherungsmechanismen zu umgehen und sich somit Zutritt zum Netzwerk zu verschaffen. Daraus resultiert, dass in Bereichen in denen brisante Daten über W-Lans transportiert werden, diese Mechanismen nichts zu suchen haben und dringend durch neuere Sicherungsmechanismen ersetzt werden sollten. Allerdings gilt auch im privaten Bereich, dass ein Schutz mittels WEP und MAC-Filter nicht mehr ausreichend ist und auf neuere Mechanismen zurückgegriffen werden sollte.

Da der Industrie die Lücken im IEEE 802.11 Standard seit längerem bekannt sind, wurden bis heute eine Vielzahl von neueren Sicherheitsmechanismen (vorgestellt in Kapitel 5) entwickelt und teilweise standardisiert. Mechanismen wie WEPPlus und Fast Packet Keying müssen als Versuch alte Techniken zu verbessern, angesehen werden und bieten letztendlich keinen erweiterten Schutz gegenüber den IEEE 802.11 Sicherungsmechanismen. Daher werden sie auch nur sehr selten verwendet.
Der Standard IEEE 802.11i und seine Technologien WPA, AES-Verschlüsselung und Authentifizierung mittels IEEE 802.1x und EAP bieten dem Anwender sehr viel mehr Sicherheit. Weiterer Vorteil ist, dass sie dem Anwenden relativ wenig zusätzlichen Aufwand und Probleme bereiten. Sie können, spätestens nach einem Firmwareupdate, auf nahezu jedem IEEE 802.11 Gerät eingesetzt werden. Genau aus diesen Gründen ist im privaten Bereich ein Schutz mittels dieser Standards sicher aktuell die beste Wahl. Im Bereichen in denen sehr sensible Daten ausgetauscht werden, ist die Authentifizierung mit IEEE 802.1x sehr empfehlenswert bei der Datenverschlüsselung, sollte weiterhin über den Einsatz eines VPN nachgedacht werden [BSI05].

Virtual Private Networks bieten aktuell den besten Schutz in Sachen Datenverschlüsselung. Zudem kann bei ihnen der Verschlüsselungsgrad auf das Anwendungsgebiet angepasst werden. Im privaten Bereich ist ein VPN jedoch relativ schwer zu realisieren, da es sehr wenige IEEE 802.11 Router/Access Points gibt die einen VPN-Server zur Verfügung stellen. Somit ist das Haupteinsatzgebiet

von VPN weiter in der Industrie oder anderen großen Netzwerken zu sehen.

Die in Kapitel 7 beschriebene Anleitung zum Einrichten eines sicheren W-Lans bietet einen groben Überblick wie ein Betreiber eines W-LANs vorgehen kann um sein Netzwerk zu schützen. Die Einrichtung ist dabei nicht so komplex, dass sie von einen Experten vorgenommen werden muss, sondern nahezu jeder computerinteressierte Laie sollte in der Lage sein eine solche Einrichtung innerhalb von kurzer Zeit vorzunehmen. Sollten die beschriebenen Punkte beachtet werden, so bietet ein Funknetzwerk aus meiner Sicht besonders dem Privatanwender ein Maß an Sicherheit, was dem eines kabelgebundenen Netzwerkes ebenbürtig ist.

8.1 Ausblick

Wie bereits im Kapitel 2 kurz beschrieben, erfreuen sich W-LANs heute immer größerer Beliebtheit. Dies liegt nicht zuletzt an der sehr komfortablen Einrichtung und Bedienung. Genau aus diesem Grund kann davon ausgegangen werden, dass W-LANs in der Zukunft immer mehr Einsatzgebiete finden werden und somit das altbewährte Ethernet immer weiter verdrängen werden. Für den Anwender hat dies zur Folge, dass er immer leichter und kostengünstiger ein Funknetzwerk aufbauen wird können. Auf der anderen Seite bedeutet es jedoch auch, dass sich Anwender und besonders die Industrie immer mehr Gedanken um die Sicherheit in W-LANs machen müssen. Da aktuell keine neuen Sicherungsmechanismen vor der unmittelbaren Veröffentlichung stehen und bereits bestehende Mechanismen wie insbesondere IEEE 802.11i nach wie vor noch nicht der Standard sind, wird die nahe Zukunft wohl der besseren Verbreitung und Modifikation dieser bereits bestehenden Mechanismen gehören. Dieser Umstand stellt kein Problem dar, da nach [BSI03] und [Rec04] Verfahren wie WPA, AES, EAP und auch VPN derzeit als sehr sicher angesehen werden können und aktuell auch kein Anlass besteht hier neue Verfahren zu entwickeln. Wichtiger scheint die Tatsache, dass der Anwender dafür sensibilisiert werden muss, sorgfältig mit den technischen Möglichkeiten umzugehen und inbesondere sichere Passwörter und Schlüssel zu verwenden. In Bereichen in denen sehr sensible Daten transferiert werden, ist es sicher sinnvoll über die Verwendung eines VPNs nachzudenken oder noch besser dort auf den Einsatz von Funknetzwerken zu verzichten und stattdessen Ethernet einzusetzen.

Neben dem Sicherheitsproblem haben aktuelle W-LANs den Nachteil, dass ihre Übertragungsraten nach wie vor nicht mit denen kabelgebundener Lösungen konkurieren können. Als Lösung dieses Problemes könnte der Standard IEEE 802.11n dienen. Eine erste Version dieses Standards wurde Anfang 2006 verabschiedet. Er wird vom Enhanced Wireless Consortium (EWC)[22] weiterentwickelt und ständig verbessert. Dem EWC gehören inzwischen mehr als 70 Firmen an. Somit kann davon ausgegangen werden, dass dieser Standard auf jeden Fall weiterentwickelt wird. Als wichtigste Neuerung des IEEE 802.11n Standard muss die sogenannte MIMO Technik genannt werden [IRT06]. MI-

[22] http://www.enhancedwirelessconsortium.org/home (20.03.2007)

MO steht für Multiple-Input-Multiple-Output und verweist auf die Verwendung von mehreren Sende- und Empfangsantennen zur Steigerung der Übertragungsrate. Insbesondere die Übertragungsrate in größerer Entfernung soll durch MIMO deutlich angehoben werden. Somit soll es möglich werden konstantere Übertragungsraten, welche für Realtime Anwendungen wie beispielsweise IP-TV, VoIP oder Video Telefonie notwendig sind, zu gewährleisten. MIMO im eigentlichen Sinn, liefert keinen Ansatz zur generellen Steigerung der Übertragungsrate. IEEE 802.11i wird aber von manchen Herstellern als Deckmantel für die Anwendung von anderen Techniken zur Steigerung der Übertragungsrate verwendet. Dadurch besteht durchaus Hoffnung, dass IEEE 802.11i in Zukunft in allen Bereichen deutlich schneller werden wird, als die aktuellen Standards.
Da bis heute jedoch nur wenige Geräte mit IEEE 802.11n Unterstützung veröffentlicht worden sind, und diese auf Grund der noch nicht endgültigen Ratifizierung nicht notwendiger Weise mit dem fertigen IEEE 802.11n Standard funktionieren müssen [IRT06], bleibt abzuwarten wie sich dieser Standard weiter entwickeln wird.

Literatur

[Rec04] Rech, J.: „Wireless LANs - 802.11-WLAN-Technologie und praktische Umsetzung im Detail“. Hannover: Heise. 2004

[Sik01] Sikora, A. : „Wireless LAN - Protokolle und Anwendungen“. München: Addison-Wesley. 2001

[BSI05] Bundesamt für Sicherheit in der Informationstechnik: „Technische Richtlinie Sicheres WLAN. Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen“. Ingelheim: SecuMedia. 2005

[BSI03] Bundesamt für Sicherheit in der Informationstechnik: „Sicherheit im Funk-LAN - (WLAN, IEEE 802.11)“ http://www.netzmafia.de/skripten/netze/wlan_bsi.pdf (10.09.2006)

[Ott04] Otto, T.: „Studienarbeit - Netzwerkauthentifizierung im WLAN“ http://www.ibr.cs.tu-bs.de/arbeiten/schmidt/otto_eap/otto_eap.pdf (18.09.2006)

[Rad04] Rademacher M.: „Diplomarbeit - Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks“ http://www.m-lehrstuhl.de/mcommerce/veranstaltung/WS_2004_AG /Diplomarbeit%20-%20Sicherheits-%20und%20Schwachstellenanalyse %20entlang%20des%20Wireless-LAN-Protokollstacks.pdf (15.09.2006)

[Sha1] Shamir A., Mantin I. und Fluhrer S. : „Weaknesses in the Key Scheduling Algorithm of RC4“ http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (13.02.2007)

[IRT06] Institut für Rundfunktechnik: „MIMO-OFDM - Erhöhung von Performance und spektraler Effizienz bei Wireless-Systemen“ http://www.irt.de/IRT/publikationen/BlaueBerichte /Lipfert-MIMO7-fin-book.pdf (15.03.2007)

[Gol01] WLAN - Sicherheitslücke in WEP-Verschlüsselung geschlossen http://www.golem.de/0112/17523.html (17.01.2007)

[RSA01] „RSA Security Helps Create Solution to Secure Wireless LANs“ http://www.rsa.com/press_release.aspx?id=1135 (07.02.2007)

[Wiki1] http://de.wikipedia.org/wiki/IEEE_802.11 (12.09.2006)

[Wiki2] http://de.wikipedia.org/wiki/Ettercap (10.01.2007)

[Wiki3] http://de.wikipedia.org/wiki/Aircrack (15.01.2007)

[OSI1] http://www.hki.uni-koeln.de/people /schassan/teach/Bilder/Tanenbaum/Tanenbaum_7011_01-17.jpg (13.03.2007)

[Uni] http://www.uni-koblenz.de/GHRKO/pics/wlan/findmac (16.10.2006)