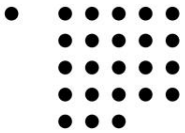


Fachhochschule Köln
University of Applied Sciences Cologne

Labor für Kommunikationstechnik und Datensicherheit

Konzept eines WLAN Gateways unter Benutzung von VPN und Zertifikaten

Mentor: Prof. Stefan Karsch
Autoren: Daniel Jedecke info@daniel-jedecke.de
Manuel Atug manuel@atug.de
Dennis Engel bilbogm@gmx.de
Jörg Ebbinghaus joerg.ebbinghaus@web.de
Referenz: wlan-doku.tex
Version: v1.1
Datum: 9. Juli 2004

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

In diesem Projekt soll exemplarisch eine sichere konzeptionelle Lösung für einen campus- oder unternehmensweiten Betrieb einer Wireless LAN-Infrastruktur aufgezeigt werden.

Diese konzeptionelle Lösung klärt NICHT die Verwaltungs- und Organisatorischen Angelegenheiten.

Heute wird unter Sicherheitsaspekten eine Kombination von WEP-Verschlüsselung und VPN-Tunnel als sicher erachtet. Auf dieser Grundlage werden auch wir den Anschluss an das Netz absichern.

Als Server kommt ein AMD Duron mit 256 MB Ram, 2 Netzwerkkarten und 80 GB Festplatte zum Einsatz. Auf diesem Rechner wird ein Debian Linux 3.rc2 installiert. Dabei wird ein gepatchter Kernel für FreeS/WAN eingesetzt. Dazu später mehr.

Technisch sind bereits folgende Details bekannt:

- Ein Client bekommt nur Zugriff, wenn sowohl SSID als auch WEP-Schlüssel stimmen. Darüber hinaus werden Verbindungen vom Server ausschließlich dann entgegen genommen, wenn der Client eine gültige VPN-Authentifizierung erhalten hat. Der Datenverkehr erfolgt ausschließlich per IPSec Verschlüsselung, die für heutige Verhältnisse eine ausreichende Sicherheit darstellt. Die Authentifizierung soll zur besseren Kontrolle nicht per Benutzername/Passwort sondern via Zertifikatsmanagement durchgeführt werden.

- An die Benutzer werden Zertifikate mit begrenzter Gültigkeit verteilt. Diese müssen über ein Zertifikatmanagement auf dem Server verwaltet werden. Dabei sollen X.509 Zertifikate auf dem Server mit PKI aufgebaut werden. Auf dem Server kann zusätzlich über eine Revokation-List der Zugriff auf die Ressourcen auch vorzeitig verweigert werden, für den Fall des Verlustes des Zertifikates oder dessen Missbrauch.

Eine Pilotlösung ist im KTDS-Labor der FH Köln, Campus Gummersbach geplant und umgesetzt worden.

Zusätzlich wurde das Projekt in den Räumen des KTDS-Labors vorgestellt. Hier der Ankündigungstext:

Das Labor für Kommunikationstechnik und Datensicherheit (KTDS) stellt am Mittwoch, den 07.07.2004 von 10:00 Uhr bis 11:00 Uhr das Projekt “Konzept eines W-LAN Gateways unter Benutzung von VPN und Zertifikaten“ in einem Vortrag der vier Studenten Daniel Jedecke, Manuel Atug, Dennis Engel und Jörg Ebbinghaus vor, welches von Prof. Karsch betreut wurde. Hierbei wird die in diesem Projekt ausgearbeitete sichere Lösung für den problematischen Einsatz von WLAN vorgestellt und an praktischem Beispiel nachvollziehbar erläutert.

Agenda

- Kurze Vorstellung der bekannten Schwächen in WLAN
- Erläuterung von IPSec
- Vorführung des Konzeptes in Theorie
- Generierung der benötigten Zertifikate
- Vorführung der Windows Client Konfiguration
- Aufbau der gesicherten Verbindung und Anzeige der Logdaten

Die Folien werden zusammen mit diesem Dokument auf den KTDS-Labor Webseiten, sowie evtl. auf den Webseiten der Autoren veröffentlicht. Selbstverständlich können auch die Autoren selber per Email angefragt werden, sollten die Dateien einmal nicht verfügbar sein.

2 Probleme beim Einsatz drahtloser Netze

2.1 Was ist WLAN?

Bevor man auf die Problematiken eines WLAN Netzes genauer eingehen kann, sollte ein Grundverständniss über die Technik vorhanden sein. Daher werden in diesem Teil zunächst die Grundlagen von WLAN besprochen, um dann die daraus resultierenden Probleme zu erläutern. Anschließend werden anhand von 2 Fallbeispielen im privaten Umfeld und im Unternehmen diese Probleme verdeutlicht.

WLANs basieren auf dem 1997 verabschiedeten Standard IEEE 802.11. Die zurzeit am weitesten verbreitete Technik ist die Erweiterung 802.11b mit 11 Mbit/s. Der Trend geht aber hin zu der aktuellen Erweiterung 802.11g mit 54 Mbit/s Übertragungsgeschwindigkeit. WLANs sind Funknetze, die sich im Gegensatz zu drahtgebundenen Netzen sehr komfortabel aufbauen lassen. Es ist nicht nötig, aufwändig Kabel zu verlegen, oder mehrere Rechner über Switches zu verbinden.

Nachstehend die Entwicklungsgeschichte der Standards für WLAN:

- 1997: Der erste Standard für Wireless LANs liegt vor. Er unterstützt drei Physical-Layer-Spezifikationen (PHY): Infrarot, "Frequency Hopping Spread Spectrum" (FHSS) mit 1 und 2 MBit/s sowie das Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) mit ebenfalls 1 und 2 MBit/s. Beide Funkübertragungstechniken verwenden den lizenzfreien 2,4-GHz-Bereich, das so genannte ISM-Band (Industrial, Scientific, Medical).

- 1999: Zwei neue Spezifikationen treten auf den Plan. Die erste, IEEE 802.11b, ist eine Erweiterung des ursprünglichen Standards. Sie basiert auf dem DSSS-Verfahren, verwendet aber ein effizienteres Kodierungsverfahren namens "Complimentary Code Keying" (CCK). Die Bruttodatenrate beträgt 11 MBit/s; zieht man den Protokoll-Overhead ab, bleiben in der Praxis für den Datentransfer etwa 5,5 MBit/s übrig. Die zweite Norm ist 802.11a, die das 5,2-GHz-Band nutzt und eine Übertragungsgeschwindigkeit von 54 MBit/s vorsieht. Im Gegensatz zu 802.11b arbeitet 802.11a mit mehreren Trägerfrequenzen und der Modulationstechnik "Orthogonal Frequency Division Multiplexing" (OFDM).

- 2000: Im März formiert sich innerhalb der Arbeitsgruppe IEEE 802.11 eine Study Group. Sie prüft, ob es technisch machbar ist, den 802.11b-Standard zu erweitern, um Datenraten von mehr als 20 MBit/s zu erzielen. Im Juli desselben Jahres erhält die Gruppe offiziell den Status einer Task Group und beginnt mit den Arbeiten an der Norm IEEE 802.11g. Das Ziel: eine Übertragungsrate von 54 MBit/s in WLANs, die im 2,4-GHz-Band arbeiten.

- 2001: Im Mai legen Texas Instruments (TI) und Intersil zwei Entwürfe einer 802.11g-Norm vor. Der von TI sieht eine Bandbreite von 22 MBit/s vor und basiert auf dem PBCC-22-Kodierungsschema, der von Intersil 54 MBit/s auf Grundlage der CCK-OFMD-Kodierung. Im November wird Intersils Ansatz im Normentwurf als Standardverfahren fixiert, während Texas Instruments Technik als Option zur Verfügung stehen soll. Die Arbeitsgruppe 802.11h formiert sich, um eine Version des WLAN-Standards IEEE 802.11a zu erarbeiten, die sich mit den Vorgaben des European Telecommunications Standards Institute (ETSI) und dem Hiperlan-2-Projekt verträgt.

Grundsätzlich können Funk-LANs in zwei verschiedenen Architekturen betrieben werden. Einmal im so genannten ad-hoc Modus, wobei die Clients hier direkt miteinander kommunizieren und einmal im so genannten infrastructure Modus. Im infrastructure Modus verbinden sich die Clients mit einem Access-Point um so Zugang zum Netzwerk zu erhalten. Ein Access-Point kann auch zusätzlich an ein kabelgebundenes Netzwerk angeschlossen sein.

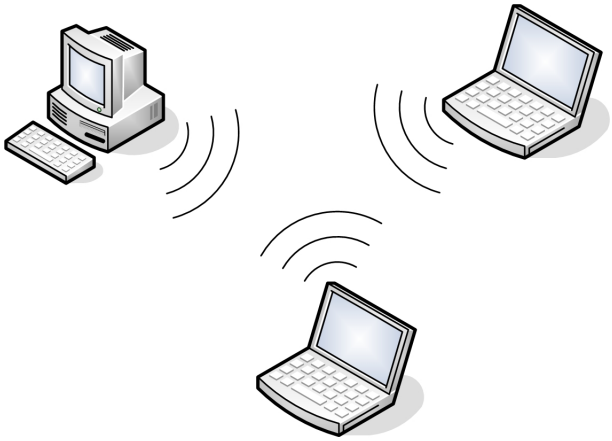


Abbildung 1: AD-Hoc Netzwerk

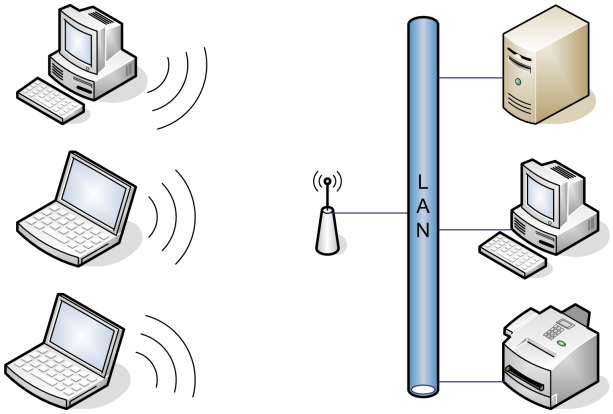


Abbildung 2: Infrastructure Netzwerk

Im Gegensatz zum ad-hoc Modus können beim infrastructure Modus mehrere Einsatzvarianten zum tragen kommen.

- Mittels mehrerer Access-Points können überlappende Funkzellen installiert werden, so dass beim Übergang eines Clients in die nächste Funkzelle die Funkverbindung aufrecht erhalten werden kann ("Roaming"). Auf diese Weise können große Bereiche flächendeckend versorgt werden. Die Reichweite einer Funkzelle ist extrem abhängig von den Umgebungsbedingungen und liegt im Bereich von ca. 10 - 150 Meter.

- Zwei Access-Points können auch als Brücke (Bridge) zwischen zwei leitungsgebundenen LANs eingesetzt werden. Ebenso ist der Einsatz eines Access-Points als Relaisstation (Repeater) zur Erhöhung der Reichweite möglich.

- Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access-Points kann ein Funk-LAN auch zur Vernetzung von Liegenschaften eingesetzt werden. Hier können lt. Herstellerangaben Reichweiten im Kilometerbereich erreicht werden. Die Access-Points können dabei als Relaisstation oder Brücke betrieben werden.

Der Standard verwendet die Bezeichnungen Independent Basic Service Set (IBSS) für Funk- Netzwerke im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur- Modus mit einem Access-Point. Mehrere

gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netzwerk wird Distribution System (DS) genannt.

2.2 Probleme beim WLAN

Die Probleme beim Einsatz von Wireless LAN sind zahlreich. Funknetze sind ebenso wie Ethernet Broadcast Medien. Allerdings ist das Abhören von Datenübertragungen über Luft gegenüber den kabelgebundenen Übertragungswegen wesentlich einfacher, da hier kein physischer Zugriff auf das Netzwerk nötig ist. Es reicht also aus, wenn bspw. der Angreifer in seinem Auto vor einem Gebäude steht (Parking Lot Attack). Ein Einbruch in das Gebäude um Zugang zum Internen Netz zu erhalten ist nicht mehr nötig.

Die am Markt verfügbaren WLAN-Systeme sehen in der Regel zwar Sicherheitsmechanismen vor, doch haben diese zum Teil erhebliche Lücken. Dadurch sind Angriffe relativ leicht möglich. Dabei unterscheidet man zwischen passiven (Abhören) und aktiven Angriffen (Eindringen). Von den Sicherheitslücken sind insbesondere die Systeme nach IEEE 802.11 betroffen. Zwar bringt der Standard einige Sicherheitsmechanismen wie SSID und WEP mit, die das Eindringen in ein Netzwerk wohl erschweren, aber nicht verhindern können. Seit Mitte 2001 sind die Nachteile dieser Sicherheitsmechanismen bekannt und können auch von Laien überwunden werden.

Die SSID bezeichnet den Namen eines WLAN Gerätes. Nur wer diesen Namen kennt, kann sich mit dem Gerät verbinden. Es gibt die Option, die SSID zu verstecken, jedoch wird diese in so genannten Beacon-Paketen mitgeschickt und kann somit von entsprechenden Werkzeugen erkannt werden. Oft wird auch der vom Hersteller vorgegebene Name für die SSID verwendet.

WEP steht für Wired Equivalent Privacy und stellt eine fehlerhaft implementiere Verschlüsselung dar. Als Referenz hierzu sei auf http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html verwiesen.

Anleitungen und Tools für das Eindringen in solche Netze können ohne weiteres aus dem Internet bezogen werden.

Als Proof-of-Concept sei hier auf die zwei folgenden Werkzeuge für WEP-Entschlüsselung verwiesen:

- http://airsnort.shmoo.com - Airsnort ist ein Werkzeug, um den WEP Schlüssel aus Netzwerkdatenmitschnitten zu rekonstruieren
- http://wepcrack.sourceforge.net - Wepcrack ist ein Werkzeug, um WEP Schlüssel per Brute-Force Attacke zu brechen

Das Auffinden von WLANs ist auch relativ simpel. Auch hier kann man sich im Internet informieren oder durch so genanntes Wardriving oder Warchalking eigene Funknetze aufspüren. Beim Wardriving oder Warwalking entdeckte Access-Points werden häufig von so genannten Warchalkern mit Hilfe von Kreidezeichnungen angezeigt. Verschiedene Symbole beschreiben dabei die verwendeten Sicherheitseinstellungen, sowie Erreichbarkeit und Signalqualität.

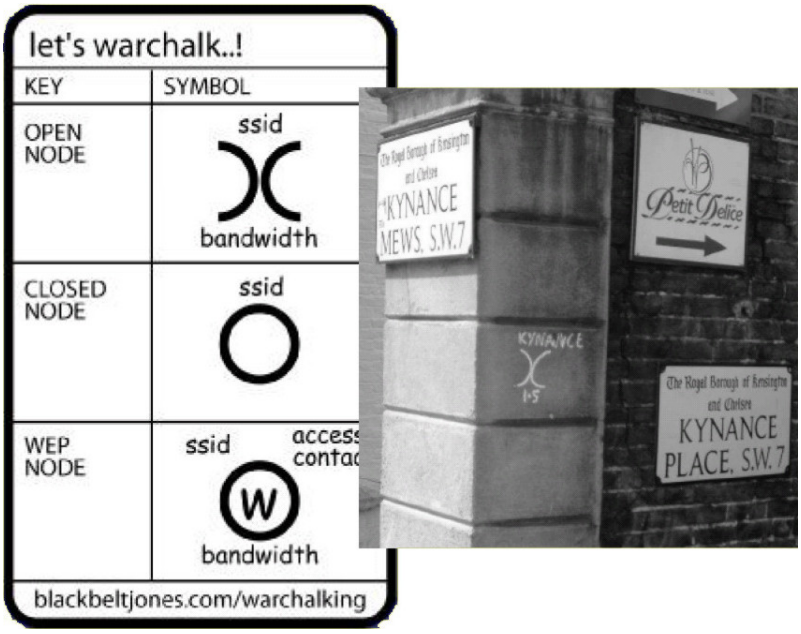


Abbildung 3: Warchalking

2.3 Fallbeispiel Private Nutzung von WLAN:

Das Risiko Opfer eines Angriffs, oder zumindest einer ungewollten Mitbenutzung des Internetzuganges zu werden ist sicherlich höher als viele annehmen. Bei einem vom IT-Security Unternehmen SacredBytes durchgeführten Wardriving im Stadtkern von Frankfurt/Main wurden innerhalb einer Stunde 66 Access-Points aufgezeichnet. Davon war bei 28 APs WEP aktiv, 38 waren unverschlüsselt. Zudem lieferten 17 APs Standard-SSIDs, die darauf schließen lassen, dass noch die Werkseinstellung aktiv ist.

Im Klartext: Jeder Angreifer mit Standard WLAN-Equipment kann sich in einem WLAN frei bewegen, Daten mitlesen, im Internet surfen...

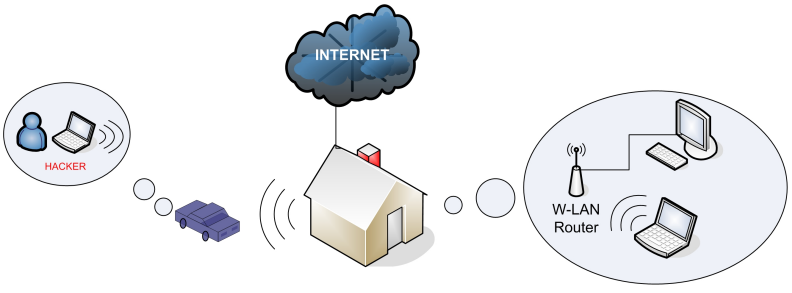


Abbildung 4: Private Umgebung

2.4 Fallbeispiel Nutzung von WLAN im Unternehmen:

Bei Unternehmen ist das Risiko Opfer eines Angriffs zu werden ungleich höher. Im Gegensatz zu privaten Briefen und Fotos, die im privaten Bereich zu erwarten sind, ist hier die Industriespionage zu nennen, die bei einem ungeschützten Netz, in dem keine Sperre durchbrochen werden muss, nicht einmal strafbar ist. Wenn der Access-Point wie in der Abbildung im Intranet integriert ist, wird es dem Angreifer ermöglicht, auf sämtliche Ressourcen zuzugreifen. Funk-Netze werden hier oft als Erweiterung zu den Kabelnetzen verwendet. Der Access-Point stellt hier auch eine Hintertür zum Unternehmensnetz dar. Sämtliche aufwendig installierten Schutzmaßnahmen wie Paketfilter und Application Firewalls (symbolisiert durch Router I und Router II), die den Zugriff aus dem Internet regeln werden hier umgangen.

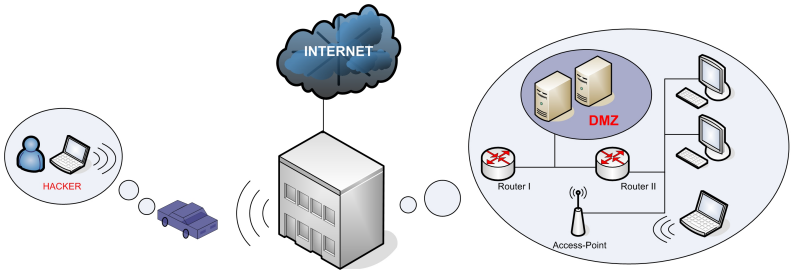


Abbildung 5: Unternehmens Umgebung

3 Ziele & Sicherheitsanforderungen

Vorderstes Ziel dieses Projektes ist es, ein lauffähiges System zur Verfügung zu stellen, um den Einsatz eines Wireless LANs exemplarisch im KTDS-Labor unter besserer Sicherheit zu betreiben, als die im WLAN integrierten Merkmale mit sich bringen.

Hier bieten sich mehrere Möglichkeiten an. Durch Kombinationen ergibt sich eine noch größere Auswahl. Schließlich haben wir uns für eine Kombination folgender Sicherheitskomponenten und Dienste entschieden:

- WEP 128 Bit Verschlüsselung
- "Geheime" SSID
- VPN Tunnel in der WEP-Verschlüsselung
- IPSec Verschlüsselung im VPN Tunnel
- Variabler IPSec Schlüssel mit kurzer Lebensdauer
- Authentifizierung ausschließlich über x509 Zertifikat
- Begrenzte Gültigkeitsdauer des Zertifikates
- DHCP zur Begrenzung der gleichzeitigen Verbindungen
- DNS Anfragen erst im IPSec Tunnel
- Firewall zur Begrenzung des Datenverkehrs auf VPN Verbindungen

Bei der Gestaltung eines Sicherheitskonzeptes für Funknetzwerke sind drei Prämissen zu berücksichtigen:

1. Zugriffskontrolle
2. Datenintegrität
3. Vertraulichkeit

`Zugriffskontrolle` Eine Zugriffskontrolle soll sicherstellen, dass nur legitimierte Nutzer an der Kommunikation teilnehmen können (Autorisierung). Weiterhin soll sie auch gewährleisten, dass sich die Nutzer mit einem vertrauenswürdigen Partner (hier Access-Point) verbinden (Authentifizierung), statt die Kommunikation über einen ≫rogue≪ (deutsch: Schurke) Access-Point abzuwickeln.

`Datenintegrität` Die Datenintegrität hat als Ziel, dass Angreifer davon abgehalten werden, die Daten einer Nachricht unbemerkt für die Kommunikationspartner zu verfälschen. Somit ist die Authentizität gewährleistet.

`Vertraulichkeit` Zur Erfüllung der Vertraulichkeit wird meist Verschlüsselung angewandt. Dadurch soll nur der Partner, für den die Übertragung bestimmt ist, den Inhalt der Nachricht lesen können.

Als weiteres Ziel können wir noch nennen, dass dieses Projekt zwar auf einen sehr beschränkten Umfang eines WLANs ausgelegt ist, jedoch zumindest ansatzweise auch Gedanken einfließen sollen, die die Umsetzung in weitaus größeren Rahmen ermöglicht. Denkbar ist hier neben der exemplarischen Laborumgebung ein campusweites Netz (Standort Gummersbach) oder sogar ein FH-weites Netz mit zentraler Authentifizierungsstelle. Jedoch machen uns derzeit noch technische Probleme im Kontext des Roamings im WLAN zu schaffen. Hier bleibt abzuwarten, was die technische Entwicklung in nächster Zeit bringt.

Einen guten übersichtlichen Einstieg in die Thematik und Problematik WLAN-Sicherheit bietet die Semesterarbeit von Sebastian Klamar[1] der oben bereits kurz zitiert wurde.

[1] http://tux.wh17.tu-dresden.de/šebi/pub/Sicherheit-WLAN.pdf

4 Lösungsansatz

Als Lösung für diese Probleme nutzen wir die Fähigkeiten von IPSec aus. IPSec steht für IP Security und stellt eine frei verfügbare Verschlüsselungstechnologie dar, um sicher zwischen zwei Punkten zu kommunizieren.

Da WEP als unsicher gilt, bauen wir innerhalb des WEP verschlüsselten Netzes einen IPSec Tunnel ein, um die Identität und Integrität der Daten zu gewährleisten.

Hierzu bedienen wir uns FreeS/WAN, einer Open Source Lösung, um einen Linux Gatewayrechner zu konfigurieren, der nur noch verschlüsselte Daten zulässt. FreeS/WAN implementiert IPSec als Kernelpatch.

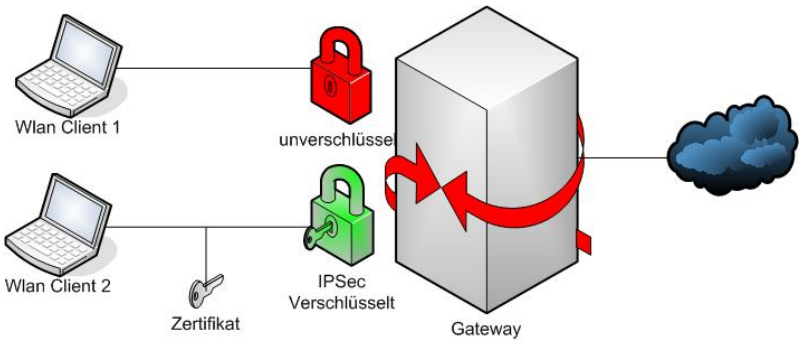


Abbildung 6: Lösungsansatz

5 Voraussetzungen

5.1 Hardware

Eingesetzt werden kann prinzipiell jeder Computer der über eine Wireless LAN Karte verfügt.

Die Wireless LAN Karte der Client Systeme sollte eine 128 Bit WEP Verschüsselung anbieten. Ansonsten gibt es keine weiteren Anforderungen an die Hardware. Auf Serverseite reichen 2 Netzwerkkarten aus.

5.2 Server

Für den Server gelten die gleichen Regeln wie für den Linux Client, da das System gleich aufgebaut ist. Wir empfehlen jedoch den Einsatz von Debian, da hier die Konfiguration am einfachsten ist.

5.3 Access-Point

Der Access-Point sollte als minimale Voraussetzung 128 Bit WEP-Verschlüsselung anbieten und wird an eine der beiden Netzwerkkarten des Servers angeschlossen.

5.4 Clients

Die Clients müssen softwareseitig ein paar Voraussetzungen erfüllen, um mit IPSec arbeiten zu können. Im Folgenden werden wir auf die speziellen Anforderungen der einzelnen Betriebssysteme eingehen. Es müssen ein paar Software Komponenten nachinstalliert werden, um eine mit IPSec verschlüsselte Verbindung aufbauen zu können.

5.4.1 Windows

Unter den Windows Client Systemen raten wir zum ausschließlichen Einsatz der Versionen:

- Microsoft Windows 2000 mit Service Pack 4
- Microsoft Windows XP mit Service Pack 1

Außerdem müssen zur späteren Zweckerfüllung bei beiden Systemen die Support-Tools nachinstalliert werden. Diese sind auf der Installations-CD unter \SUPPORT\TOOLS\ zu finden.

Allgemein ist zu raten, das System mit allen verfügbaren Updates auszustatten um mögliche Sicherheitslücken zu schließen.

Theoretisch ist der Zugang zu unserem Testnetz auch mit anderen Windows Systemen möglich, jedoch sind die durchzuführenden Updates und Patches für diese Systeme so umfangreich, dass es den Rahmen dieser Arbeit sprengen würde, für jedes erdenkliche System die notwendigen Informationen zur Verfügung zu stellen. Wer hier entsprechend Arbeit investieren möchte, ist herzlich eingeladen dies zu tun. Prinzipiell schließen wir keine Systeme von der Teilnahme am Projekt aus. Wer entsprechende Anpassungen vorgenommen hat, darf uns gerne eine Liste mit nötigen Updates und gerne auch ein HowTo zukommen lassen.

5.4.2 Linux

Bei Linux kann jedes Derivat benutzt werden, welches den Kernel 2.4.x oder 2.6.x mit gepatchtem FreeS/WAN nutzt. In FreeS/WAN muss aber vorher noch der x.509 Patch eingebunden werden. Wer dies nicht möchte, kann sich auf der SuperFreeS/WAN Seite auch ein fertiges Paket herunterladen.

FreeS/WAN wird schon bei vielen Linux Versionen mitgeliefert, jedoch meist nicht in der aktuellen Version. FreeS/WAN stellt eine freie IPSec Variante dar.

6 Benutzte Hardware

6.1 Server

Benutzte Hardware - Server		
Typ	**Hersteller**	**Bezeichnung**
Prozessor	AMD	Duron 1,3 GHz
Ram	Infinion	256 MB
Mainboard	Elitegroup	
Netzwerkkarte 1	3 Com	
Netzwerkkarte 2	3 Com	
Festplatte	Western Digital	80 GB

6.2 Access-Point

Benutzte Hardware - Access-Point		
Typ	**Hersteller**	**Bezeichnung**
Access-Point	Cisco	AP 1200

6.3 Clients

Benutzte Hardware - Clients		
Client 1		
Typ	**Hersteller**	**Bezeichnung**
Prozessor	Intel	Mobile Celeron 1,5 GHz
Ram	Infinion	512 MB
Mainboard	Intel	x810 Chipset
Netzwerkkarte 1	Realtek	
Netzwerkkarte 2	Lucent	Orinoco Wireless Gold
Festplatte	IBM	30 GB
Client 2		
Prozessor	Transmeta	Duron 1,3 GHz
Ram	Infinion	256 MB
Netzwerkkarte 1	Realtek	
Netzwerkkarte 2	Lucent	Orinoco Wireless Gold
Festplatte	Western Digital	80 GB

7 PKI Zertifikate

IPSec Verbindungen werden über einen gemeinsamen Schlüssel aufgebaut. Diese Lösung mag bei einigen Clients vielleicht noch interessant sein, wenn die Zahl der User aber steigt wird diese Technik schnell unübersichtlich. Um dieses Problem zu umgehen, bekommt jeder User ein eindeutiges Zertifikat, welches jederzeit von der Public Key Infrastructure (PKI) revoked (zurückgewiesen) werden kann. Zertifikate basieren auf asymmetrischer Kryptografie. Dabei kann man das asymmetrische Verfahren so verstehen, dass eine beliebige Person eine Botschaft in eine Kiste packt und ein Schloss einschnappen lässt. Das Öffnen des Schlosses ist dann nur noch dem Besitzer mit dem passenden Schlüssel möglich.

Ein Zertifikat besteht aus folgenden Komponenten:

- Aus dem zu zertifizierenden öffentlichen Schlüssel
- Aus allen Angaben über den Schlüsselinhaber, insbesondere seinem Namen und seiner E-Mail-Adresse (Common Name nach X.509)
- Zertifikat-Attribute, z.B. Zertifikat-Seriennummer, Gültigkeitsdauer oder Angaben zur Verwendbarkeit
- Der Beglaubigung des Zertifikat-Gebers, dass diese Angaben stimmen

Zusätzlich bekommt der User einen privaten Schlüssel, mit welchem er das Zertifikat nutzen kann. Ohne diesen kann er keine mit diesem Zertifikat verschlüsselten Texte entschlüsseln. Zur Verschlüsselung reicht das Zertifikat jedoch aus. Hierzu sei ein Verweis auf asymmetrische Verschlüsselung gegeben, auf der Zertifikate basieren[2]

Für Windows-Clients verwenden wir das PKCS12 Format. Dieses ist ein Container Format, welches zum Beispiel von Netscape, Internet Explorer und Outlook Express verwendet wird. In diesem Container liegt das öffentlich zugängliche Zertifikat, der passende private Schlüssel, sowie das Zertifikat der RootCA. Die beiden Zertifikate werden genutzt, um einen passenden Eintrag in den Stammzertifikaten zu erstellen. Der private Schlüssel authentisiert den öffentlichen Schlüssel.

Man unterscheidet bei den Verschlüsselungsverfahren zwischen der symmetrischen und der asymmetrischen Verschlüsselung.

Bei der symmetrischen Verschlüsselung besitzen beide Partner, zum Beispiel Alice und Bob den gleichen Schlüssel. Dieser muss über einen sicheren Weg von Alice zu Bob gelangen, damit nur diese beiden eine Nachricht untereinander verschlüsseln und entschlüsseln können.

Bei der asymmetrischen Verschlüsselung wird die Nachricht für Bob mit dem öffentlichen Schlüssel von Bob verschlüsselt. Nur Bob kann diese Nachricht durch seinen privaten Schlüssel entschlüsseln.

Der Nachteil der asymmetrischen Verschlüsselung ist der hohe mathematische Aufwand. Aus diesem Grund wird in der Regel ein Hybridverfahren verwendet, wobei symmetrische und asymmetrische Verschlüsselung kombiniert werden.

[2] http://www.dfn-pca.de/bibliothek/bulletins/info/ssl-tls-clients/cert-management-suse73-netscape-communicator-478/1.0/node5.html

8 Umsetzung

Wir werden nun auf die konkrete Implementierung des Servers eingehen und einige Infos zum Aufbau des Systems geben. Speziell wird der Betriebssystemkern, sowie die IPSec Implementierung erläutert.

8.1 Betriebssystem

Als Betriebssystem kommt ein normales Debian Woody Release Candidate 2 zum Einsatz. Dieses bringt von Haus aus eine stabile und sichere Grundlage für den Einsatz als Gateway mit. Wer noch wenig Erfahrung mit der Installation von Debian Systemen hat, sollte sich die zahlreichen Hilfen auf der Debian Homepage ansehen.

Nach der Installation des Basissystems werden einige zusätzliche Pakete eingespielt, die später wichtig werden. Hierzu zählt die Firewall, die Routing Tools, ein neuer Kernel sowie OpenSSL. Diese werden nacheinander auf dem System installiert.

Wir benutzen für dir Installation eine aktuelle "Net Install CD" des Debian Projektes. Diese hat den Vorteil, dass alle Pakete aktuell aus dem Netz geladen werden, und keine Sicherheitskritischen Pakete den Weg auf das System finden. Jedoch muss der Rechner dazu über eine bereits geöffnete Internetverbindung verfügen. Wer dies nicht hat, kann sich auch die kompletten Debian CDs aus dem Netz laden (sieben CDs oder eine DVD!) oder einfach bei einem Händler für wenig Geld ordern[3].

Wenn wir nun eine CD haben und von dieser booten, dann erscheint nach kurzer Zeit eine Eingabeaufforderung. Hier geben wird "bf24" ein, um den Kernel 2.4 zu laden. Standardmäßig wird sonst ein Kernel 2.2 benutzt, der nicht die nötige Unterstützung für aktuelle Hardware aufweisen kann.

Der genaue Installationsprozess wird im Debian Anwenderhandbuch[4] sehr gut erklärt, weshalb wir hier nicht auf die genaue Installation eingehen werden.

Nach einiger Zeit sollte das Debian System installiert sein und wir können uns als "root" anmelden, um die Konfiguration einzurichten.

8.2 Kernel

Um die volle Funktionalität von IPSec nutzen zu können, benötigen wir einen neuen Kernel. Gleichzeitig nutzen wir den Zeitpunkt, um einen aktuellen Kernel zu installieren, da es in Versionen kleiner 2.4.23 zu Sicherheitslücken kommt, die wir von vornherein ausschließen möchten.

Aus diesem Grund setzen wir auf einen aktuellen Kernel[5]. Grundsätzlich sollte immer der aktuellste Kernel verwendet werden, was bei uns zum Zeitpunkt der Dokumenterstellung die Version 2.4.24 war. Wer noch nie einen Kernel kompiliert hat, sollte sich über eine der vielen Kernel-HowTo's informieren[6].

Das Patchen des Kernels passiert durch das FreeS/WAN Paket fast vollkommen automatisch. FreeS/WAN erwartet jedoch vorher einen fertig konfigurierten Kernel unter "/usr/src/linux". Falls der Kernel nicht dort liegt, sollte man vorher einen symbolischen Link auf das Verzeichnis legen. Dies passiert mit dem Befehl "ln -s Quellverzeichnis Zielverzeichnis". Nun kann man in das FreeS/WAN Verzeichnis wechseln und mit der Installation des Patches beginnen.

Wenn man sich auf der Konsole befindet, kann man die Installation mit dem Befehl "make menugo" beginnen. FreeS/WAN patcht nun automatisch den Kernel und öffnet den Konfigurationsdialog auf der Konsole. Unter "Network Settings ->FreeS/WAN" sind alle Optionen automatisch aktiviert. Wenn man nun die Konfiguration speichert, beginnt sofort das neue kompilieren des Kernels. Im Anschluss werden automatisch die IPSec Programme kompiliert und mit dem Befehl "make install" werden diese auch automatisch im System installiert.

8.3 PKI

Um eine einfache Zertifikatserstellung zu ermöglichen, nutzen wir das Paket "OpenSSL". Dieses lässt sich bei Debian Systemen relativ einfach nachinstallieren. Durch den Befehl "apt-get install openssl" beginnt das automatische

[3] http://www.liniso.de
[4] http://www.openoffice.de/linux/buch/
[5] http://www.kernel.org
[6] http://www.linuxplanet.com/linuxplanet/tutorials/3196/1/

laden, eine bestehende Internetverbindung vorausgesetzt, sowie das installieren des Paketes.

Zuerst einmal sollte die Hauptkonfigurationsdatei "openss.ncnf" im Verzeichnis "/etc/openssl/" ändern. Hier werden alle grundlegenden Einstellungen verwaltet. Wir öffnen die Datei mit einem beliebigen Editor und ändern folgende Zeilen:

```
default_days = 3650     # Gültigkeitsdauer

[req]
default_bits = 2048     # Schlüssellänge

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = DE
countryName_min = 2
countryName_max = 2

localityName = Locality Name (eg, city)
localityName_default = Gummersbach

0.organizationName = Organization Name (eg, company)
0.organizationName_default = FH Koeln

# we can do this but it is not needed normally :-)
#1.organizationName = Second Organization Name (eg, company)
#1.organizationName_default = World Wide Web Pty Ltd

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Campus Gummersbach

commonName = Common Name (eg, YOUR Username or Email)
commonName_max = 64
```

Abbildung 7: Auszug aus der openssl.cnf

OpenSSL bietet eine einfache Schnittstelle um schnell eine komplette PKI aufzusetzen. Unter Debian findet man unter "/usr/lib/ssl/misc/CA.sh" findet man ein Skript um schnell verschiedene Aufgaben einer PKI durchzuführen.

In unsrem Fall legen wir unter dem Verzeichnis "/var" ein neues Verzeichnis mit dem Namen "rootca" an. Hier werden alle Zertifikate gespeichert und verwaltet.

Um eine neue CA (Certificate Authority) zu erzeugen geben wir nun im neuen Verzeichnis einfach das folgende ein:

/usr/lib/ssl/misc/CA.sh -newca

Zuerst werden wir nach einem "CA certificate filename" gefragt. Hier drücken wir einfach "Enter" um eine neue CA zu erstellen. Nun werden wir nach einer Pass Phrase gefragt. Diese sollte man sich gut merken, da wir diese später immer wieder brauchen. Wenn wir eine Pass Phrase eingegeben haben, müssen wir diese noch mal eingeben um alles zu bestätigen.

Bis zum "Common Name" können wir nun "Enter" drücken, da wir ja alles wichtige in der Konfigurationsdatei definiert haben. Als Common Name sollten wir für die "Root CA" einen passenden Namen auswählen. Hier wäre z.B. "Root CA WLAN Projekt" ein treffender Name. Jetzt ist die Root CA fertig und wir können weitere Zertifikate erstellen.

Eine Grafik zeigt anschaulich die nächsten Schritte:

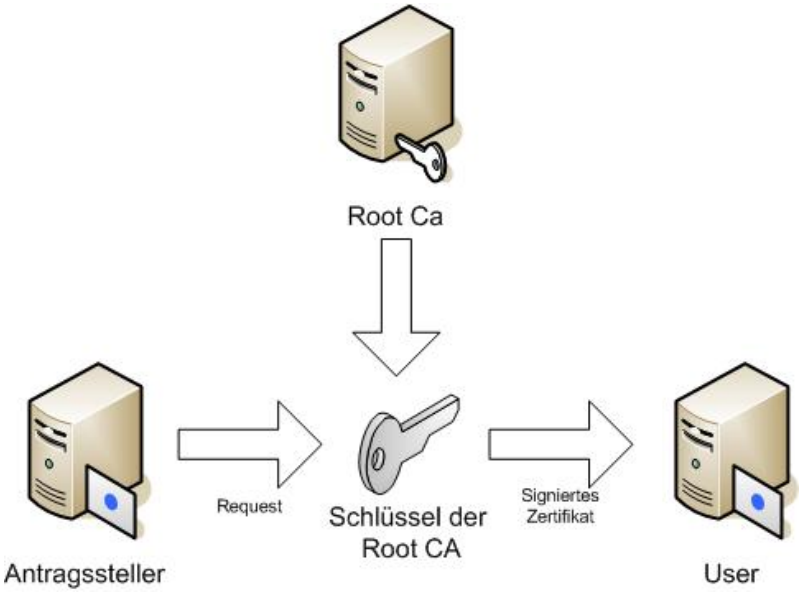


Abbildung 8: Ausstellen eines Zertifikates

Das erste Zertifikat sollen wir für das Gateway selber anlegen.

Einen neuen Request erstellen wir mit:

/usr/lib/ssl/misc/CA.sh -newreq

Hier werden wir nun wieder nach einer Pass Phrase gefragt. Diese sollte anderes als die Root CA Pass Phrase sein. Sonst fahren wir wie oben fort und geben später als Common Name einfach "Gateway" ein. Nun folgen noch ein paar fragen, die aber einfach alle mit "Enter" bestätigt werden können.

Das Zertifikat ist nur erstellt, muss jedoch noch von der Root CA signiert werden. Das geschieht mir folgenden Befehl:

/usr/lib/ssl/misc/CA.sh -sign

Wir geben nun die Passphrase der Root CA ein. Das Zertifikat ist nun signiert. Nun sollte das Zertifikat noch passende Namen bekommen:

mv newreq.pem gateway.key
mv newcert.pem gateway.pem

Jetzt haben wir Zertifikate, die überall verwendet werden können.

Windows User brauchen jedoch ein spezielles ".p12" Format. Diese generieren wir auch noch schnell:

openssl pkcs12 -export -in gateway.pem -inkey gateway.key -certfile demoCA/cacert.pem -out gateway.p12

Und wenn wir gerade schon dabei sind, lassen wir uns direkt für die IPSec Konfiguration die Subject Zeile ausgeben:

openssl x509 -in demoCA/cacert.pem -noout -subject

Wir sollten nun noch mindestens ein Zertifikat für einen User generieren. Einfach die Schritte bis zum generieren der ".p12" Datei wiederholen und als Common Name den User Namen eingeben.

8.4 VPN

Nachdem wir jetzt Rechner im Netz durch Zertifikate sicher identifizieren können nutzen wir dies, um basierend auf den Zertifikaten verschlüsselte Verbindungen aufzubauen.

Der wichtigste Anlaufpunkt für die Konfiguration von IPSec sind folgende Dateien und Verzeichnisse:

- /etc/ipsec.conf
- /etc/ipsec.secure
- /etc/ipsec.d/

Hier werden alle benötigen Einstellungen vorgenommen.

version 2.0 # conforms to second version of ipsec.conf specification

basic configuration
config setup
# Debug-logging controls: "none" for (almost) none, "all" for lots.
klipsdebug=none # Debuging abschalten
plutodebug=none # Debuging abschalten
interfaces="ipsec0=eth1" # Welches Interface benutzt IPSec
uniqueids=no

conn roadwarrior # Unsere Verbindung zum Roadwarrior
left=192.168.23.1 # Unsere IP
leftsubnet=0.0.0.0/0 # Wohin leiten wir weiter
leftrsasigkey=%cert # Wo liegen die Zertifikate
leftcert=gateway.pem # Unser Zertifikat
leftid="/C=DE/L=Gummersbach/O=FH Koeln/OU=Campus Gummersbach/CN=VPN Gateway" # Unsere ID
right=%any # Alle ankommenden Verbindungen zulassen
rightrsasigkey=%cert # Wo liegen die Zerifikate
auto=add

Opportunistic Encryption abschalten:
conn block
auto=ignore
conn private
auto=ignore
conn private-or-clear
auto=ignore
conn clear-or-private
auto=ignore
conn clear
auto=ignore
conn packetdefault
auto=ignore

Abbildung 9: Ipsec.conf

8.5 Firewall

Als Firewall nutzen wir eine iptables basierte Paketfirewall. Um jedoch nicht jede iptables Regel lernen zu müssen, nutzen wir das Programm "FIAIF", welches nach einfacher Konfiguration die passenden Firewall Regeln erstellt und installiert.

Wichtig ist in diesem Zusammenhang, dass nur IPSec verschlüsselte Verbindungen durch gelassen werden sollen. Alle anderen Verbindungen müssen abgeblockt werden. Da wir aber nicht einfach alle Verbindungen blocken können,

müssen wir uns vorher ein paar Gedanken über das Konzept der Firewall machen. Da wir einen DHCP Server haben, der die Wireless LAN Clients automatisch mit einer IP versorgt, müssen wir dieses Protokoll in der Firewall zulassen. Zudem nutzen wir für die Administration eine Secure Shell (SSH) welche ebenfalls freigeschaltet sein muss.

8.5.1 Unverschlüsseltes WLAN nach Extern

Falls beim WLAN Client der richtige WEP Schlüssel eingeben wurde, bekommt er automatisch eine IP vom DHCP Server auf dem Gateway zugewiesen. Wir müssen also DHCP Verbindungen in der Firewall erlauben.

Zur besseren Kontrolle erlauben wir Ping Anfragen auf das Gateway, um dessen Erreichbarkeit zu testen.

Um jetzt jedoch eine IPSec Verbindung aufzubauen, müssen wir in der Firewall auch die IPSec Authentifizierung freischalten.

8.5.2 Verschlüsseltes WLAN nach Extern

Sobald der IPSec Tunnel aufgebaut wurde, bekommt der Client vollen Zugriff auf das Internet. Hierzu müssen wir nur NAT auf der Firewall einrichten.

8.5.3 Extern nach WLAN

Von Extern sind zur Wartung nur SSH-Anfragen erlaubt.

8.6 FIAIF Umsetzung

In "FIAIF" teilen wir das Netzwerk in drei Zonen auf. In diesen lassen sich alle oben genannten Unterscheidungen umsetzen.

- Extern - Verbindungen von und ins Internet
- Intern - Verbindungen von und ins unverschlüsselte WLAN
- IPSec - Verbindungen von und ins verschlüsselte WLAN

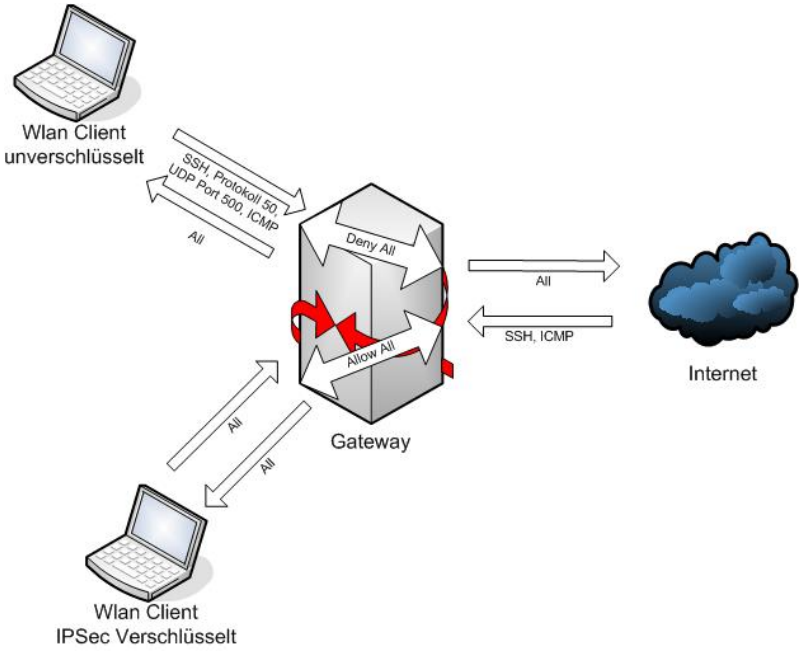


Abbildung 10: Grafischer Überblick

8.6.1 Konfigurationsdateien

Hier folgen nun ein paar Auszüge auf den Konfigurationsdateien:

```
NAME=EXT     # Name der Zone
DEV=eth0     # Welches Device wird kontrolliert?
DYNAMIC=0    # Wird die IP dynamisch zugewiesen?
GLOBAL=1     # Zeigt dieses Device ins Internet?

DHCP_SERVER=0     # Läuft auf dem PC ein DHCP Server?

# Alle Regeln die den Input regeln
INPUT[0]="ACCEPT tcp ssh 0.0.0.0/0=>0.0.0.0/0"
INPUT[1]="ACCEPT icmp echo-request 0.0.0.0/0=>0.0.0.0/0"
INPUT[2]="ACCEPT igmp 0.0.0.0/0=>224.0.0.0/4"
INPUT[3]="DROP ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die den Output regeln
OUTPUT[0]="ACCEPT ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die das Weiterleiten von Paketen regeln
FORWARD[0]="IPSEC ACCEPT ALL 0.0.0.0/0=>0.0.0.0/0"
FORWARD[1]="INT DROP ALL 0.0.0.0/0=>0.0.0.0/0"

# Hier werden bestimmte Relpy's definiert
REPLY_AUTH="EXT tcp-reset tcp auth 0.0.0.0/0=>0.0.0.0/0"
REPLY_TRACEROUTE="EXT icmp-port-unreachable udp 33434:33464 0.0.0.0/0=>0.0.0.0/0"
```

Abbildung 11: Auszug aus der zone.ext

```
NAME=INT     # Name der Zone
DEV=eth1     # Welches Device wird kontrolliert?
DYNAMIC=1    # Wird die IP dynamisch zugewiesen?
GLOBAL=0     # Zeigt dieses Device ins Internet?

DHCP_SERVER=1     # Läuft auf dem PC ein DHCP Server?

# Alle Regeln die den Input regeln
INPUT[0]="ACCEPT tcp ssh 0.0.0.0/0=>0.0.0.0/0"
INPUT[1]="ACCEPT udp 500 0.0.0.0/0=>192.168.23.1"
INPUT[2]="ACCEPT 50 0.0.0.0/0=>192.168.23.1"
INPUT[3]="DROP ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die den Output regeln
OUTPUT[0]="DROP ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die das Weiterleiten von Paketen regeln
FORWARD[0]="ALL DROP ALL 0.0.0.0/0=>0.0.0.0/0"
```

Abbildung 12: Auszug aus der zone.int

```
NAME=IPSEC     # Name der Zone
DEV=ipsec0     # Welches Device wird kontrolliert?
DYNAMIC=1      # Wird die IP dynamisch zugewiesen?
GLOBAL=0       # Zeigt dieses Device ins Internet?

DHCP_SERVER=1     # Läuft auf dem PC ein DHCP Server?

# Alle Regeln die den Input regeln
INPUT[0]="ACCEPT ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die den Output regeln
OUTPUT[0]="ACCEPT ALL 0.0.0.0/0=>0.0.0.0/0"

# Alle Regeln die das Weiterleiten von Paketen regeln
FORWARD[0]="ALL ACCEPT ALL 0.0.0.0/0=>0.0.0.0/0"

# NAT aktivieren SNAT[0]="EXT ALL 0.0.0.0/0=>0.0.0.0/0"
```

Abbildung 13: Auszug aus der zone.ipsec

9 Clientkonfiguration

Hier empfehlen wir, bei der Ausgabe einer Zugangsberechtigung an die Benutzer eine Diskette mit folgendem Inhalt zu übergeben:

- Das IPSec-Tool von http://vpn.ebootis.de/package.zip
- Das Microsoft-Support-Tool ipsecpol.exe (W2K) und ipseccmd.exe (WXP)
- Eine angepasste ipsec.conf
- Die HowTos für Windows und Linux im PDF-Format

9.1 Windows2000/XP Client

Folgende Schritte müssen unter Windows 2000/XP durchgeführt werden:

1. Unter Windows 2000 muss das neueste Service Pack installiert sein oder zumindest das "High Encryption Package" um 3DES zu unterstützen. Bei Windows XP ist dies bereits integriert.
2. Den Inhalt der vom Labor erhaltenen Diskette in ein Verzeichnis auf der Festplatte kopieren und die zip-Datei entpacken.
3. Anschließend müssen von der Windows Installations-CD die "Support Tools" in das selbe Verzeichnis nachinstalliert werden, zu finden auf der Windows 2000 / XP CD unter \SUPPORT\TOOLS.
4. Nach der Installation sollte sich die Datei ipsecpol.exe (bei Windows 2000) oder ipseccmd.exe (bei Windows XP) in dem Verzeichnis befinden.
5. Anschließend folgt der Import des Zertifikates:
   (a) Start ->Ausführen ->mmc (Abbildung "MMC-Konsole öffnen")
   (b) ipsec.msc aus dem obigen Verzeichnis öffnen
   (c) auf das Plus bei Zertifikate (lokaler Computer) klicken
   (d) Rechtsklick auf Eigene Zertifikate
   (e) alle Tasks
   (f) Importieren (Abbildung "Importieren von einem Zertifikat")
   (g) p12-Datei auswählen und Passwort eingeben
   (h) Zertifikatsspeicher automatisch auswählen
   (i) Fertig

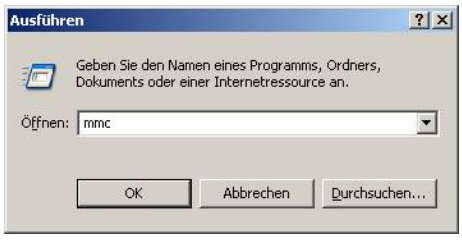


Abbildung 14: MMC-Konsole öffnen

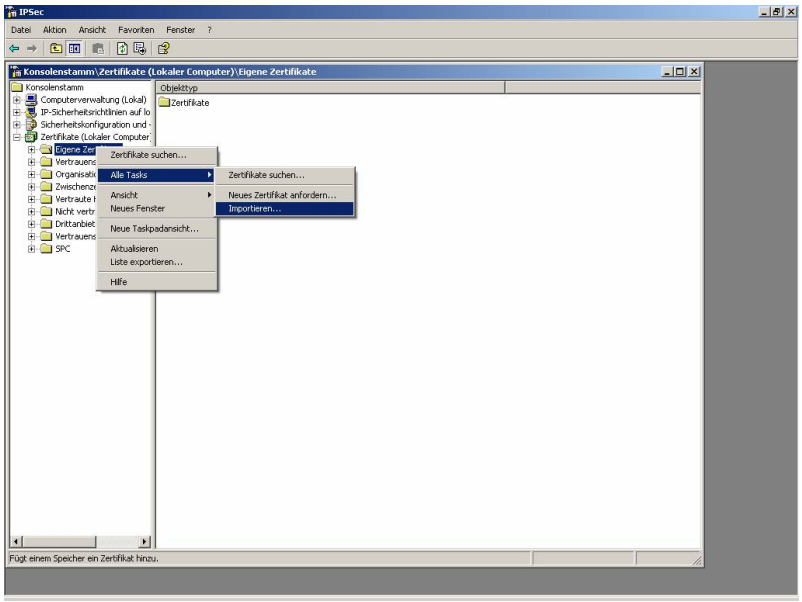


Abbildung 15: Importieren von einem Zertifikat

6. Die Konsoleneinstellungen speichern und schließen

7. In der ipsec.conf sollte nun noch die MAC-Adresse der Wireless LAN Karte des Clients eingetragen werden, da es sonst zu Problemen kommen kann.

8. Abschließend führt man die ipsec.exe aus demselben Verzeichnis aus. Hierdurch wird eine Netzwerkregel erstellt, die den gesamten Datenverkehr über das WLAN Interface verschlüsselt.

9. Um die Funktionalität zu testen, kann man die IP des Servers pingen. Hierbei sollte zunächst die Meldung "IP Sicherheit wird verhandelt" auftauchen, später dann ein normaler Ping-Reply. Natürlich muss man sich zu diesem Test im Bereich des Access-Points befinden.

10. Da es durch die Vergabe der dynamischen Adressen jedes Mal zu einer neuen Route der IPSec Verbindung kommen kann, empfiehlt es sich, zwei Stapelverarbeitungsdateien mit einem Link auf dem Desktop anzulegen. Durch die erste wird, nach erfolgreichem DHCP Handshake die IPSec Route mit der aktuellen IP Adresse erstellt und aktiviert. Mit der zweiten wird diese Route beim Verlassen des Funkbereiches wieder deaktiviert.
    1. Datei: ipsec.exe
    2. Datei: ipsec.exe -off
    Dabei ist darauf zu achten, dass sich die ipsec.conf Datei auf derselben Verzeichnissebene befindet.

Ipsec.conf des Clientrechners
conn roadwarrior # Name der Verbindung
left=%any # Verbindungen von jeder IP starten
right=192.168.23.1 # IP des Gateways
rightca="C=DE, L=Gummersbach, O=FH Koeln, OU=Campus Gummersbach, CN=VPN Gateway Root CA" # Unsere ID
rightsubnet=* # Unser Subnetz
network=lan # Windowsspezifische Einstellungen
auto=start # Verbindung automatisch starten
pfs=yes # Windowsspezifische Einstellungen

9.2 Linux Client

Folgende Schritte müssen unter Linux durchgeführt werden:
Da der Linux-Client zunächst den selben angepassten Kernel wie der Gateway selber benötigt, kann hier exakt wie bei dem Server vorgegangen werden. Daher können die Anweisungen im Abschnitt "Kernel" hier identisch durchgeführt werden.

Die signierte "username.pem", welche ausgehändigt wurde wird das Verzeichnis /etc/ipsec.d/certs/ kopiert.

Anschließend wird der private Schlüssel "username.key" unter /etc/ipsec.d/private/ abgelegt.

Die Datei /etc/ipsec.conf wird jetzt mit folgenden Einstellungen editiert:

Ipsec.conf des Clientrechners
version 2.0 # IPSec Version 2.0 config setup # Standardeinstellungen klipsdebug=none # Debugging für klips aus plutodebug=none # Debugging für pluto aus interfaces=ïpsec0=eth1- # Welches Interface uniqueids=no conn roadwarrior # Name der Verbindung
left=%any # Verbindungen von jeder IP starten
leftrsasigkey=%cert # Wo liegen die Zerifikate
leftcert=username.pem # Unser Zertifikat
right=192.168.23.1 # IP des Gateways
rightsubnet=0.0.0.0/0 # Wohin leiten wir weiter
rightid="C=DE, L=Gummersbach, O=FH Koeln, OU=Campus Gummersbach, CN=VPN Gateway Root CA" # Unsere ID
auto=add

Opportunistic Encryption abschalten:
conn block
auto=ignore
conn private
auto=ignore
conn private-or-clear
auto=ignore
conn clear-or-private
auto=ignore
conn clear
auto=ignore
conn packetdefault
auto=ignore

Hinweis: Eine gute Erklärung der Parameter erhält man auf der Konsole durch den Befehl "man ipsec.conf".

Jetzt starten wir mit "/etc/init.d/ipsec restart" und "/etc/init.d/network restart" IPSec und das Netzwerk neu und die Verbindung steht.

In der Datei /var/log/auth.log werden Informationen über IPSec, die Verbindungen und die Authentifizierung ausgegeben.

10 Mögliche Erweiterungen

Nachdem wir nun ein Grundsystem haben, mit welchen man alle grundlegenden Funktionen benutzen kann, überlegen wir uns nun noch mögliche Erweiterungen für dieses Szenario.

Die nächsten Unterpunkte werden aber nur theoretisch abgehandelt, da sie den Rahmen dieses Schriftstückes sprengen würden.

10.1 Traffic Shaping

Eine Überlegung wäre, über einen Verzeichnisdienst genau festzuhalten, wie viele Daten ein einzelner User aus dem Internet lädt. Dies kann geprüft werden, und je nachdem wie viel ein User im Monat lädt, kann man dynamisch seine Downloadraten begrenzen. Iptables bringt alles mit was gebraucht wird. Die Lösung lässt sich recht einfach über einen LDAP Server und passende Konsolenskripte realisieren.

10.2 OpenCA

Um eine schnelle Anmeldung zu erlauben, könnten wir Usern erlauben, sich ein Zertifikat zu erstellen und dieses dann zur weiteren Signierung an uns zu schicken. Wir könnten dann, über eine zweite Web Ebene dieses Zertifikat freischalten. Damit entfällt einiges an Aufwand. da wir nur noch das Ok geben müssen. Das Projekt OpenCA[7] bietet dieses Funktionalität. Leider befindet sich das Projekt noch im Beta Status, scheint aber schon recht ausgereift zu sein.

10.3 Statistiken

Durch ein kleines Skript kann man Statistiken darüber erstellen, wie lange die einzelnen User online waren. Alle IPSec Verbindungen werden in der Datei "/var/log/auth.log" protokolliert. Ein kleines Skript könnte diese Informationen auslesen und in eine Datenbank schreiben.

10.4 Proxy für Gäste

Man könnte überlegen, auf den Gateway einen Proxy für bestimmte Seiten einzurichten. Damit könnten sich die User z.B. beim Admin melden und ein Zertifikat beantragen. Auch könnte der Proxy genutzt werden, um wichtige Nachrichten zu publizieren, wie Stundenpläne, aktuelle Ausfälle, usw.

Dieses Konzept ließe sich einfach über einen Squid Proxy realisieren. Die Firewall müsste hierzu noch angepasst werden und die Squid-Konfiguration sehr restriktiv eingestellt werden. Danach sollte der Nutzung des WLANs für Gäste nichts mehr im Wege stehen.

10.5 Kernel 2.6.x / racoon

Eine Anpassung an die aktuelle 2.6.x Kernel-Reihe mit dem im Kernel bereits integriertem racoon als IPSec-Implementierung sollte überprüft und getestet werden, um dieses Konzept auch für die Zukunft nutzen zu können. Somit könnte der Server und auch Clientbereich gesplittet werden in die Bereiche Linux mit Kernel 2.4.x und FreeS/WAN, sowie Linux mit Kernel 2.6.x und racoon.

10.6 WPA / Radius

Zu überlegen wäre auch, ob ein Folgeprojekt testet und ausarbeitet, inwieweit sich WPA und eine Authentifikation mit Radius-Server realisieren und in dieses Konzept einbinden liesse.

10.7 Roaming

Ebenfalls kann ein Folgeprojekt testen und ausarbeiten, ob bei mehreren Access-Points eine Einbindung der Roaming-Funktionalität möglich wäre. Damit wäre der Einsatz mehrerer Access-Points ermöglicht, ohne dass Verbindungen abbrechen, wenn zu einem anderen Access-Point übergewechselt wird.
Ideen gibt es also viele... schön wäre es, wenn sie auch alle umgesetzt werden!

[7] http://www.openca.org

11 Sicherheitsanalyse

11.1 SSID und ESSID

Der Standard bietet die Möglichkeit einen Netzwerknamen (ESSID bzw. SSID: (Extended) Service Set Identity) zu vergeben. Dabei gibt es zwei Betriebsarten. Wird durch den Nutzer die Kennung "any" angegeben, akzeptiert die Funk-LAN-Komponente beliebige SSIDs. Im anderen Fall wird der eingetragene Name überprüft und nur Teilnehmer mit der gleichen SSID können am Netzwerk teilnehmen. Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID dazu, den nächsten Access-Point zu finden. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie mit einfachen Mitteln in Erfahrung bringen. Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden. Das Unterdrücken der SSID auf diese Weise ist jedoch nicht standardkonform. Alle Access-Points werden von den Herstellern mit einer vorkonfigurierten SSID ausgeliefert. Alle Cisco Geräte haben z. B. den Namen "tsunami", oder alle Acer Geräte haben den Namen "default". Beim SSID ist auch die erste dünne Sicherheitsschicht zu finden.

Ein leicht zu erratender oder ein bekannter SSID macht das Netz einfacher zu identifizieren. Daher sollte der SSID genau so behandelt werden wie ein Passwort: Es sollte ein langer Text sein der nicht in einem Wörterbuch steht und sich aus beliebigen Zeichen zusammensetzt. Und zwar einschließlich von Buchstaben, Zahlen und Symbolen. Der SSID ist kein wirklicher Sicherheitsschutz und auch nie dafür gedacht gewesen. Er kann, wenn man ihn falsch vergibt, eine Orientierungshilfe für Angreifer sein. Ändert man den vom Hersteller vorgegebenen Namen nicht, dann kann der Angreifer leicht die verwendete Hardware identifizieren und spezifische Sicherheitslöcher leichter ausnutzen. Setzt man den Namen auf einen erklärenden Text wie zum Beispiel 'Firma xyz, Entwicklung, 1. Stock', so macht man es dem Angreifer leichter sich zu orientieren. Stattdessen sollten man also kryptische, nichts sagende Namen für den SSID verwenden: Mit einem Namen wie "sdfT561ö42" rückt man keine Information freiwillig raus und das ist genau das, was man tun sollte.

11.2 MAC

Jede Netzwerkkarte verfügt über eine vom Hersteller vergebene, eindeutige Hardwareadresse. Die so genannte MAC-Adresse (Media Access Control) identifiziert die Netzwerkkarte eindeutig und unverwechselbar. Einige Access-Points unterstützen deshalb die Erstellung einer Positiv-Liste von MAC-Adressen, die sich mit dem Access-Point verbinden und somit Teilnehmer des Funknetzwerkes werden dürfen. Da die Liste der erlaubten MAC-Adressen manuell gepflegt werden muss, ist ein nicht unerheblicher Aufwand erforderlich, der die Verwendung von Positiv-Listen auf Basis der MAC-Adressen in vielen Einsatzszenarien unmöglich macht. Außerdem lassen sich die MAC-Adressen (z.B. 00:40:CA:BE:82:30) durch den Einsatz spezieller Software (z.B. ifconfig unter Unix/Linux und smac unter Microsoft Windows) bewusst fälschen und bieten somit keinen ausreichenden Schutz.

Für die Zukunft kommt noch das 802.1X Protokoll ins Spiel. Dieses Protokoll macht die Sache deutlich sicherer, denn die Authentifizierung wird dabei auf völlig anderem Wege gelöst. Es gibt verschiedene Möglichkeiten 802.1X im LAN zu implementieren. So ist zum Beispiel beim Windows 2000 Server der benötigte Internet Authentification Server (IAS Server) mit den für 802.1X notwendigen Diensten dabei.

Problematisch daran ist allerdings, das längst nicht alle (praktisch keiner) der günstigen Access-Points dieses Protokoll unterstützen. Damit es aber auch tatsächlich eingesetzt werden kann, ist die Unterstützung durch den Access-Point Voraussetzung. Im Endeffekt läuft das darauf hinaus, dass 802.1X momentan nur in größeren Firmennetzen eingesetzt werden kann, bei denen eben nicht die preisgünstigen Access-Points verwendet werden. Nur weil der benötigte Server in Form von Software vorhanden ist, kann man mit dem Protokoll nicht viel anfangen. Leider ist auch dieses System nicht vollständig sicher. Erste Untersuchungen zeigen, dass auch dieses System Schwachstellen für Man-In-The-Middle Angriffe und Session Hijacking aufweist.

11.3 WEP

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

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

- **Vertraulichkeit**: Aus dem Schlüssel und dem IV wird ein pseudozufälliger Bitstrom generiert. Die Chiffratdaten ergeben sich, indem die Klardaten bitweise mit dem Bitstrom XOR-verknüpft werden (XOR = exklusives Oder). Beim Empfänger werden die Klardaten wiederum aus den Chiffratdaten ermittelt, indem derselbe Bitstrom mit den Chiffratdaten XOR-verknüpft wird.

- **Integrität**: Für jedes zu übertragene Datenpaket wird eine 32-Bit CRC-Checksumme berechnet. Anschließend wird das Datenpaket mit der angehängten Checksumme verschlüsselt. Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Ist die Checksumme korrekt, wird das Datenpaket angenommen, andernfalls wird es verworfen.

- **Authentisierung**: In Verbindung mit der WEP-Verschlüsselung kann zwischen zwei Authentisierungsmodi gewählt werden: "Open" (hierbei findet keine Authentisierung statt) und "Shared Key". Für die Authentisierung im "Shared Key"-Modus wird ein sog. Challenge-Response-Verfahren durchgeführt: Der Access-Point generiert 128 zufällige Bytes und sendet diese in einem Datenpaket unverschlüsselt an einen Client (Challenge). Der Client verschlüsselt das Datenpaket und sendet es zurück zum Access-Point (Response). Der Client hat sich erfolgreich authentisiert, wenn der Access-Point die Response zur Challenge entschlüsseln kann.

Der Authentisierungsprozess ist nur einseitig: der Access-Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten. (Siehe nachfolgende Abbildung)

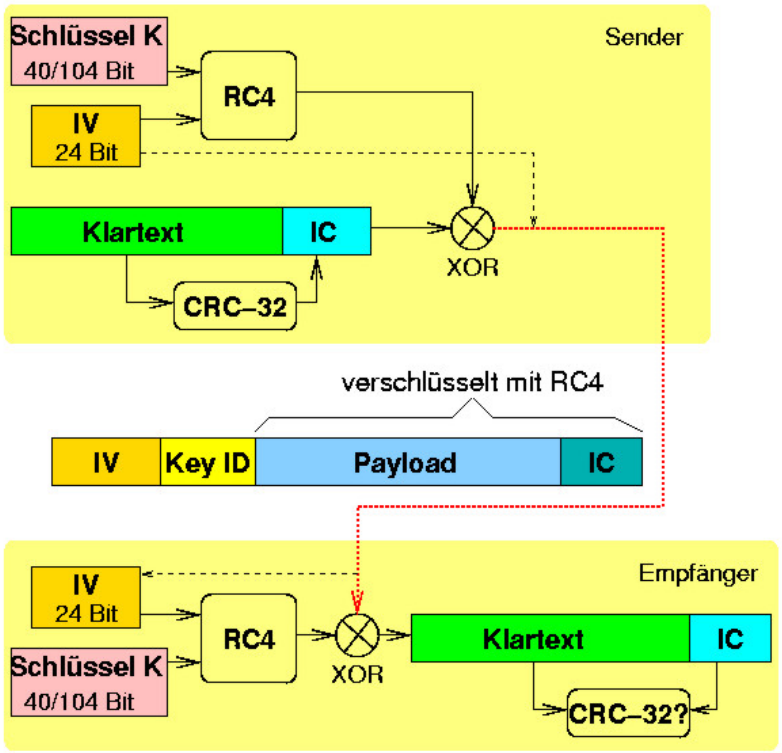


Abbildung 16: WEP

Mit diesen beiden Informationen kann der Angreifer den RC4 Algorithmus verwenden und gelangt so an den für die Verschlüsselung verwendeten Schlüssel. Ist der Schlüssel nun aber bekannt, dann ist auch sofort der WEP Schlüssel

bekannt. Ein Einbruch in die Authentifizierung macht also nicht nur diese sondern auch gleich noch die WEP Verschlüsselung hinfällig. Das interessante Resultat davon ist, dass man besser gar keine Authentifizierung verwendet, denn dadurch schützt man zumindest das später verwendete WEP Verfahren. Das bedeutet paradoxerweise, dass die sicherste Methode der Authentifizierung innerhalb von WLAN die 'open' Methode ist, bei der sich jedermann mit dem Access-Point unterhalten kann. Auch wenn es seltsam klingt, dass man eine Sicherheitsschicht entfernen soll um sicher zu werden: Diese spezielle Schicht ist derartig fehlerhaft, dass das Entfernen der Schicht die Lage sicherer macht!

11.4 Sicherheitsprobleme

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

- Sicherheitskritische Grundeinstellung
  - Im Auslieferungszustand sind die Funk-LAN Komponenten häufig so konfiguriert, dass keine oder nur einige der zudem schwachen Sicherheitsmechanismen aktiviert sind.
- SSID Broadcast
  - Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das Funk-LAN vor Unbefugten zu verstecken (so genanntes "Closed System"). Dieser Schutz wirkt gegen diverse frei verfügbare Tools wie z. B. NetStumbler, jedoch kann mittels Funk-LAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.
- Manipulierbare MAC Adressen
  - Jede Netzwerkkarte verfügt über eine eindeutige Hardwareadresse die sog. MAC-Adresse (Media Access Control-Adresse). Diese MAC-Adressen der Funk-Clients können relativ einfach abgehört und manipuliert werden, somit sind die in den Access-Points zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar.
- Verwendung nur eines Schlüssels
  - Der WEP-Standard sieht zwar die Verwendung von bis zu vier Schlüsseln vor. Die Angabe des Indexes zur Signalisierung, welcher Schlüssel bei der aktuell verschlüsselten Nachricht verwendet wird, macht es jedoch erforderlich, dass die Schlüssel auf allen Stationen in der gleichen Reihenfolge eingetragen sind. Deshalb wird in der Praxis oft nur ein Schlüssel verwendet.
- Kein Wirkliches Geheimnis
  - Zur Kommunikation mit einem der Access-Points des Basic Service Sets (BSS) verwenden die mobilen Stationen einen der vier geheimen Schlüssel. Der Schlüssel ist nicht nur für die jeweilige Station geheim, sondern jeder Netzteilnehmer teilt sich das Wissen über den "geheimen" Schlüssel auch mit allen anderen Rechnern des BSS. Von einem Geheimnis kann also keine Rede sein!
- kein Schlüsselmanagement
  - Die gemeinsamen, geheimen Schlüssel müssen manuell in jeder Station eingetragen werden, da der Standard kein Schlüsselmanagement vorsieht. Bei einer Kompromittierung, z. B. durch Diebstahl einer Karte, muss der Netzadministrator die WEP-Schlüssel auf allen mobilen Clients per Hand ändern oder die Nutzer zum Ändern veranlassen. Ohne Zweifel ist dies für die Verwaltung zu aufwendig und fehleranfällig.
- keine individuelle Authentifizierung
  - Wenn alle Stationen den/die gleichen Schlüssel verwenden, dann ist eine Authentifizierung eines einzelnen, individuellen Nutzers nicht möglich. Hinzu kommt, dass bereits durch den Besitz einer WLAN-Karte (z. B. durch Abhandenkommen eines Laptops) dem Angreifer der Zugang zum Funknetz geöffnet wird.

- Keine Authentifizierung des Netzes gegenüber Nutzer
  - Die mobilen Stationen authentifizieren sich zwar mehr oder weniger gegenüber dem Access-Point, eine genauere Identifikation des Access-Points gegenüber dem Nutzer erfolgt jedoch nicht. Diese Designschwäche eröffnet dem Angreifer die Möglichkeit, Spoofing-Angriffe erfolgreich durchzuführen.
- Lieferung Klartext-Kryptopaar
  - Bei der Shared Key Authentication sendet die mobile Station die vom Access-Point erhaltene Zufallszahl verschlüsselt zurück. Da für die Verschlüsselung der Challenge-Response der gleiche Schlüssel verwendet wird wie für die Verschlüsselung aller anderen Datenpakete, erhält der Angreifer auf einfache Weise ein Klartext-Kryptopaar, das er für weitergehende Angriffe nutzen kann.

11.5 Schwachstellen im RC4 Design

Der RC4 Algorithmus stammt aus dem Jahre 1987 und wurde damals von Ron Rivest erfunden. Lange Zeit wurde der RC4 damals geheim gehalten und nicht weitergegeben bis es schließlich mit Hilfe unbekannter Quellen ein Sicherheitsleck gab und der Algorithmus veröffentlich wurde. Das war im Jahre 1994 - und auch mehr oder minder das Ende der RC4 Sicherheit. Jahre später entschloss sich die Industrie den RC4 für die WEP Verschlüsselung einzusetzen, und genau daraus resultierten einige der WEP Sicherheitsprobleme. RC4 war schon längere Zeit Grundlage für Veröffentlichungen, und nach der offiziellen Verwendung von RC4 in WLANs dauerte es nicht lange, bis sich ein weiteres Paper den zuvor veröffentlichten anschloss. In diesem Paper von Scott Fluhrer (Cisco), Itsik Mantin und Adi Shamir (beide Weizmann Institut), beschreiben die Autoren, dass der RC4 Algorithmus an einer Reihe von Schwachstellen leidet. Die beiden wichtigsten davon sind die Folgenden:

- Im Rahmen des RC4 gibt es eine Reihe an "schwachen" Schlüsseln die verwendet werden, es einem Angreifer aber erlauben, die eigentliche für die Verschlüsselung verwendete Ziffer zu errechen. Dazu muss der Angreifer zuvor aber eine Reihe an mit diesen schwachen Schlüsseln verschlüsselten Daten sammeln.
- Kennt ein Angreifer einen Originaltext und das zugehörige mit dem RC4 verschlüsselte Gegenstück, so kann er den verwendeten Schlüssel direkt und ohne Umwege ermitteln. (Das ist bei einer eingeschalteten Authentifizierung im Access-Point der Fall.)

Der IV hat nur 24 Bits und daher gibt es nur eine feste Menge an Permutationen die der RC4 für den IV verwenden kann. Mathematisch gesehen gibt es gerade einmal 16.777.216 (2 hoch 24) mögliche Kombinationen für den IV. Das klingt natürlich nach viel aber auf der anderen Seite sind 16 Millionen Pakete nun auch gerade keine große Zahl: Je nach Aktivität des Clients sprechen wir hier von einigen Stunden, maximal einigen Tagen. Die Wissenschaftler Fluhrer, Mantin und Shamir fanden heraus, dass es so genannte schwache Initialisierungsvektoren gibt, die mit einer fünfprozentigen Trefferwahrscheinlichkeit Hinweise auf ein Byte des Schlüssels geben und somit die komplette Entschlüsselung des WEP-Schlüssels ermöglichen. Um einen Angriff erfolgreich durchzuführen, muss ein Angreifer etwa vier bis sechs Millionen Datenpakete des Funknetzes passiv abhören. Dabei ist die für den Angriff benötigte Zeit nicht nur von der Anzahl der abzuhörenden Pakete abhängig, sondern im Wesentlichen auch von der durchschnittlichen Paketgröße und Auslastung des Access-Points. Die folgenden Tabellen zeigen eine Abschätzung der Dauer eines passiven Angriffs in Abhängigkeit der benötigten Datenmenge, der Anzahl der Pakete und der durchschnittlichen Paketgröße:

	Paketgröße		
Anzahl Pakete	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 17: Benötigte Datenmenge in Abhängigkeit von der durchschnittlichen Paketgröße und der Anzahl der Pakete

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

Abbildung 18: Benötigte Zeit in Abhängigkeit von der Datenmenge und der durchschnittlichen Auslastung des Access-Points für 802.11b Systeme

Die Tabellen zeigen, dass es einem Angreifer möglich ist, den kompletten WEP-Schlüssel zu ermitteln, wenn er ausreichend schwache Initialisierungsvektoren (ca. 1500) gefunden hat. Bei einer durchschnittlichen Paketgröße von 1024 Byte und einer Gesamtmenge von ca. vier Millionen Datenpaketen sind demnach etwa 3,81 GB an abgehörten Daten notwendig, um einen erfolgversprechenden Angriff auf den RC4-Algorithmus durchführen zu können. Bei einem Access-Point mit einer mittleren Auslastung von 1 Mbit/s benötigt der Angriff etwa 8,47 Stunden.

11.6 Nachteile von WLANs

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

- Unkontrollierte Ausbreitung der Funkwellen
  - Auch über die spezifizierte Reichweite von 10 - 150 Metern hinaus breiten sich die Funkwellen der Funk-LAN-Komponenten aus und können je nach Umgebungsbedingungen und der Leistungsfähigkeit der verwendeten Empfangsgeräte empfangen werden. Dies bedeutet, dass auch über die Nutzreichweite der Funk-LANs hinaus eine konkrete Abhörgefahr besteht.
- Bedrohung der Verfügbarkeit
  - Funk-LANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die Funk-LAN Kommunikation stören und im Extremfall den Betrieb des Funk-LANs verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z. B. Bluetooth Geräte, andere Funk-LANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras, etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff erfolgen. Darüber hinaus sind Denial-Of-Service-Angriffe auch möglich durch wiederholtes Senden bestimmter Steuer- und Managementsignale.
- Erstellung von Bewegungsprofilen
  - Da die Hardwareadresse einer Funk-LAN-Karte, die sog. MAC-Adresse, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können Bewegungsprofile über mobile Nutzer, die sich in öffentliche Hot Spots einbuchen, erstellt werden. Da die MAC-Adresse grundsätzlich unverschlüsselt übertragen wird, ist das Erstellen von Bewegungsprofilen keinesfalls nur den Betreibern der Hot Spots möglich. Prinzipiell kann jeder, der an geeigneten öffentlichen Plätzen eine Funk-LAN-Komponente installiert, die MAC-Adressen anderer Nutzer mitlesen. Sendet der Nutzer zusätzlich personenbezogene Daten unverschlüsselt über das Funknetz, können auch diese mitgelesen und mit dem Bewegungsprofil zusammengeführt werden.

11.7 Sichere Konfiguration der Komponenten

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

- Standard SSID ändern (am Access-Point und bei allen Clients): Die SSID sollte keine Rückschlüsse auf Firma oder Netzwerk zulassen.
- Standard Passwort zur Konfiguration des Access-Points ändern
- SSID Broadcast am Access-Point abschalten - falls technisch möglich
- MAC Adress-Filterung am Access-Point einschalten - falls technisch möglich
- WEP Verschlüsselung einschalten - falls möglich 128 Bit
- In Verbindung mit der WEP Verschlüsselung ist, falls technisch möglich die Authentisierungsmethode "Open" zu wählen, da die Option "Shared Key" zusätzliche Sicherheitsprobleme birgt.
- WEP Schlüssel periodisch wechseln. Hinweis: WEP Schlüssel, SSIDs und Zugangspassworte sollten entsprechend anerkannter Passwortgestaltungsregeln so gewählt werden, dass sie einen möglichst wirksamen Schutz gegen Angreifer bieten.
- Aufstellort und Antennencharakteristik des Access-Points sollten so gewählt werden, dass möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Dabei ist zu beachten, dass sich die Funkwellen sowohl horizontal als auch vertikal ausbreiten.
- Die Sendeleistung am Access-Point sollte, falls technisch möglich reduziert werden, damit nach Möglichkeit nur das gewünschte Gebiet funktechnisch versorgt wird. Hierbei ist zu beachten, dass zur Erzielung der maximalen Datenübertragungsrate ein bestimmtes Signal-Rauschverhältnis erforderlich ist.

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

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

- Beim Einsatz mehrerer Access-Points sind die benutzten Frequenzkanäle benachbarter Access-Points möglichst überlappungsfrei zu wählen.

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

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

Durch korrekte Konfiguration und Administration der Funkkomponenten des Funk-LANs können trotz bekannter Unzulänglichkeiten viele Angriffe abgewehrt werden, die mit frei verfügbaren Tools durchführbar sind. Dadurch wird Schutz gegen unbeabsichtigtes Einloggen in ein Funk-LAN und gegen Mithören des Funk-LAN-Datenverkehrs durch Gelegenheitslauscher erreicht. Die Verfügbarkeit des Systems kann mit diesen Maßnahmen ggf. geringfügig erhöht werden, bleibt aber dennoch leicht angreifbar. Diese Maßnahmen reichen jedoch im Allgemeinen nicht aus zum Schutz von sensiblen Daten. Eine Ausnahme bildet ein Firmwareupgrade auf einen neuen Sicherheitsstandard wie WPA oder 802.11i. In Behörden- und Firmennetzen mit einer größeren Anzahl von Benutzern sind darüber hinaus einige Maßnahmen nicht im erforderlichen Umfang praktikabel. In diesen Fällen sind weitere Maßnahmen erforderlich.

11.8 Angriffsszenarien

Die möglichen Angriffe auf drahtlose Funknetzwerke lassen sich prinzipiell in fünf Hauptkategorien einteilen:

- Unautorisierte Hardware (engl.: insertion attack)

  - Die Gefahr durch unautorisierte Hardware besteht in dem Anschluss von drahtlosen Geräten (z.B. Access-Points) an das Firmennetz, die zuvor keinen firmeninternen Sicherheitsprozess durchlaufen haben, beziehungsweise keiner Sicherheitsüberprüfung durch den Systemadministrator unterzogen worden sind. Dabei kann die unautorisierte Hardware entweder durch den Angreifer selbst oder einen unbedachten Firmenmitarbeiter installiert werden, der beispielsweise die Reichweite eines drahtlosen Netzwerkes nach seinen Wünschen vergrößern oder überhaupt ein drahtloses Netzwerk in Betrieb nehmen möchte. Ein unerlaubt installierter Access-Point wird Rogue Access-Point (verbrecherischer Zugangspunkt) genannt, weil ein Angreifer dadurch die gesamten Sicherheitsvorkehrungen einer Firma unterwandern kann. Sobald ein Angreifer einen solchen Zugangspunkt zum Netzwerk gefunden hat, wird dieser durch den unautorisierten Einsatz von Clients versuchen, mit seinem drahtlosen Endgerät eine Verbindung zu einem Access-Point des Firmennetzes aufzubauen und von dort in das gesamte (Firmen-) Netzwerk einzudringen.

- Abfangen und Manipulation des drahtlosen Netzwerkverkehrs (engl.: interception and monitoring wireless traffic)

  - Das Abhören und die Manipulation von Daten ist eine beliebte Attacke in drahtgebundenen und drahtlosen Netzwerken. Durch so genannte Snifferprogramme (z.B. ethereal, Airopeek) bzw. Netzwerk-Analyseprogramme kann ein Angreifer, sofern sich seine Funknetzwerkkarte im so genannten "Promiscuous Mode" betreiben lässt, den gesamten Datenverkehr in der Abstrahlungsfläche eines drahtlosen Netzwerkes abhorchen. Eventuell vorhandene WEP-Schlüssel, die den unerlaubten Zugang zu einem drahtlosen Netzwerk verhindern sollen, können mit frei verfügbaren Werkzeugen (z.B. AirSnort) überwunden werden. Sobald ein Angreifer in der Lage ist, die drahtlose Kommunikation abzufangen und die

notwendigen Autorisierungsdaten zu ermitteln (z.B. durch Entschlüsseln des WEP-Schlüssels), kann dieser manipulierend in eine bestehende Netzwerkverbindung (z.B. ARP-Spoofing) eingreifen und eine aktuell laufende Kommunikationssitzung eines Nutzers übernehmen (Hijacking). Die Übernahme einer bestehenden TCP- oder UDP-Verbindung ist selbst dann möglich, wenn diese verschlüsselt (z.B. SSL oder SSH-Verbindung) erfolgt (Man in the middle-Attacke). Des weiteren kann sich das Mitschneiden des Netzwerkverkehrs nicht nur auf das drahtlose Funknetz beschränken, da ein Angreifer mittels "Broadcast Monitoring" auch den Netzwerkverkehr des drahtgebundenen Netzwerkes mitlesen kann, wenn vom Access-Point eine Verbindung (z.B. via Hub/Switch) in das drahtgebundene Netzwerksegment existiert.

- Fehlkonfigurationen (engl.: misconfiguration) und bekannte Sicherheitslücken der Access-Points

  – Viele drahtlose Endgeräte sind im Auslieferungszustand für eine schnelle, einfache und reibungslose Inbetriebnahme konfiguriert, d.h. eventuell vorhandene Sicherheitsmechanismen (z.B. WEP) sind weitestgehend deaktiviert. Da die Hersteller auf die aus Kompatiblitätsgründen deaktivierten Schutzmaßnahmen nicht bzw. nur unzureichend hinweisen wissen viele Anwender nicht um die Gefahren, die durch die Ausschaltung der Sicherheitstechniken entstehen. Außerdem ist, falls ein Access-Point diese Funktionalität überhaupt bietet, die automatische IP-Adressvergabe via DHCP (Dynamic Host Configuration Protocol) in vielen Fällen eingeschaltet, damit ein Anwender im lokalen Netzwerk nicht manuell die IP-Adressen zuweisen muss und eine möglichst problemlose Datenkommunikation zwischen den einzelnen Teilnehmern des drahtlosen Netzwerkes möglich ist. Diese Funktion, die eigentlich unerfahrenen Anwendern den Betrieb eines drahtlosen Netzwerkes erleichtern soll, kann von einem Angreifer missbraucht werden, um selbst unerlaubterweise Teilnehmer eines Funknetzes zu werden.

    Des weiteren verwenden viele Firmen und Privatleute anstatt einer alphanumerischen Zeichenkette, einen Begriff aus dem Wörterbuch bzw. aus ihrem Firmen- oder Privatumfeld als WEP-Schlüssel und werden somit bewusst oder unbewusst anfällig für eine "Brute Force"- oder Dictionary-Attacke. Bei einer Brute Force bzw. Dictionary-Attacke versucht ein Angreifer, Zugang zu einem passwortgeschützen System zu erlangen, indem er automatisiert eine große Anzahl Passwörter durchprobiert, bis er das richtige Passwort gefunden hat. Ein Angreifer hat es noch leichter, wenn der Betreiber eines Funknetzwerkes das durch den Hersteller eines Access-Points vorgegebene Passwort überhaupt nicht ändert, da im Internet Listen mit den entsprechenden Standardpasswörtern[8] kursieren. Zusätzlich besitzen manche Programmteile der auf einigen Access-Points verwendeten Betriebssysteme zum Teil erhebliche Sicherheitslücken, die auf unsaubere Programmierung zurückzuführen sind. Ein Angreifer kann beispielsweise durch speziell präparierte Anfragen sensible Administrationsdaten (z.B. Passwörter) abfragen oder ganze Konfigurationsdaten aus dem Access-Point auslesen.

    Leider verwenden Hardwarehersteller teilweise auch Standard- oder Masterpasswörter, welche nur durch ein Firmwareupdate geändert werden können. Hierzu sei Beispielhaft auf einige Newstickermeldungen[9][10][11] verwiesen.

- Blockierung (engl.: jamming)

  – Das gezielte Blockieren (engl.: jamming) eines Access-Points bzw. der übertragenen Funkwellen stellt ein großes Problem dar. Ein Angreifer kann einen Access-Point mit einer so genannten "Denial of Service"-Attacke lahmlegen, indem er den Access-Point über einen längeren Zeitraum mit einer großen Anzahl Paketen bombardiert, bis dieser unter der Last zusammenbricht und damit das gesamte, funkbasierte Netzwerk lahmlegt. Derartige Störungen können, gewollt oder ungewollt, auch durch andere Quellen (z.B. schnurlose Telefone etc.) entstehen, die den gleichen Frequenzbereich verwenden.

- Client-Client Attacke (engl.: client to client attacks)

  – Alle Teilnehmer eines funkbasierten Netzwerkes speichern die sensiblen Zugangsdaten (z.B. WEP-Schlüssel), die zur Authentifizierung und Kommunikation mit einem Access-Point verwendet werden, lokal zwischen. Da viele Hersteller die Zugangsdaten auf den Festplatten der Teilnehmer komplett ohne oder nur mit einer sehr schwachen Verschlüsselung versehen, kann ein Angreifer durch das gezielte

[8] http://www.phenoelit.de
[9] http://www.heise.de/newsticker/meldung/48005
[10] http://www.heise.de/newsticker/meldung/47941
[11] http://www.heise.de/newsticker/meldung/46388

Ausnutzen einer Schwachstelle des Betriebssystems eines Teilnehmers in den Besitz der Zugangsdaten gelangen. Des weiteren sind alle lokalen Daten auf den Festplatten der einzelnen Teilnehmer des Funknetzes prinzipiell bedroht, sofern diese nicht mit besonderen Maßnahmen geschützt sind (z.B. Dateisystemverschlüsselung). Der Einbruch in ein funkbasiertes Netzwerk erfolgt entweder durch Ausnutzung einer bekannten Schwachstelle der vorgestellten Sicherheitsmechanismen (z.B. schwache Initialisierungsvektoren im WEP-Protokoll) oder durch einen gezielten Angriff gemäß der identifizierten Angriffsvarianten. Den schematischen Ablauf eines typischen Angriffs auf ein drahtloses Netzwerk veranschaulicht die Grafik in Anhang A.

11.9 Erweiterungen zum WEP

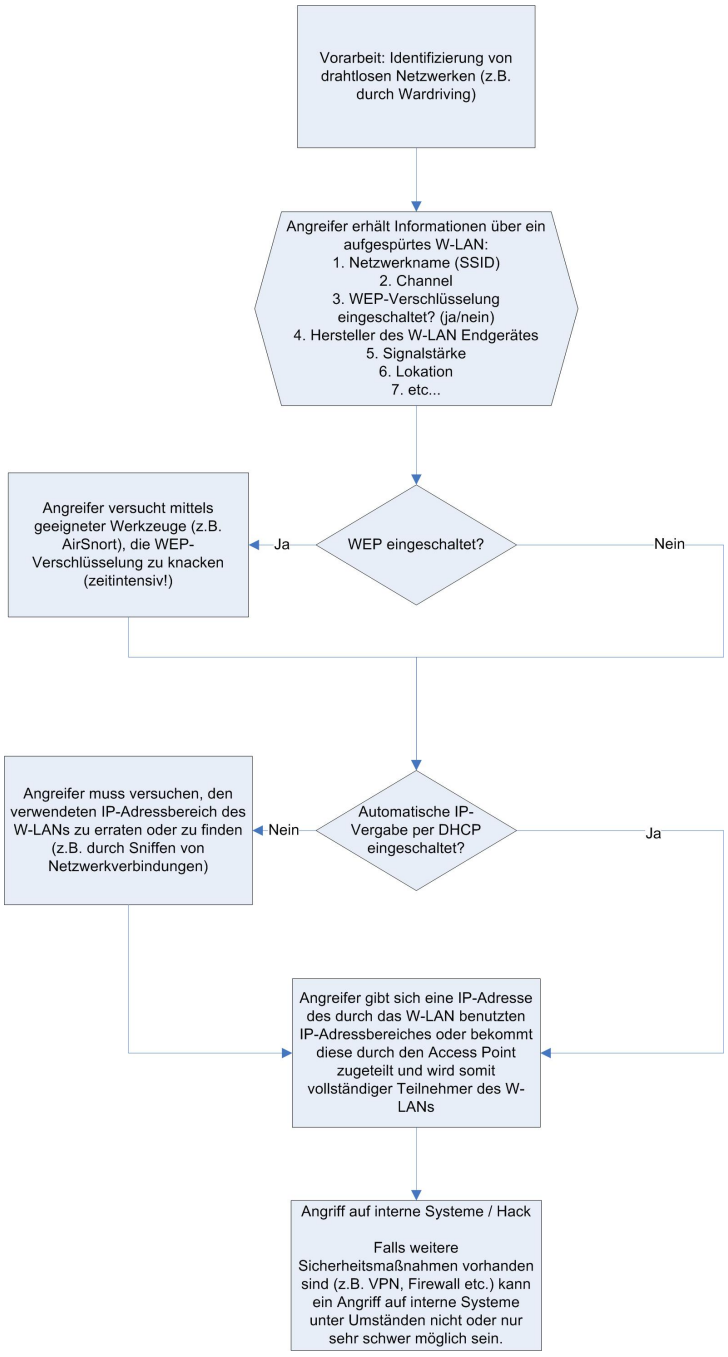
- SSH-Tunneling
  - Mit Hilfe eines SSH-Tunnels kann eine verschlüsselte Verbindung auf Transportebene herstellerunabhängig aufgebaut werden. Durch diesen verschlüsselten Tunnel können nach Aufsetzen sensible Anwendungen geschleust werden, die ihre Daten sonst, da im Klartext gesendet, dem Angreifer aufgrund der zusätzlichen Unsicherheit von WEP preisgeben würden.
- VPN
  - Mit einem VPN (Virtual Private Network) in Form von IPsec werden ebenfalls Tunnel mit Verschlüsselung aufgesetzt. Jedoch arbeiten diese Tunnel nicht auf der Socket-/Transportebene, sondern eine Ebene tiefer, auf der IP-/Netzwerk-Ebene. VPNs werden meist dazu eingesetzt, um verschiedene Subnetze bzw. die verschiedenen Niederlassungen einer Firma über ein unsicheres Netz miteinander zu verbinden. Der Verkehr über das unsichere Netzwerk erfolgt innerhalb von Tunneln, die zwischen den VPN-Gateways aufgebaut werden.
- 802.1X
  - IEEE 802.1X ist das Herzstück der neuen Sicherheitsarchitektur der IEEE, des Robust Security Networks (RSN). Es ist ein Framework, das für die IEEE 802-Protokollfamilie sichere Zugriffskontrolle, Authentifizierung sowie Schlüsselmanagement bieten soll. Die Sicherheitsbeschränkungen finden auf der MAC-Ebene statt. Damit prädestiniert sich 802.1X als Erweiterung zu WEP.
- 802.11i
  - 802.11i ist das neue Sicherheitsprotokoll für Wireless LANs. Aufgrund der vielen Sicherheitslöcher in WEP und der hohen Anzahl der bisher eingesetzten W-LANs mit dem 802.11b Standard wird es 2 Versionen des neuen Protokolls geben.
    1. TKIP - ein WEP-Patch für existierende Hardware
    2. CCMP - Nachfolger von WEP und TKIP

Alte Systeme können so auch von den neuen Sicherheitselementen profitieren. Insgesamt wird WEP um 4 Sicherheitselemente erweitert. Die Grundelemente von WEP, nämlich der RC4-Algorithmus zur Verschlüsselung und das Zusammenspiel von WEP-Schlüssel und Initialisierungsvektor mussten beibehalten werden, da diese Funktionen in fast allen Access-Points in Hardware implementiert sind - wie sonst könnte die schmalbrüstige Ausstattung gängiger Access-Points den CPU-intensiven RC4-Verschlüsselungsalgorithmus ausführen. TKIP adaptiert vier Algorithmen, die altbewährten Konzepten entstammen und platziert diese mit leichten Anpassungen (durch die Hardware bedingt) um WEP:

1. Message Integrity Code (MIC), ≫Michael≪ genannt
   - Fälschungen erkennen
2. Neue Paketsequenzkontrolle
   - Replay-Attacken verhindern
3. Per-Packet-Key-Mixing
   - Korrelation zwischen im Klartext versandtem IV und Chiffrierschlüssel (WEP-Basis-Schlüssel + IV) beseitigen
4. Re-keying für frische Chiffrier- und Integritätsschlüssel
   - Key re-use unterbinden

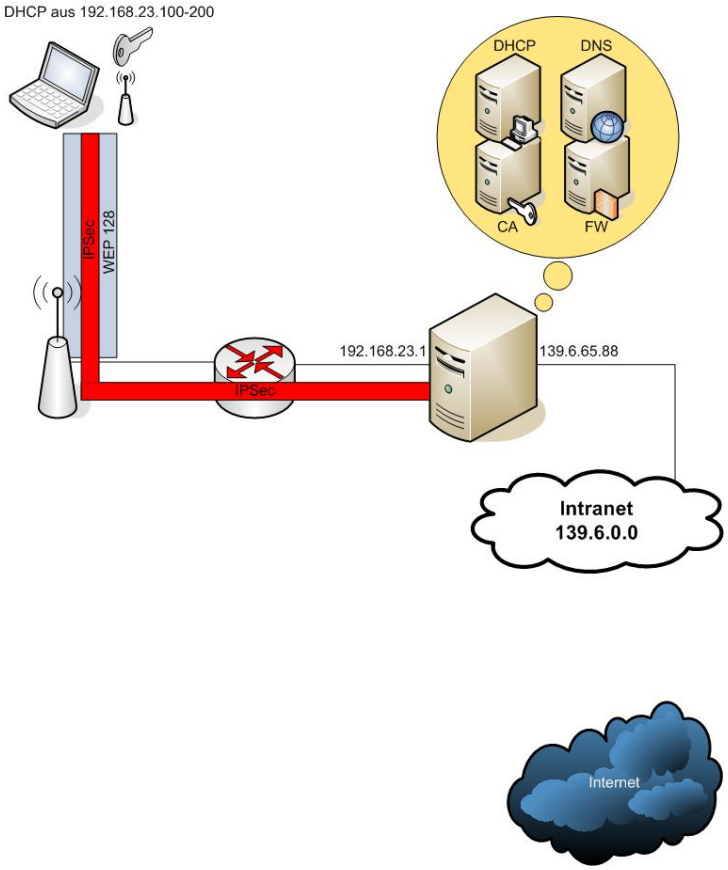
A Angriffsschema

Hier ein Schema, nach dem ein Angriff in der Regel erfolgt.



B Einsatzumgebung

Hier die Einsatzumgebung des Projekts mit anzeige der gesicherten Verbindungen und Funktionalitäten.



C Literatur

1. Entwicklungsgeschichte der WLAN-Standards
   - http://www.tecchannel.de/netzwerk/networkworld/technologyupdate/1125/
2. Symbole Warchalking
   - http://www.warchalking.org/story/2002/8/20/17730/3808
3. Schwachstellen RC4
   - http://www.wisdom.weizmann.ac.il/ itsik/RC4/Papers/Rc4_ksa.ps
4. Bundesamt für Sicherheit in der Informationstechnik
   - http://www.bsi.bund.de/literat/doc/drahtloskom/drahtloskom.pdf
5. TU-Chemnitz, Wireless Local Area Networks
   - http://rnvs.informatik.tu-chemnitz.de/wlan/index.htm
6. TU-Dresden, Sicherheit von Wireless LANs
   - http://tux.wh17.tu-dresden.de/ sebi/pub/Sicherheit-WLAN.pdf
7. Lösungsansätze für das Wave-LAN Security Desaster
   - http://www.cryptolabs.org/wep/WeisOhligWLANsecurity.pdf
8. Wave-LAN: Wireless Encryption Placebo
   - http://ds.ccc.de/075/wireless-enc-placebo
9. Cryptolabs Wave-LAN Security
   - http://www.cryptolabs.org/wep/
10. Verbesserte WLAN Sicherheit mit WPA, EAP und 802.11i
    - http://www.franken.de/de/veranstaltungen/kongress/2003/03-3-1-wlan-wpa.pdf
11. BSI: Sicherheit im Funk-LAN
    - http://www.bsi.de/literat/doc/wlan/wlan.pdf
12. Secure Wireless LAN (WLAN)
    - http://www.infoguard.com/docs/dokumente/NCP_Wlan_d.pdf
13. Wireless LAN Security : 802.11b and Corporate Networks
    - http://documents.iss.net/whitepapers/wireless_LAN_security.pdf
14. Cracking WEP Keys : Applying Known Techniques to WEP Keys
    - http://www.lava.net/ñewsham/wlan/WEP_password_cracker.ppt
15. SSID Defaults
    - http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/ssid_defaults-1.0.5.txt
16. AirSnort Homepage
    - http://airsnort.shmoo.com/

17. WEPCrack Homepage
    - http://wepcrack.sourceforge.net/
18. OpenCA Homepage
    - http://www.openca.org/
19. OpenSSL Homepage
    - http://www.openssl.org/
20. Debian GNU/Linux Anwenderhandbuch
    - http://www.openoffice.de/linux/buch/
21. FIAIF Homepage
    - http://www.fiaif.net/
22. FreeS/WAN Homepage
    - http://www.freeswan.org
23. Super FreeS/WAN
    - http://www.freeswan.ca/code/super-freeswan/
24. IPSec Einrichtung mit racoon für Linux 2.6, FreeBSD und Mac OS X
    - http://mopoinfo.vpn.uni-freiburg.de/docs/ipsec-racoon.php
25. WarChalking.org
    - http://www.warchalking.org/
26. Wardriving.com
    - http://www.wardriving.com

D Glossar

3DES *3DES* ist die Verbesserung des symmetrischen DES-Verschlüsselungsverfahrens, bei dem der DES-Algorithmus drei mal angewendet wird, um eine höhere Sicherheit zu erreichen.

802.1X *802.1X* (Port based Network Access Protocoll) ist ein Entwurf für eine Authentisierungsnorm. Dieser bezieht sich auf den Port, und wird zur Zeit von Microsoft in das Betriebssystem Windows XP implementiert.

802.11 *802.11a* bezeichnet einen Industriestandard für drahtlose Netzwerkkommunikation.

802.11a *802.11a* - Erweiterung der physikalischen Schicht, 1999 veröffentlicht (54 Mbit/s im 5-GHz-Band)

802.11g *802.11g* - Erweiterung der physikalischen Schicht (54 MBit/s im 2,4-GHz-Band)

802.11h *802.11h* - Reichweitenanpassung, Indoor- und Outdoor-Kanäle (im 5-GHz-Band)

802.11i *802.11i* - Erweiterungen bezüglich Sicherheit und Authentifizierung

Access-Point Der *Access-Point* ist ein Gerät, über das Benutzer mit Funk-basierten Geräten auf ein Kabel-basiertes LAN zugreifen können.

ad-hoc Mode *ad-hoc Mode* ist ein WLAN Modus, in dem verschiedene Clients untereinander kommunizieren.

ARPspoofing *ARPspoofing* ist das Senden von gefälschten ARP-Paketen.

Bridge Die *Bridge* ist ein Verbindungsrechner zwischen zwei gleichartigen Netzen (also zum Beispiel zweier Ethernets oder zweier Token Rings), meist zwischen zwei Local Area Networks (LANs).

Broadcast *Broadcast* Broadcast (Sendung) nennt man eine Übermittlung an alle Teilnehmer innerhalb eines Verteilers oder Netzwerks.

BSS Das *BSS* BSS (Base Station Subsystem) umfasst den funkbezogenen Teil eines GSM-Netzes.

CA *CA* (Certificate Authority) ist eine Instanz, die Zertifikate verwaltet.

CCK *CCK* (Complimentary Code Keying))ist ein effizientes Kodierungsverfahren.

CCMP *CCMP* ist der Nachfolger von WEP und TKIP.

CPU Die *CPU* (dt.: Prozessor) ist die zentrale Rechen- und Steuereinheit eines Computers. Sie besteht aus einem oder mehreren Mikroprozessoren (Chips), die die Befehle der Programme interpretieren und ausführen.

CRC *CRC* ist ein Verfahren (bzw. eine bestimmte Klasse von Verfahren) zur Bestimmung einer Prüfsumme für Daten (z. B. Netzwerkverkehr oder eine Datei), um Fehler bei der Übertragung oder Duplizierung der Daten erkennen zu können.

Debian Woody *Debian Woody* ist ein Betriebssystem basierend auf Linux.

DES *DES* steht für Data Encryption Standard. DES ist der wohl bekannteste Algorithmus zur symmetrischen Verschlüsselung.

DHCP	Das *DHCP* (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computer in einem Netzwerk (z.B. Internet oder LAN).
DNS	*DNS* ist ein Benennungsschema für an das Internet angeschlossene Rechner.
DoS	*DoS* (Denial of Service) oder DDoS (Distributed Denial of Service) sind Angriffe auf Server mit dem Ziel sie und ihre Dienste arbeitsunfähig zu machen.
DSSS	Beim *DSSS* (Direct-Sequence-Spread-Spectrum-Verfahren) werden die Nutzdaten per Exklusiv-Oder (XOR) mit einem Code verknüpft und anschließend auf die Bandbreite moduliert.
ESS	*ESS* - Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet.
ESSID	*ESSID* ist der Name für ein Funk-Netzwerk, das auf IEEE 802.11 basiert.
ETSI	Das *ETSI* ist das Europäische Institut für Telekommunkationsstandards mit Sitz in Frankreich.
FHSS	*FHSS* - Frequenzwechselverfahren, bei dem die Frequenzbänder nicht wie beim DSSS in direkter Folge, sondern sprungartig gewechselt werden. Vorteil dieses Verfahrens ist die geringere Störanfälligkeit, da die Frequenzbänder sehr schnell gewechselt werden.
FIAIF	*FIAIF* ist ein Skript System um schnell und einfach Iptables Firewalls zu generieren.
Firewall	Als *Firewall* bezeichnet man Rechner, die den Datenverkehr zwischen einem lokalen Netz (LAN) und anderen Netzwerken, z.B. dem Internet, regeln. Die Firewall soll das lokale Netz vor unbefugten Zugriffen schützen.
FreeS/WAN	*FreeS/WAN* ist eine freie IPSec Implementierung.
HotSpot	*HotSpot* ist ein öffentlich zugänglicher WLAN Access-Point.
Hub	Der *Hub* (engl. = Nabe, Mittelpunkt) wird in der Telekommunikation verwendet, um Netzwerk-Segmente oder auch einzelne Rechner, z. B. durch ein Ethernet, miteinander zu verbinden.
IAS	*IAS* ist die Abkürzung für International Accounting Standards. Es handelt sich dabei um ein Regelwerk zur Rechnungslegung welches vom "International Accounting Standards Committee" (IASC), einer unabhängigen juristischen Person, erstellt wird.
IBSS	*IBSS* (Independent Basic Service Set) ist die Bezeichnung für Funk-Netzwerke im Ad-hoc-Modus.
IEEE	Die *IEEE* erarbeitet unter anderem technische Standards und Empfehlungen im Bereich der elektronischen Datenverarbeitung (EDV).
infrastructure Mode	*infrastructure Mode* ist WLAN Modus, bei dem die Clients mit einer zentralen Stelle kommunizieren.
IPSec	*IPSec* ist eine Erweiterung für TCP/IP die Verschlüsselung anbietet.

Kernel *Der Linux-Kernel* ist ein UNIX-artiger Betriebssystem-Kern, der 1991 vom Finnen Linus Torvalds für die x86-Architektur geschrieben wurde. Er steht unter der freien GPL-Lizenz. Er bildet die hardwareabstrahierende Schicht, d.h. er stellt der auf dieser Basis aufsetzenden Software eine einheitliche Schnittstelle unabhängig von der Hardware-Architektur zur Verfügung.

LAN *LAN* ist ein lokales Kommunikationsnetzwerk innerhalb eines relativ kleinen geographischen Gebiets, bestehend aus einem oder mehreren Servern (LAN-Servern), Workstations, einem Netzwerk- Betriebssystem, einem einheitlichen Protokoll und speziellen Kabeln als Kommunikationsleitung.

LDAP Das*LDAP* (Lightweight Directory Access Protocol) definiert einen Standard für die Kommunikation mit Datenbanken im Internet.

Linux *Linux* ist ein von Linus Torvalds als Ersatz für UNIX entwickeltes Mehrbenutzer-Betriebssystem.

MAC Die *MAC* gehört zur Datensicherungsschicht (Data Link-Layer, Schicht zwei des OSI-Schichtenmodells). Sie regelt die Nutzung des betreffenden Übertragungsmediums (Codierung und Modulation des zu übertragenden Signals) und den Hardware-Zugriff innerhalb eines Netzes.

man-in-the-middle *man-in-the-middle* ist eine Angriffsmethode, bei der sich ein Hacker zwischen eine Verbindung hängt.

NAT *NAT* ist in Computernetzwerken ein Verfahren, bei dem private IP-Adressen auf öffentliche IP-Adressen abgebildet werden. Werden auch die Port-Nummern umgeschrieben spricht man dabei von maskieren.

OpenCA *OpenCA* ist eine frei verfügbare CA.

OpenSSL *OpenSSL* ist eine frei verfügbare SSL Implementierung.

ping *ping* st ein Dienstprogramm für das Internet. Es kann überprüfen, ob ein bestimmter Rechner im Netz erreichbar (online) ist. Es wird üblicherweise eingesetzt, um die Verbindung zu einem bestimmten Server zu überprüfen.

Proxy *Proxy* ist ein Programm, das zwischen Server und Client vermittelt. Dem Server gegenüber verhält sich das Programm wie ein Client, dem Client gegenüber wie ein Server.

Repeater Der *Repeater*wird in der Telekommunikation verwendet, um zwei logische Netzwerke miteinander zu verbinden. Er ermöglicht die maximale Ausdehnung eines Kabelnetzes über dessen physikalische Grenze hinaus zu erweitern.

revoking *revoking* ist der Ausdruck für das zurückweisen eines Schlüssels.

roaming *roaming* bezeichnet die Möglichkeit eines Mobilfunk-Teilnehmers, sein Mobiltelefon auch in anderen Mobilfunknetzen zu benutzen als dem, dessen Kunde er ist.

root *root* ist der Name des Systemsadministrators bei UNIX Systemen.

Router *Router* ist ein Vermittlungsrechner, der am Aufbau einer Verbindung in einem Computernetz mit Paketvermittlung, zum Beispiel dem Internet, beteiligt ist. Solche Rechner leiten ("routen") die Datenpakete anhand der Adresse eines route-fähigen Protokolls wie z.B. TCP/IP zum jeweiligen Zielrechner.

SNMP Das Simple Network Management Protocol *(SNMP)*ist ein Protokoll für die Verwaltung und Wartung von Rechnern und Peripheriegeräten in einem lokalen Netz (LAN).

SSH *SSH* (Secure Shell) ermöglicht den sicheren Zugang zu einem Server über ein unsicheres Netzwerk, wie dem Internet.

SSID *SSID* (Service Set Identifier) ist der Name für ein Funk-Netzwerk, das auf IEEE 802.11 basiert.

Switch Ein *Switch* ist ein elektronisches Gerät zur Verbindung von Netzwerk-Segmenten, ähnlich einem Hub. Es dient zu Verbindung mehrerer Computer über ein lokales Netzwerk (LAN). Dies erfolgt auf der Schicht 2 (Sicherungsschicht) des OSI-Modells.

TCP/IP Das "Transmission Control Protocol/Internet Protocol" ist das Standard-Internet- Protokoll. Es bietet die Möglichkeit zu Fehlerkorrektur und Routensteuerung.

TKIP *TKIP* (Temporal Key Integrity Protocol). Um die Sicherheit in 802.11-Netzen zu verbessern hat die Wireless Ethernet Compatibility Alliance (WECA) das TKIP entwickelt, das das Wired Equivalent Privacy-Konzept (WEP) ersetzen soll. TKIP verwendet wie WEP den RC4-Algorithmus für die Verschlüsselung. Der Schlüssel ändert sich temporär, und zwar immer dann, wenn ein Datenpaket von 10 KB übertragen wurde.

TLS *TLS* ist die Abkürzung für "Transport Layer Security". TLS steht als potentieller Nachfolger von SSL in den Startlöchern. Das neue Protokoll verspricht noch mehr Sicherheit bei der Kommunikation im Internet.

UDP *UDP* ist ein Protokoll der dritten Schicht (host-to-host-layer) des TCP/IP-Modells.

Unix *Unix* (von UNiplexed Information and Computing System) wurde 1969 von AT&T entwickelt. Es war das erste Betriebssystem, das in einer höheren Programmiersprache ("C") geschrieben wurde, und ist daher weitgehend plattform-unabhängig. UNIX ist multiuser- und multitasking-fähig und bietet eine Fülle von Netzwerkfunktionen wie z.B. TCP/IP. Es wird vor allem auf Großrechnern eingesetzt.

VPN *VPN* In einem "Virtual Private Network" *(VPN)* werden die öffentlich zugänglichen Leitungen des Internet in einer Weise genutzt, als wären sie Teil eines privaten Leitungsnetzes. Die zu einem VPN gehörenden Internet-Rechner tauschen ihre Daten untereinander nur in verschlüsselter Form aus, so daß diese Rechner gewissermaßen ein privates Netz innerhalb des öffentlichen Internet bilden.

Warchalking *Warchalking* wird beim WarWalking und WarDriving verwendet, um mittels auf die Wand oder den Boden aufgebrachten Zeichen Wireless LANs ausfindig zu machen. Hierbei wird eine szenetypische Schreibweise verwendet. So bedeutet z.B. ein geschlossener Kreis, dass es sich bei dem vorliegenden WLAN um ein geschlossenes handelt. Zwei entgegengesetzte Kreishälften bedeuten ein offenes, ungesichertes Netz. Rund herum sind technische Informationen platziert.

WEP *WEP* (Wired Equivalent Privacy) ist das Protokoll, das das Verschlüsselungsverfahren in einem WLAN bestimmt.

WLAN *WLAN* ist die Abkürzung für Wireless Local Area Network.

WPA *WPA* steht für Wi-Fi Protected Access und soll die für Angriffe anfällige Sicherheitstechnik WEP ersetzen. Dazu wird die Lösung vor allem bei der Datenverschlüsselung und der Benutzer-Authentifizierung Verbesserungen bringen. Für die Verschlüsselung wird das "Temporal Key Integrity Protocol" (TKIP) eingesetzt, das alle bekannte Sicherheitslücken von WEP schließt. So werden mehrere Schlüssel für jedes Paket verwendet sowie ein Message-Integrity-Check und ein erweiterter Initialisierungsvektor eingeführt.

X.509 *X.509* ist ein Standard der ITU-T für Zertifikate und Authentifizierungsdienste aus dem die Namen und die digitale Signatur des Ausstellers hervorgehen. X.509 ist Bestandteil des Verzeichnisdienstes X.500 für weltweite, verteilte und offene Systeme. Bei diesen, nach X.509 standardisierten Zertifikaten kann es sich auch um E-Mail-Zertifikate handeln, die der sicheren Übertragung von E-Mails und Dateien dienen und auch zur Identifikation gegenüber Websites benutzt werden.