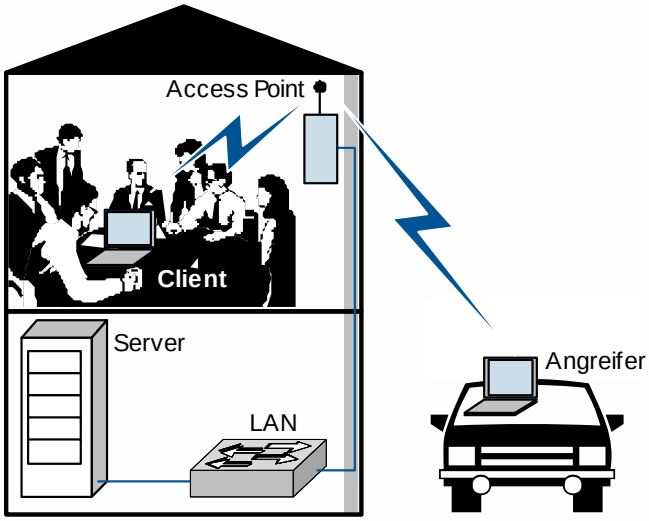
Bundesamt
für Sicherheit in der
Informationstechnik

# BSI - Technische Richtlinie

| | |
|---|---|
| Bezeichnung: | **Sicheres WLAN (TR-S-WLAN)** |
| | **Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen** |
| Anwendungsbereich: | |
| Kürzel: | BSI-TR 03103 Teil 1 |
| Version: | 1.0 |
| Veröffentlichung: | 10/2005 |




Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

**Autoren**

An der Erstellung dieser Technischen Richtlinie waren beteiligt:

ComConsult Beratung und Planung GmbH

- Dr. Simon Hoff
- Dr. Joachim Wetzlar

BSI – Bundesamt für Sicherheit in der Informationstechnik

- Dr. Wilhelm Pütz
- Berthold Ternes

**Danksagung**

Wir bedanken uns bei allen, die Vorversionen dieses Textes gelesen und uns wertvolle Hinweise und Korrekturen geliefert haben:

Dr. Alfred Arnold, Olaf Schilperoort
LANCOM Systems GmbH

Falk Bachmann, Michael Raschke
EDS Operations Services GmbH

Reyk Flöter
vantronix secure systems GmbH

Wilhelm Fries, Roman Meyer,
Norbert Vogel, Oliver Walter
Benutzergruppe Netzwerke

Tobias Glemser
Tele-Consulting GmbH

Matthias Hofherr
GeNUA Gesellschaft fuer Netzwerk- und Unix-Administration mbH

Andree Kabisch, Kerst van Raden
eMNetCon Netzwerk Consulting GmbH

Michael Muth
DVZ Mecklenburg-Vorpommern

Christoph Plur
Cisco Systems GmbH

Patrick Postel
iPIsec Ltd.

Herbert Saupp
Bundeskriminalamt

Markus Schaffrin
eco Electronic Commerce Forum – Verband der deutschen Internetwirtschaft e.V.

Eicke Schomann
Funk Software Europe, Inc.

Dr. Günther Welsch
Deutsche Telekom AG

Michael Wirth
Microsoft Deutschland GmbH

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 1888 9582 0
E-Mail: lwc@bsi.bund.de
Internet: http://www.bsi.bund.de

# Vorwort

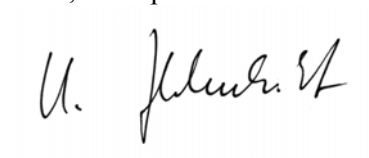
Bereits heute nimmt Wireless LAN als Zugangstechnik zu IT-Systemen einen festen Platz ein. Doch bei aller Freude über fehlende Kabel und steigende Mobilität, wie steht es um die Sicherheit von WLAN?

Die Datenübertragung muss über die gesamte Funkstrecke und darüber hinaus ausreichend abgesichert sein: gegen Abhör- und Störbarkeit genauso wie gegen unerlaubte Zugänge. Mit der Vielfalt der Anwendungsmöglichkeiten sind jedoch die Sicherheitsinfrastrukturen enorm komplex geworden. Um WLAN-Nutzer hierbei zu unterstützen, hat das BSI die Technische Richtlinie Sicheres WLAN initiiert.

Ziel der Richtlinie ist es, Wireless LAN Systeme und deren Einsatz in IT-Infrastrukturen sicherer zu machen. Die Richtlinie enthält deshalb konkrete Empfehlungen zur Planung, Beschaffung, Installation und Konfiguration von sicheren WLANs – egal ob in der Wirtschaft oder der Behörde. Anhand unterschiedlich großer WLANs werden verschiedene Einsatzszenarien beschrieben: WLAN im Büro, am Hotspot oder als drahtlose Kopplung zwischen kabelbasierten lokalen Netzen. Die Empfehlungen richten sich an Planer, Beschaffer, Betreiber und Nutzer von WLAN-Systemen. Zusätzlich werden Sicherheitsfunktionalitäten von WLAN-Produkten definiert und Verfahren zur Prüfung angegeben – das nutzt Herstellern und Prüfinstanzen.

Ich bin mir sicher: Die Richtlinie hilft dabei WLAN-Sicherheit zu verstehen und umzusetzen. Damit alle Nutzer auch zukünftig von den Vorteilen dieser Technologie profitieren können.

Bonn, im September 2005



Dr. Udo Helmbrecht, Präsident des BSI

# Inhalt

# Dokumenteninformation

| Version | Datum | Name | Beschreibung |
|---|---|---|---|
| 1.0 | 4. Juli 2005 | Dr. Simon Hoff | Erste veröffentlichte Version |

# 1 Vorbemerkungen

Wireless LAN (kurz: WLAN) haben als drahtlose Erweiterung eines traditionellen Lokalen Netzes (Local Area Network, LAN) einen festen Platz in den Zugangstechniken zur IT-Infrastruktur eingenommen. Nicht nur in den klassischen Anwendungsbereichen Büro, Produktion, Logistik und Medizin sondern auch im privaten Sektor sind WLAN auf dem Vormarsch. Moderne Arbeitsmethoden sind geprägt von Mobilität. Dabei ersetzt das Notebook zunehmend den klassischen Desktop PC als Arbeitsplatz, und das WLAN erlaubt auf komfortable Weise den mobilen Zugang zu allen benötigten Informationen unabhängig vom aktuellen Aufenthaltsort.

Die Kommunikation geschieht dabei über Funk, und dies bedeutet immer Übertragung auf einem Shared Medium. Damit verbunden ist stets die prinzipielle Abhörbarkeit, die Möglichkeit des unerlaubten Zugangs zum WLAN und die Störbarkeit von Übertragungen (beabsichtigt oder nicht). Neben Mechanismen zur geregelten simultanen Nutzung des Mediums durch mehrere Nutzer erfordert ein System zur Datenübertragung über Funk immer auch Mittel zur Authentifizierung der Teilnehmer dem Netz gegenüber (und umgekehrt) sowie die Verschlüsselung der Daten zumindest auf der Funkstrecke. In diesen grundsätzlichen Anforderungen unterscheiden sich WLAN nicht von klassischen mobilen Kommunikationssystemen wie dem Global System for Mobile Communications (GSM) oder anderen drahtlosen lokalen Kommunikationssystemen z. B. gemäß Digital Enhanced Cordless Telecommunications (DECT).

Im Bereich der WLAN haben sich Systeme nach den Standards der Serie IEEE 802.11 des Institute of Electrical and Electronics Engineers (IEEE) durchgesetzt. Leider stellten sich die in IEEE 802.11 ursprünglich spezifizierten kryptografischen Mechanismen als unzulänglich heraus. Die verwendete Verschlüsselungsmethode kann dabei innerhalb von kürzester Zeit gebrochen werden, und mit allgemein zugänglichen Werkzeugen wird der Einbruch in fremde WLAN zudem noch erleichtert.

Diverse WLAN-Ausrüster haben daraufhin ihre Systeme mit proprietären Zusatzfunktionen versehen, und die Arbeitsgruppe IEEE 802.11 war gefordert, den Standard nachzubessern. Inzwischen kann sich der Planer eines WLAN einer Palette unterschiedlicher, teilweise standardisierter, Mechanismen bedienen, um das WLAN adäquat hinsichtlich der Sicherheitsziele Vertraulichkeit und Integrität abzusichern. Funknetze haben generell Schwächen im Bereich der Verfügbarkeit. Der Schwerpunkt der Absicherung liegt daher neben Redundanzkonzepten in der Überwachung des WLAN bezüglich der Verfügbarkeit.

Dieses Dokument stellt die wesentlichen marktgängigen und sich in der Standardisierung abzeichnenden Methoden und Mechanismen zur WLAN-Absicherung vor. Architekturen, Realisierungsalternativen und Anwendungsbereiche werden diskutiert. Den Schwerpunkt bildet dabei die drahtlose Infrastrukturanbindung von Endgeräten. Wo es erforderlich ist, wird allerdings auf die spezifischen Eigenschaften anderer Verwendungen von WLAN-Techniken, beispielsweise zum Aufbau von Richtfunkstrecken, hingewiesen. Das Dokument soll als Orientierungshilfe dienen und das Fundament bereiten für das Verständnis des in den separaten Teilen zwei und drei dargestellten WLAN-Sicherheitskonzepts sowie der Produktauswahl- und Prüfkriterien.

Dieses Dokument richtet sich an alle, die mit der Absicherung einer WLAN-Installation, sei es in der Rolle als Einkäufer, Planer oder Betreiber, befasst sind. Es werden WLAN unterschiedlicher Größe (im Sinn der abgedeckten Fläche oder Anzahl der aktiven Clients) und Anwendung (z. B. Büro, Logistik, Medizin, Hotspots) betrachtet.

Für eilige Leser sei hier auf die Zusammenfassung in Kapitel 14 verwiesen.

# 2 Wireless LAN nach IEEE 802.11 im Überblick

Die technischen Finessen im Bereich der WLAN nach IEEE 802.11 haben inzwischen eine Komplexität erreicht, die den Rahmen dieses Dokuments sprengen würde. Daher wird sich im Folgenden beschränkt auf die Beschreibung der wesentlichen Anwendungen und der zugehörigen Aufbauprinzipien (Kapitel 2.1), der Struktur der Standardfamilie IEEE 802.11 in Kapitel 2.2 und abschließend derjenigen Grundfunktionen in einem WLAN, die einen unmittelbaren Bezug zum Thema der WLAN-Sicherheit haben (Kapitel 2.3).

## 2.1 Anwendungen und Aufbauvarianten

Als drahtlose Erweiterung traditioneller LAN eignen sich WLAN insbesondere für Anwendungen, die eine Kommunikation mit mobilen Endgeräten unabhängig von deren aktuellem Aufenthaltsort innerhalb eines gewissen lokalen Versorgungsgebiets (Gebäude oder Campus) erfordern. Die drahtlose Anbindung der Clients erfolgt über spezielle Funkfeststationen, sogenannte Access Points, die als Bridge auf Layer 2 zwischen der Funkschnittstelle und der kabelbasierten Infrastruktur dienen (siehe Abbildung 1). Dieser sogenannte **Infrastruktur-Modus** macht den größten Teil der WLAN-Installationen aus.

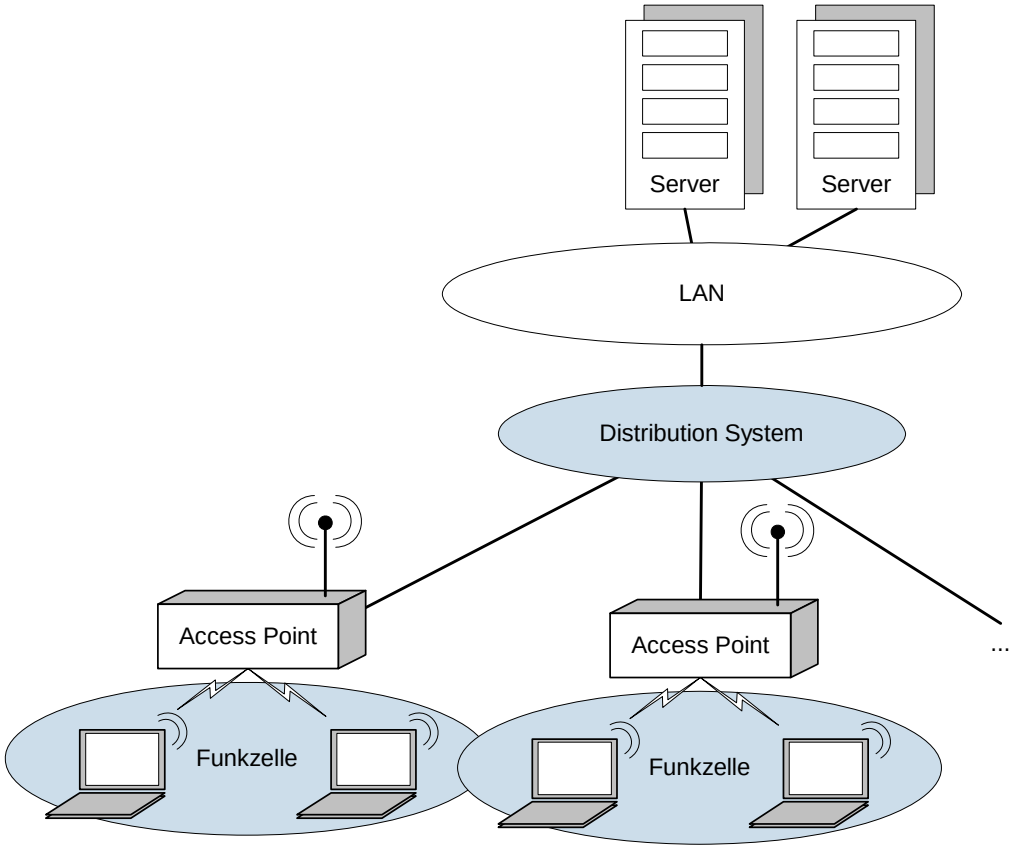



Abbildung 1: Aufbau eines Infrastruktur-WLAN

Ein Access Point (zusammen mit der durch ihn aufgespannten Funkzelle) wird in IEEE 802.11 als Basic Service Set (BSS) bezeichnet. Das Lokale Netz, welches die einzelnen BSS miteinander und mit

der weiteren Infrastruktur verbindet, heißt Distribution System (DS)[1]. Die Gesamtheit aller BSS an einem DS nennt der Standard Extended Service Set (ESS).

Es kann durchaus vorkommen, dass an einem Ort WLAN unterschiedlicher Betreiber bzw. Organisationen empfangen werden können. Damit ein Client weiß, in welches WLAN er sich einbucht, wird für ein ESS ein Name vergeben, der sogenannte **Service Set Identifier** (SSID). Die maximale Länge eines SSID beträgt 32 Byte. Der SSID wird auf Client und Access Point konfiguriert. Die Client-Software unterstützt meist verschiedene Profile, die es erlauben, mehrere WLAN (sprich: mehrere SSIDs) zu konfigurieren.

Clients können auch ohne Zuhilfenahme einer Infrastruktur direkt miteinander kommunizieren. Dieser sogenannte **Ad-hoc-Modus** wurde bereits 1997 in den IEEE-Standard aufgenommen, ist aber in der Praxis im Vergleich zur Verwendung des Infrastruktur-Modus noch eher selten anzutreffen[2]. Dieser Modus stellt eine potentielle Störquelle für Infrastruktur-WLAN dar und muss daher unabhängig von seiner Verbreitung hier betrachtet werden.

Analog können „Access Points“ (in diesem Fall als Wireless Bridges bezeichnet) durchaus auch direkt miteinander über Funk kommunizieren, um Strecken zu überbrücken, bei denen die Verwendung einer klassischen kabelbasierten Technik nicht wirtschaftlich ist. Typischerweise werden dabei kabelbasierte LAN-Segmente über größere Distanzen verbunden. Die WLAN-Übertragung wird also für die **LAN-Kopplung** wie eine Richtfunkstrecke genutzt, wie in Abbildung 2 gezeigt.

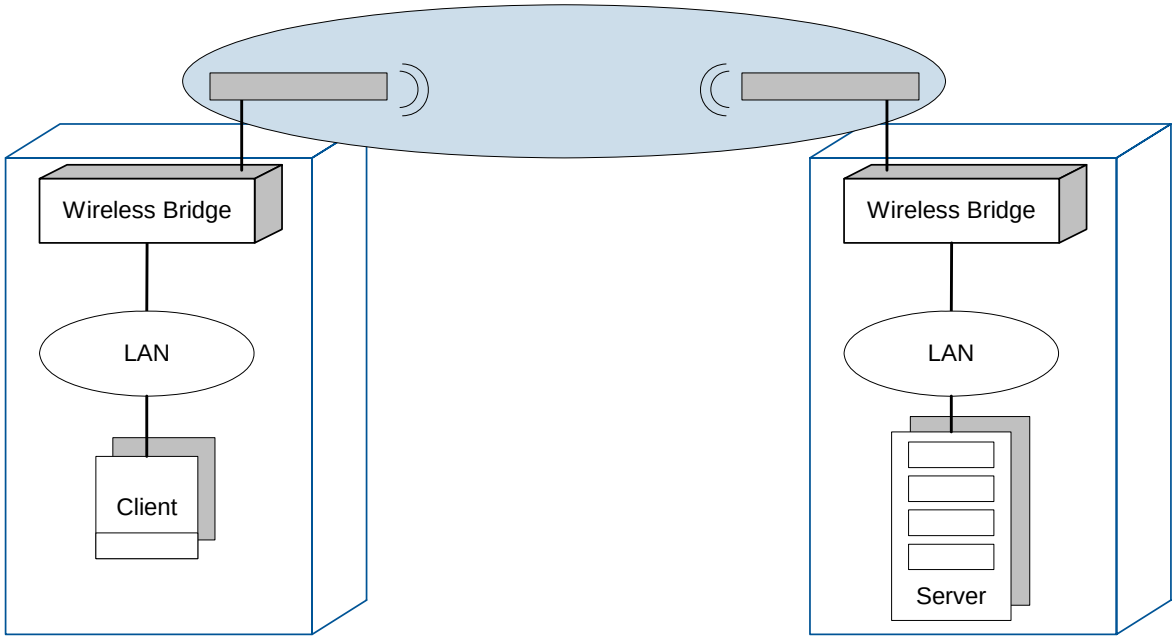



Abbildung 2: WLAN als Richtfunk zur LAN-Kopplung

[1] Das Distribution System muss nicht zwangsläufig ausschließlich ein kabelbasiertes LAN sein. Es kann auch hier mit Funktechniken gearbeitet werden. Beispielsweise kann die Kommmunikation zwischen Access Points auch über eine WLAN-Funkverbindung erfolgen (im Standard IEEE 802.11 als Wireless Distribution System bezeichnet, kurz: WDS). Generell ist diese Technische Richtlinie auch für den Einsatz von WLAN-Technik im Distribution System anwendbar (siehe etwa Kapitel 13). Es kommen jedoch auch andere Funktechniken im Distribution System in Betracht. Hier wird aktuell insbesondere die Verwendung von Worldwide Interoperability for Microwave Access (WiMAX) bzw. IEEE 802.16 diskutiert (siehe [IEEE04c]).

[2] Es gibt aber durchaus Entwicklungen, die auf den Ad-hoc-Modus bauen. Zu erwähnen sind hier beispielsweise die Arbeiten an Mobile Ad-hoc Networks (MANET) innerhalb der IETF, die sich unter anderem mit der Frage beschäftigen, wie ein effizientes Routing in mobilen, teilvermaschten Netzen geschehen kann.

## 2.2 IEEE 802.11 und die Erweiterungen

Wie die anderen IEEE-Standards für Lokale Netze, etwa Ethernet und Token Ring, definiert IEEE 802.11 lediglich die Protokolle zur physikalischen Übertragung und für den Kanalzugriff (Medium Access Control, MAC) sowie das Netzmanagement für diese Protokollebenen. Im Rahmen der Spezifikation des MAC-Protokolls legt IEEE 802.11 in der Version von 1997 und mit geringfügigen Erweiterungen von 1999 auch Mechanismen zur Authentifizierung und Verschlüsselung fest (Wired Equivalent Privacy, kurz: WEP). Die Funktionsweise von WEP und die mit WEP verbundenen Probleme werden in Kapitel 3 beschrieben.

IEEE 802.11 spezifiziert sechs Varianten zur physikalischen Übertragung und ein gemeinsames Verfahren für den Kanalzugriff (siehe [IEEE99]):

- In dem 1997 veröffentlichten Standard IEEE 802.11 sind neben der Übertragung mit Infrarot im Industrial-Scientific-Medical-Frequenzband (kurz: ISM) bei 2,4 GHz zwei Bandspreizverfahren festgelegt worden: Direct Sequence Spread Spectrum (DSSS) und Frequency Hopping Spread Spectrum (FHSS). IEEE 802.11 erlaubt dabei Datenraten von 1 MBit/s oder 2 MBit/s.
- DSSS wurde dann 1999 in der Ergänzung **IEEE 802.11b** zur Übertragung höherer Datenraten bis maximal 11 MBit/s erweitert (siehe [IEEE99b]). IEEE 802.11b hat sich inzwischen als Marktführer im WLAN-Bereich etabliert.
- Um Datenraten bis zu 54 MBit/s und eine höhere Anzahl von sich überlappenden Systemen anbieten zu können, operiert **IEEE 802.11a** im 5-GHz-Bereich (siehe [IEEE99a]). IEEE 802.11a nutzt als Übertragungstechnik Orthogonal Frequency Division Multiplexing (OFDM). IEEE 802.11a wurde ebenfalls 1999 verabschiedet.
- Die im Juni 2003 veröffentlichte Ergänzung **IEEE 802.11g** spezifiziert eine physikalische Übertragungsebene, die im ISM-Band bei 2,4-GHz operiert und mit IEEE 802.11b abwärtskompatibel ist (siehe [IEEE03g]). Dabei verwendet IEEE 802.11g die Übertragungstechnik OFDM nach IEEE 802.11a und erlaubt daher auch Datenraten bis 54 MBit/s.

Infrarotsysteme haben es nie zur Produktreife gebracht. In der Praxis hat sich bis heute DSSS nach IEEE 802.11b durchgesetzt. Ältere DSSS-Systeme mit maximal 2 MBit/s sind kaum noch zu finden. FHSS-Systeme sind noch an manchen Stellen im Einsatz (z. B. Produktionsbereiche, medizinische Bereiche), da sie wegen ihrer Robustheit geschätzt sind.

Der Kanalzugriff (Medium Access Control, MAC) geschieht für alle spezifizierten Übertragungstechniken einheitlich über Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Dieses Protokoll liefert einen Best-Effort-Dienst.

**IEEE 802.11h** ist eine Erweiterung von IEEE 802.11a und wurde im September 2003 verabschiedet (siehe [IEEE03h]). Diese Erweiterung war erforderlich, da für den Einsatz eines WLAN bei 5 GHz in Europa das Problem besteht, dass der Frequenzbereich auch von militärischen und zivilen Radar- und Navigationsanwendungen genutzt wird. Daher hat das European Telecommunications Standards Institute (ETSI) zunächst die Vorgabe gemacht, dass eine Zulassung nur dann erfolgen kann, wenn das System eine dynamische Frequenzwahl (Dynamic Frequency Selection, DFS) und eine Anpassung der Sendeleistung (Transmit Power Control, TPC) unterstützt. Diese Funktionen dienen zur Verringerung von Störungen, die Radar- und Navigationsanwendungen durch ein parallel betriebenes WLAN erfahren könnten. Die notwendigen Erweiterungen des MAC Layer zur Realisierung der Funktionen DFS und TPC werden in IEEE 802.11h beschrieben. Maßgeblich für die Zulassung in Europa ist allerdings die Einhaltung der Norm EN 301 893 (siehe [ETSI03]), da hier im Sinne einer System-unabhängigen Black Box die Parameter und Schwellwerte für TPC und DFS sowie die zugehörigen Testserien und -methoden beschrieben werden.

**IEEE 802.11i** spezifiziert verbesserte Sicherheitsmechanismen, die erforderlich waren, da die ursprünglich in IEEE 802.11 festgelegten Verfahren sich als unzulänglich erwiesen haben. Diese Erweiterung und die zugrundeliegenden Mechanismen werden im Folgenden noch im Detail beschrieben (siehe Kapitel 6). IEEE 802.11i wurde im Juni 2004 verabschiedet (siehe [IEEE04a]).

**IEEE 802.11F** (verabschiedet im Juni 2003) spezifiziert ein Inter Access Point Protocol (IAPP), der einen standardisierten, herstellerübergreifenden Datenaustausch zwischen Access Points ermöglicht. Ursprünglich sollte durch diesen Standard ein schnelleres Layer 2 Roaming (Handover) zwischen Access Points ermöglicht werden (siehe [IEEE03F]). In der Praxis hat sich dieser Standard jedoch bisher nicht durchgesetzt.

**IEEE 802.11e** erweitert die MAC-Ebene von IEEE 802.11 um Dienstgütemechanismen (Quality of Service, QoS). IEEE 802.11e spezifiziert einen erweiterten Kanalzugriff, der eine Priorisierung verschiedener Verkehrsklassen (z. B. Best Effort, Voice) und eine durch den Access Point gesteuerte Kanalvergabe erlaubt. IEEE-802.11e ist noch in Arbeit und wird voraussichtlich im Laufe des Jahres 2005 verabschiedet[3].

Abbildung 3 zeigt abschließend die Struktur des Standards IEEE 802.11 sowie die verschiedenen angesprochenen Erweiterungen. Daneben gibt es noch eine Reihe weiterer Ergänzungen in der Familie IEEE 802.11, die allerdings für das in diesem Dokument erörterte Thema nicht von Belang sind. Erwähnenswert ist, dass im September 2003 die „Task Group n“ unter dem Titel „Enhancements for higher effective Throughput“ ihre Arbeit aufnahm. Ziel ist eine Optimierung und Erweiterung von IEEE 802.11, die dem Nutzer des MAC Layers eine Leistung von mindestens 100 MBit/s bietet (im Sinne einer Nettodatenrate). Hierzu müssen entsprechende Erweiterungen der physikalischen Übertragung geschaffen und die Protokolle auf MAC Layer optimiert werden. Mit einer Verabschiedung des Standards ist wahrscheinlich nicht vor Ende 2006 zu rechnen.

Generell sind im WLAN-Bereich die extrem kurzen Entwicklungszyklen auffällig, die an die frühen Phasen der Ethernet-Evolution erinnern.

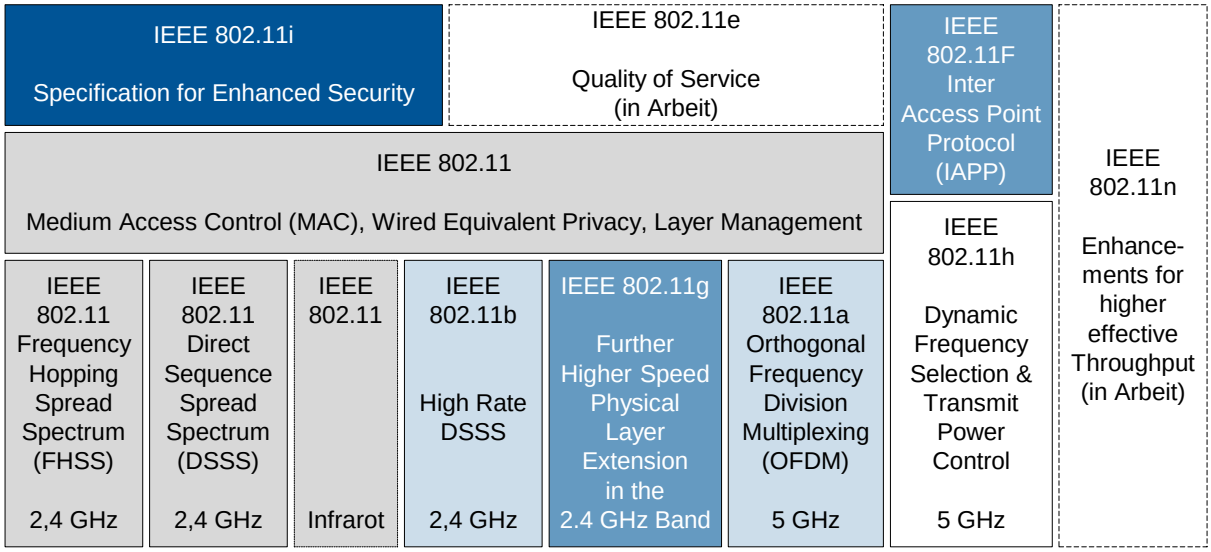



Abbildung 3: IEEE-802.11-Familie im Überblick

## 2.3 Grundfunktionen

Für den Bereich der Absicherung eines WLAN sind die folgenden Grundfunktionen von besonderer Bedeutung:

[3] Die Wi-Fi Alliance hat September 2004 den Standard Wi-Fi Multimedia (WMM) zur Unterstützung von QoS in WLAN herausgegeben und vergibt ein WMM-Zertifikat für WLAN-Produkte. WMM basiert auf einer Teilmenge von Funktionen einer Vorversion von IEEE 802.11e.

- Anmeldung eines Clients (der Standard IEEE 802.11 spricht allgemein von einer „Station“) am Access Point
- Wechsel einer Station von einem Access Point zum anderen (Zellwechsel)

### 2.3.1 Anmeldung am Access Point

Die Anmeldung eines Clients durchläuft drei Phasen. Erst nach deren Abschluss können Daten über den Access Point übertragen werden.

- **Phase 1: Scanning**

  Die Station durchläuft die verfügbaren Kanäle (z. B. in den meisten Ländern Europas 13 Kanäle im 2,4-GHz-Bereich bei Verwendung von IEEE 802.11b oder IEEE 802.11g) und sucht einen Kanal mit WLAN-Empfang. Dabei können die „Standardkanäle“ 1, 7, 13 für Europa und 1, 6, 11 für USA bevorzugt werden. Anschließend wird geprüft, ob der SSID des empfangenen WLAN mit dem lokal konfigurierten SSID übereinstimmt. IEEE 802.11 spezifiziert zwei Methoden, um diese Prüfung durchzuführen: Passive Scanning und Active Scanning.

  Bei der Methode Passive Scanning teilt der Access Point seinen SSID in dem periodisch ausgestrahlten Beacon Frame mit. Die Station vergleicht einfach empfangene SSIDs mit dem konfigurierten SSID. Diese Methode bietet sich insbesondere für öffentlich zugängliche WLAN an.

  Wird Active Scanning eingesetzt, muss der Access Point den SSID nicht im Beacon Frame mitteilen. Stattdessen schickt der Client auf dem gerade aktuellen Kanal ein Probe Request MAC Frame. In diesem Frame überträgt der Client den gewünschten SSID. Operiert auf dem Kanal ein Access Point mit diesem SSID, antwortet der Access Point, und die nächste Phase der Anmeldung wird durchgeführt. Diese Methode eignet sich insbesondere für nicht-öffentliche WLAN, bei denen die Anwesenheit einer WLAN-Versorgung möglichst nur für die eigenen WLAN Clients sichtbar sein soll.

- **Phase 2: Authentifizierung**

  IEEE 802.11 spezifiziert zwei Methoden zur Authentifizierung: Open System Authentication und Shared Key Authentication.

  Die Open System Authentication ist eine Null-Authentifizierung, d. h. sie ist immer erfolgreich.

  Die Shared Key Authentication ist eine Challenge-Response-Authentifizierung, bei der die im nächsten Kapitel beschriebene WEP-Verschlüsselung eingesetzt wird. Der Client meldet sich zunächst beim Access Point und kündigt den Authentifizierungswunsch an. Der Access Point schickt im Klartext eine pseudozufällig erzeugte Zahl an den Client (Challenge). Der Client verschlüsselt diese Zahl mit dem WEP-Verfahren und schickt das verschlüsselte Ergebnis zurück (Response). Der Access Point entschlüsselt die empfangene Response. Stimmt die gesendete Challenge mit der Antwort überein, ist der Client authentifiziert.

  Da die Shared Key Authentication für eine Kompromittierung von WEP wertvolle Informationen liefert (nämlich einen Klartext und das zugehörige Chiffrat), die ein Angreifer leicht belauschen kann, wird empfohlen, diese Authentifizierungsmethode nicht zu nutzen (siehe hierzu auch Kapitel 3.2). Somit sind über den Basisstandard IEEE 802.11 hinausgehende Mechanismen zur Authentifizierung erforderlich. Diese sind in den folgenden Kapiteln 5 bis 7 beschrieben.

- **Phase 3: Assoziation**

  Nach erfolgreicher Authentifizierung sendet der Client ein Association Request MAC Frame. Der Access Point übermittelt daraufhin eine Association ID, welche die Beziehung zwischen Client und Access Point identifiziert. Abschließend aktiviert der Access Point den Datentransfer zwischen Distribution System und Client.

Die in Phase 1 genannte Möglichkeit, den SSID zu verbergen und ein aktives Erfragen des SSID zu fordern[4], kann als schwache Sicherheitsmaßnahme betrachtet werden. Für nicht-öffentliche WLAN sollte in Betracht gezogen werden die Rundsendung (Broadcast) des SSID durch den Access Point bzw. die Möglichkeit der Assoziierung eines Clients über den Broadcast SSID zu deaktivieren.

Immerhin wird ein WLAN mit dieser Einstellung von manchen Werkzeugen nicht mehr entdeckt. Natürlich kann man beispielsweise mit einem Protokollanalysator den SSID herausfinden, sofern man einen Anmeldevorgang aufgezeichnet hat. In Infrastruktur-WLAN ist dies früher oder später der Fall, wenn ein Client sich assoziiert und der SSID damit über die Luftschnittstelle übertragen wird. Anders sieht dies bei Verbindungen zwischen Wireless Bridges für die LAN-Kopplung aus: Hier würde im Anschluss an die erste Assoziation nach Einschalten der Geräte nur dann erneut der SSID übertragen, wenn es zu einem Ausfall der Verbindung kommt, in einem stabil laufenden WLAN also nur extrem selten. Damit ein Angreifer den SSID des WLAN ermitteln kann, muss er also Neuassoziationen erzwingen. Dies ist allerdings mit vergleichsweise einfachen Mitteln (und allgemein verfügbaren Werkzeugen) möglich, denn die entsprechenden auf Layer 2 ausgetauschten Management Frames werden im Klartext ohne weitere Absicherung übertragen.

Ob für ein nicht-öffentliches Infrastruktur-WLAN der SSID verborgen werden sollte, oder ob es unkritisch ist, ihn als Broadcast zu übertragen, muss im Einzelfall entschieden werden. Dabei muss auch berücksichtigt werden, dass es bei Deaktivierung des SSID Broadcast für manche Client-Systeme zu Beeinträchtigungen bei der Netzauswahl kommen kann[5].

### 2.3.2 Zellwechsel

Die Mobilität in WLAN nach IEEE 802.11 wird durch einen Wechsel der Funkzelle auf Ebene 2 erreicht. Der Standard IEEE 802.11 nennt diesen Wechsel „BSS Transition“. In der Praxis wir auch häufig die Bezeichnung „Handover“ für einen Kanalwechsel unter Beibehaltung der Ende-zu-Ende-Kommunikationsbeziehung benutzt[6]. Die Steuermechanismen für ein Handover sind herstellerspezifisch.

Ein Handover ist zunächst transparent für das Netzwerkprotokoll. Dies führt zu grundsätzlichen Problemen in einem Distribution System, das in mehrere IP-Subnetze strukturiert ist. Als Folge wird das Distribution System oft als flaches Layer-2-Netz aufgebaut, sofern eine Online-Mobilität erforderlich ist.

Es existieren allerdings inzwischen eine Reihe von oft herstellerspezifischen Techniken, die einen Zellwechsel auf Layer 3 unterstützen (als Layer 3 Roaming bezeichnet). Dieser Aspekt wird in Kapitel 9 weiter vertieft.

Ein Handover wird in WLAN nach IEEE 802.11 durch den Client initiiert (Abbildung 4). Der Standard IEEE 802.11 legt dabei keine Kommunikation zwischen Client und Access Point bzw. zwischen den Access Points fest. Der Zellwechsel geschieht einfach durch eine Assoziierung des Clients am neuen Access Point. Die Assoziierung am alten Access Point bleibt zunächst bestehen, bis sie nach Ablauf einer gewissen Zeitspanne für inaktive Clients schließlich aus der Assoziierungsliste gelöscht wird. Dies stellt ein Problem bei Inter-Client-Kommunikation über einen Access Point (z. B. bei Voice over IP, VoIP) dar: Solange einem Access Point nicht bekannt ist, dass der Client die Funkzelle verlassen hat, leitet er die Pakete an die MAC-Adresse des Clients nicht über das Festnetz weiter. Dies bedeutet, dass die in der Funkzelle verbliebenen Stationen mit dem Client, der die Funkzelle verlassen

4 Diese Funktion wird auch als Hidden SSID bezeichnet.

5 Zu nennen sind beispielsweise einige Mobiltelefone mit PDA-Funktion und eingebautem WLAN-Adapter.

6 Manchmal wird für ein Handover auch die Bezeichnung „Layer 2 Roaming“ verwendet. Dies ist missverständlich, da im Mobilfunkbereich die Begriffe Roaming und Handover unterschiedliche Funktionen bezeichnen.

hat, nicht kommunizieren können. Die Access Points mancher Hersteller kommunizieren an dieser Stelle miteinander, damit bei einem Handover ein Client sofort aus der Assoziierungsliste des bisherigen Access Points gelöscht werden kann.

Die Entscheidung für ein Handover trifft der Client anhand einer Bewertung der Qualität der Funkverbindung. Wird die Verbindung zum aktuellen Access Point als zu schlecht eingestuft, muss der Client versuchen, einen Access Point mit besseren Empfangsbedingungen zu finden. Hierzu muss der Client ein Scanning der einzelnen WLAN-Kanäle durchführen. Dabei sucht der Client-Adapter nach einem Access Point mit besseren Empfangsbedingungen. Zusätzlich kann als Parameter die aktuelle Auslastung eines Access Points in die Auswahl eines geeigneten Access Points mit einfließen. Der Client kann gewisse Kanäle bevorzugt durchsuchen, um einen geeigneten Access Point mit möglichst geringem Aufwand zu finden.

IEEE 802.11 spezifiziert weder Verfahren noch Parameter für ein Handover. Lediglich die Existenz einer solchen Funktion wird festgeschrieben. Zudem hat der Benutzer oft kaum Einfluss auf das Handover-Verhalten.

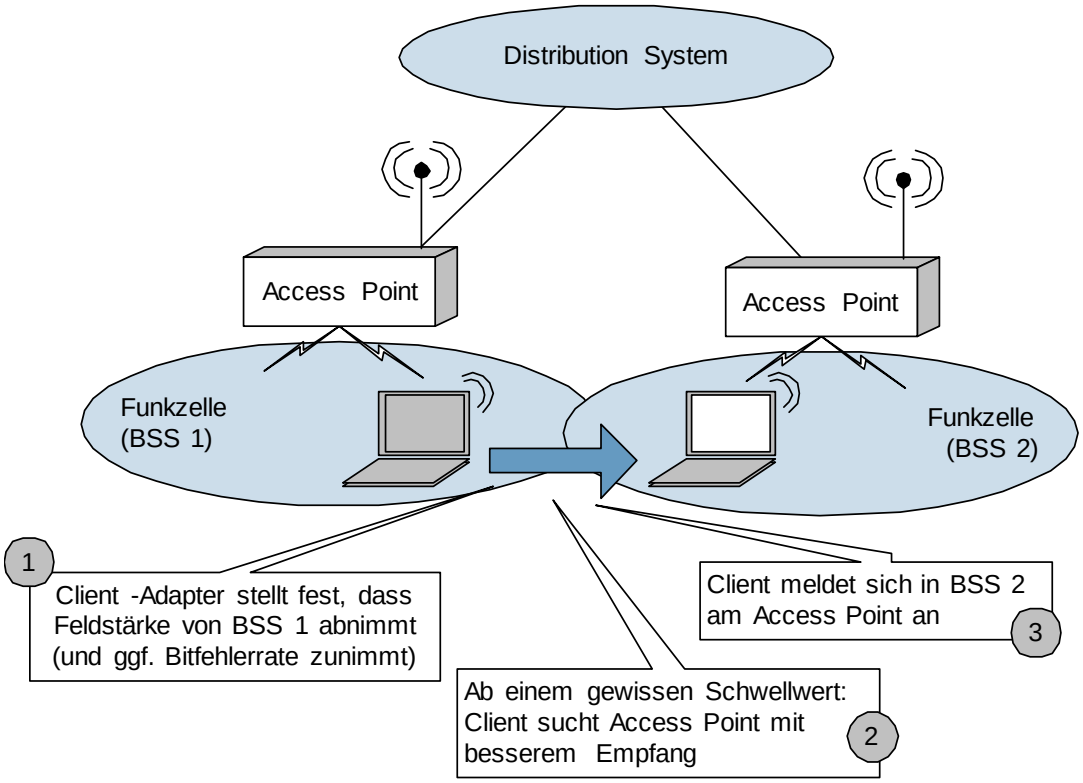



Abbildung 4: Grundsätzliche Funktionsweise eines Handovers

Erst in der Erweiterung IEEE 802.11F, die im Juni 2003 verabschiedet wurde, ist ein Inter Access Point Protocol (IAPP) standardisiert worden, welches es bei einem Zellwechsel erlaubt, die Client-spezifischen Informationen über das Distribution System vom bisherigen Access Point zum neuen Access Point zu übertragen.

# 3 Ursprüngliche Sicherheitsmechanismen in IEEE 802.11

Wie bereits erwähnt ist das Medium Funk immer ein Shared Medium, und neben den speziellen Mitteln zum Kanalzugriff müssen Sicherheitsmechanismen implementiert werden, wenn die Sicherheitsziele Vertraulichkeit, Zugangskontrolle und Datenintegrität erreicht werden sollen. In IEEE 802.11 wird hierzu das als Wired Equivalent Privacy (WEP) bezeichnete Verfahren spezifiziert, welches zur Verschlüsselung und Authentifizierung eingesetzt wird. Funktionsweise und Kompromittierung von WEP werden im Folgenden kurz beschrieben.

An dieser Stelle sei auch auf ein allgemeines, nicht technisches Problem hingewiesen, das nicht selten für einen Sicherheitsvorfall verantwortlich ist: WLAN-Geräte werden oft mit einer unsicheren Default-Konfiguration versehen, um dem Anwender auf eine möglichst einfache Weise einen drahtlosen Zugang zu verschaffen. Eine Default-Konfiguration sollte nie ohne eingehende Prüfung in Betrieb genommen werden. Der perfekteste technische Schutz hilft nichts, wenn er nicht (geeignet) aktiviert wird.

## 3.1 Funktionsweise von WEP

WEP benutzt RC4, ein symmetrisches Verschlüsselungsverfahren, das zu den sogenannten Stromchiffrierern gehört.

Mit einem Startwert (Seed) wird dabei ein Pseudozufallszahlengenerator initialisiert. Für jedes zu übertragende Byte einer Nachricht wird eine neue Pseudozufallszahl bestimmt, d. h. durch den Generator berechnet. Das verschlüsselte Byte ergibt sich einfach durch eine XOR-Verknüpfung mit der Zufallszahl. Die Entschlüsselung funktioniert analog: Der Empfänger benutzt denselben Startwert wie der Sender für die Initialisierung des Zufallszahlengenerators. Für jedes empfangene Byte der Nachricht ermittelt der Empfänger aufgrund der Gleichheit des Startwertes die gleiche Zufallszahl, die der Sender für dieses Byte verwendet hat, führt eine XOR-Verknüpfung mit dem verschlüsselten Byte durch und erhält den Klartext, siehe Abbildung 5. Der gemeinsame Startwert wird dabei aus einem geheimen Schlüssel berechnet, der bei Sender und Empfänger vorliegen muss.

Ein Angreifer kann die verschlüsselte Übertragung zwar belauschen, kennt jedoch den verwendeten Startwert nicht. Solange der Zufallszahlengenerator im kryptografischen Sinne eine genügend gute Qualität hat, sorgt die XOR-Verknüpfung dafür, dass die übertragenen Daten im Wesentlichen den Informationsgehalt eines Rauschens haben und ein Angreifer daraus nicht ohne Weiteres auf den ursprünglichen Inhalt zurückschließen kann.

Kritisch wird es, wenn bei einer späteren Übertragung noch einmal der gleiche Startwert verwendet wird. Angenommen, der Angreifer hätte dies herausbekommen und beide verschlüsselten Nachrichten $C$ und $C'$ aufgezeichnet. Zur Verschlüsselung der Klartexte $P$ und $P'$ wurde RC4 mit demselben Startwert initialisiert. In Konsequenz hat RC4 beide Male eine identische Folge $B$ von Zufallszahlen (Schlüsselstrom) geliefert. Übertragen wurde also einmal $C = P \oplus B$ und das andere mal $C' = P' \oplus B$. Der Angreifer rechnet nun ganz einfach

$$C \oplus C' = (P \oplus B) \oplus (P' \oplus B) = (P \oplus P') \oplus (B \oplus B) = P \oplus P'$$

und hat die XOR-Verknüpfung zweier Klartexte in Händen. Er kennt zwar die beiden Klartexte nicht unmittelbar, oft genug reicht aber bereits dieses Wissen, um die Klartexte mit statistischen Mitteln zu rekonstruieren. Können Teile des Klartextes von $C$ „geraten“ werden, hat man automatisch den entsprechenden Teil des Klartextes von $C'$. Dies fällt umso leichter, je öfter derselbe Schlüsselstrom verwendet wird.

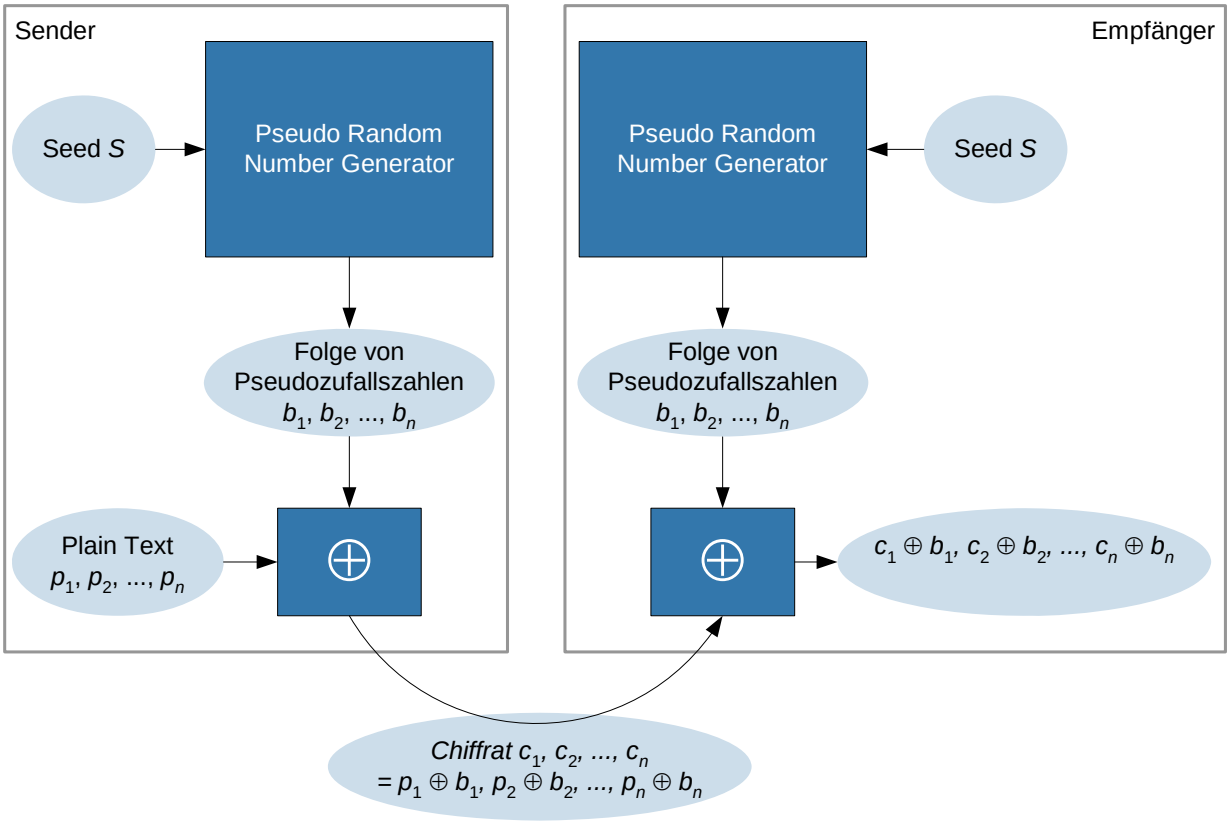



Abbildung 5: Verschlüsselung mit Zufallszahlen

Die Grundregel bei der Verwendung von RC4 (und allen anderen verwandten Verfahren) lautet also: „niemals“ denselben Schlüsselstrom verwenden. Das heißt insbesondere, dass der Startwert, der zur Initialisierung benutzt wird, erst nach einer möglichst langen Zeit wiederverwendet wird. Die Kunst bei der Benutzung von RC4 liegt also in der geschickten Konstruktion des Startwerts aus einem geheimen Schlüssel.

Die Operationen von WEP sind einfach beschrieben:

Es sind zwei Schlüssellängen spezifiziert: 40 Bit und 104 Bit. Über die Art und Weise, wie diese Schlüssel auf Access Points und Clients verteilt werden und, wie sich die Kommunikationspartner auf einen gemeinsamen geheimen Schlüssel einigen, sagt der Standard nichts aus. WEP beginnt mit der Annahme, dass jeder Teilnehmer in einem BSS mit einem gemeinsamen Schlüssel (in der Praxis von Hand) konfiguriert ist.

Die Verschlüsselung erfolgt pro Paket, und zwar wird die MAC-Nutzlast zusammen mit einem CRC-Feld zur Integritätsprüfung (Integrity Check Value, ICV) mit RC4 verschlüsselt. Damit von Paket zu Paket nicht der selbe Initialisierungswert (Seed) für RC4 verwendet wird, gibt es zusätzlich einen 24 Bit langen **Initialisierungsvektor** (IV). Schlüssel und IV zusammen bilden den Initialisierungswert (Seed) von RC4 für das zu übertragende Paket. Damit der Empfänger auch weiß, welcher Wert für den IV zu benutzen ist, wird der IV im Klartext einfach im Header des MAC-Pakets mit übertragen. Für das nächste zu übertragende Paket wiederholt sich das Verfahren mit einem neu gewählten Wert für den IV.

Abbildung 6 und Abbildung 7 zeigen schematisch den Aufbau für Ver- und Entschlüsselung.

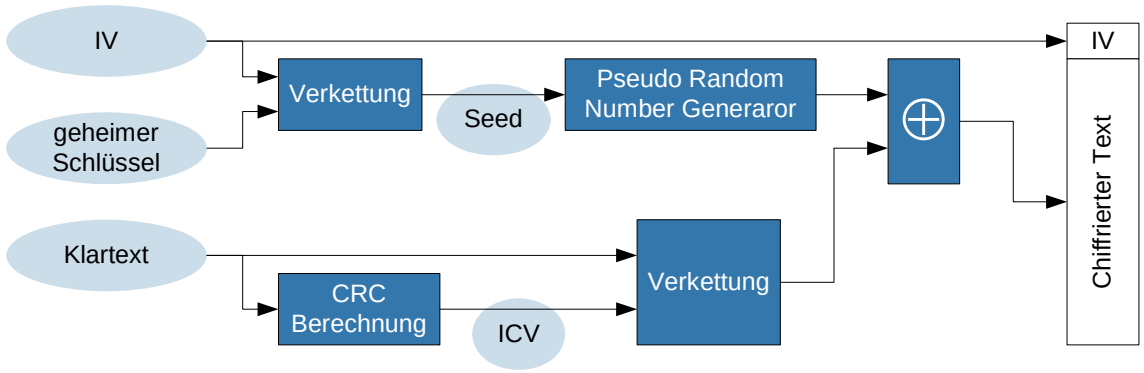



Abbildung 6: Verschlüsselung mit WEP

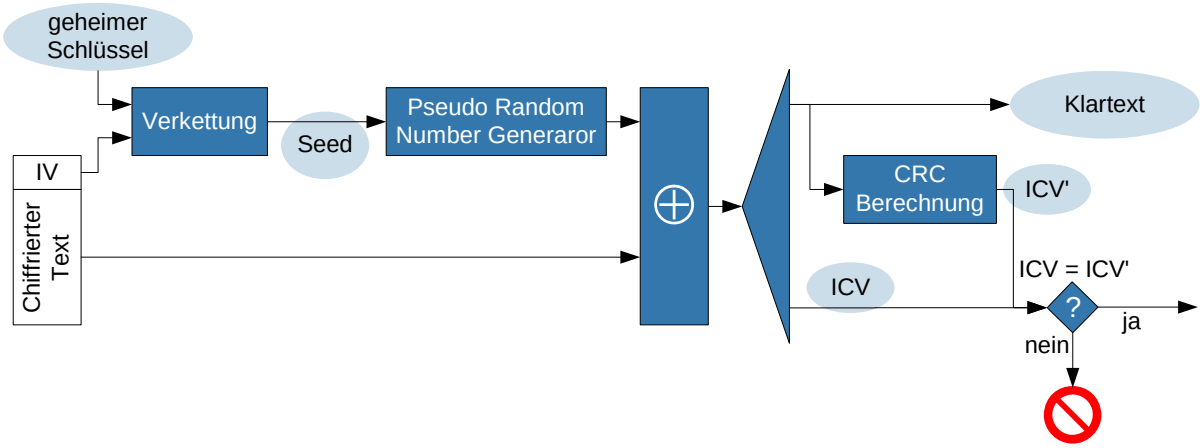



Abbildung 7: Entschlüsselung mit WEP

Das Format eines WEP-verschlüsselten Pakets zeigt Abbildung 8. Die Übertragung von IV und ICV benötigt sieben Byte. Der Standard IEEE 802.11 sieht weiterhin vor, dass auf einem Adapter bis zu vier Schlüssel konfiguriert werden können. Damit bei der Entschlüsselung der Empfänger weiß, welchen der vier Schlüssel er verwenden soll, wird in den zwei Bit des Felds „Key ID“ die Nummer (0, 1, 2 oder 3) des Schlüssels übertragen. Die übrigen sechs Bits zwischen IV und Key ID sind reserviert. Insgesamt werden für WEP acht Byte zusätzlich in einem Paket übertragen. Die in der Abbildung gezeigte Frame Checking Sequence (FCS) ist eine 32 Bit Prüfsumme (Cyclic Redundancy Code, kurz: CRC), die es in einem gewissen Rahmen gestattet, Bitfehler bei der Übertragung zu erkennen. In diesem Fall würde das MAC-Protokoll eine Neuübertragung des Pakets initiieren, sofern nicht eine gewisse konfigurierbare maximale Anzahl von Übertragungsversuchen überschritten würde.

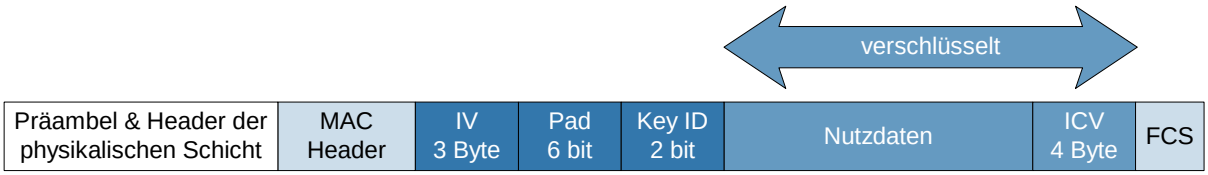



Abbildung 8: Format eines WEP-Pakets

Zu beachten ist, dass lediglich Datenpakete (also Nutzerverkehr) und nur spezielle Managementpakete vom Typ Authentication mit WEP verschlüsselt werden. Insbesondere geschieht die Übertragung der Pakete, die der Auswahl eines Access Points und der Assoziation dienen, unverschlüsselt und ohne weitere Prüfung von Authentizität und Integrität. Dies kann zu Angriffen missbraucht werden.

## 3.2 Kompromittierung von WEP

Die Verwendung eines IV mit einer Länge von 24 Bit bedeutet, dass ein Pool von $2^{24}$ (also etwa 16 Millionen) verschiedenen Initialisierungswerten für RC4 vorliegt. Spätestens danach wiederholt sich erstmalig ein IV, was bei einer Rate von 11 MBit/s und einem genügend ausgelasteten Access Point nach einigen Stunden der Fall wäre. Für das dann gesendete Paket wird ein bereits benutzter Schlüsselstrom wieder verwendet. Eigentlich hätte zwischenzeitlich ein neuer geheimer Schlüssel (40 Bit oder 104 Bit) zwischen den Kommunikationspartnern im BSS (also zwischen Clients und Access Point) vereinbart werden sollen. Dazu sagt der Standard allerdings nichts aus.

IEEE 802.11 spezifiziert kein Schlüsselmanagement.

Des Weiteren macht der Standard keine Aussage darüber, wie die IVs zu erzeugen sind. Einige Hersteller setzten in ihren WLAN-Adaptern den IV bei ihrer Initialisierung auf Null und inkrementieren paketweise um 1. Im Regelfall kommt es dann bereits sehr früh zu einer Wiederholung des IV (nämlich mit jedem neu assoziierten WLAN-Client am Access Point), und der Entschlüsselung durch den Angreifer, wie oben beschrieben, steht nichts mehr im Wege.

Zusätzlich zu dieser Attacke, die eine Entschlüsselung ohne Kenntnis der Schlüssel erlaubt, können Schwächen von WEP ausgenutzt werden, um explizit den symmetrischen Schlüssel zu ermitteln. Dies wird primär durch die charakteristischen Eigenschaften der Nutzung von RC4 und durch die Tatsache, dass der IV im Klartext übertragen wird, verursacht. Ist der Schlüssel einmal bekannt, kann mit einem Protokollanalysator für WLAN jeglicher Verkehr im Klartext aufgezeichnet werden.

Insbesondere die WEP-basierte Shared-Key-Authentifizierung stellt ein Problem dar, da hier schon während des Authentifizierungsvorgangs Informationen ausgelesen werden können, die zur Ermittlung des WEP-Schlüssels nutzbar sind und somit den Aufzeichnungszeitraum verkürzen.

Für Angriffe auf WEP existieren diverse frei verfügbare Werkzeuge, welche unter anderem eine Aufzeichnung des WLAN-Verkehrs vornehmen, die Pakete analysieren und anhand so genannter „interessanter Pakete“ eine (mit der Zeit immer besser werdende) Schätzung des Schlüssels vornehmen können, siehe [FMS01]. Interessante Pakete sind solche, deren Initialisierungsvektor eine spezifische Struktur (unter anderem beispielsweise im zweiten Byte den Wert 255) hat. Bei 40 Bit langen Schlüsseln funktioniert dies sehr gut. Bei manchen 104 Bit langen Schlüsseln kann es jedoch eine recht lange Zeit dauern, bis der Schlüssel ermittelt werden kann.

Inzwischen haben zwar einige WLAN-Ausrüster den Auswahlalgorithmus für den IV dahingehend geändert, dass gewisse IVs vermieden werden, die bei der erwähnten Angriffstechnik als interessante Pakete gewertet würden. Jedoch wurden zwischenzeitlich auch die Verfahren zur Ermittlung des Schlüssels aus aufgezeichneten Paketen verfeinert und entsprechende öffentlich verfügbare Werkzeuge sind seit Ende 2004 verfügbar.

Diese Werkzeuge gestatten bereits bei einem geringeren Volumen an aufgezeichneten Paketen mit einer hohen Erfolgsrate den WEP-Schlüssel zu ermitteln. Es genügt schon oft die rein passive Aufzeichnung von etwa 75000 Paketen (das entspricht typischerweise 100 MByte Daten), die beispielsweise bei der Übertragung von Daten zu einem WLAN-Drucker schnell erreicht werden. Weiterhin kann durch sogenannte Re-Injection-Angriffe das benötigte Verkehrsvolumen durch eine aktive Aktion des Angreifers aus wenigen aufgezeichneten Paketen künstlich erzeugt werden. Dabei wird zunächst versucht, aus den verschlüsselten Übertragungen spezielle Pakete z. B. durch einen Längenvergleich zu erraten (etwa einen ARP-Request[7]) und aufzuzeichnen. Dieser aufgezeichnete Verkehr wird

[7] Das Address Resolution Protocol (ARP) dient zur Ermittlung der MAC-Adresse, an die ein IP-Paket in einer Broadcast-Domäne geschickt werden soll, d. h. der Abbildung einer IP-Adresse auf eine MAC-Adresse.

wieder in das WLAN „injiziert“, der zugrunde liegende Protokollmechanismus wird erneut angestoßen, und Stationen im WLAN antworten (etwa mit einem ARP-Response).

Es gibt grundsätzlich noch eine weitere Möglichkeit, den Schlüssel zu ermitteln:

Da es sich bei WEP um ein symmetrisches Verschlüsselungsverfahren handelt und kein Schlüsselmanagement implementiert ist, welches zumindest in regelmäßigen Abständen die WLAN-Stationen mit einem neuen Schlüssel versorgt, hat ein WEP-Schlüssel im allgemeinen eine lange Lebensdauer. Ein Schlüsselwechsel bei einem WLAN gewisser Größe und Dynamik gestaltet sich oft sogar als unmöglich. Damit bietet sich die Möglichkeit einer klassischen Directory-Attacke an, wie sie von verschiedensten frei verfügbaren Werkzeugen unterstützt wird.

Neben diesen „klassischen“ Angriffen besitzt WEP noch eine ganze Reihe weiterer Schwächen, die zu weiterreichenden Angriffen ausgenutzt werden können. Als weitere Beispiele seien nur die Möglichkeit genannt, sich am Access Point auch ohne Kenntnis des geheimen Schlüssels zu authentifizieren sowie die Möglichkeit, unter Ausnutzung einer Schwäche der CRC-Kodierung für den ICV, Pakete „beliebig“ zu fälschen, ohne dass der CRC dies bemerkt. Letzteres ist nicht überraschend, da ein CRC für die Erkennung von Bitfehlern bei der Übertragung konzipiert wurde, nicht jedoch als Mechanismus zur Sicherstellung der Integrität der Information bei mutwilligen Angriffen.

Für die Absicherung einer WLAN-Übertragung ist WEP insgesamt als ungenügend einzustufen!

## 3.3 Herstellerspezifische Mechanismen

Nachdem die Kompromittierung von WEP veröffentlicht wurde, haben die WLAN-Ausrüster schnell spezifische Verfahren zur WLAN-Absicherung in ihre Produkte integriert. Diese Techniken wurden auch in die Standardisierung zu IEEE 802.11i eingebracht.

Mit der steigenden Verfügbarkeit von Produkten, die WPA bzw. IEEE 802.11i unterstützen, wird die Verbreitung proprietärer Techniken sinken. Da zwischen Kompromittierung von WEP und der Verfügbarkeit zertifizierter WPA-Produkte bzw. der Verabschiedung von IEEE 802.11i zwei bzw. drei Jahre vergangen sind, konnten manche herstellerspezifischen Verfahren eine breite Marktdurchdringung erzielen. Als Beispiel sei hier EAP-Cisco Wireless (kurz: LEAP) genannt, das von einer großen Palette an Client-Systemen unterstützt wird (siehe hierzu auch Kapitel 7.2.6).

In der Praxis kann es daher vorkommen, dass trotz Verabschiedung von IEEE 802.11i noch herstellerspezifische Mechanismen, im Sinne eines kleinsten gemeinsamen Nenners, im WLAN eingesetzt werden bzw. eine Koexistenz zwischen verschiedenen Verfahren ermöglicht werden muss. Mit dem letzteren Aspekt beschäftigt sich das Kapitel 8.

## 3.4 Bewertung und Zusammenfassung

Die genannten Schwächen von WEP führen dazu, dass ein WLAN nach IEEE 802.11 stets mit zusätzlichen, über den ursprünglichen Standard von 1999 hinausgehenden Mitteln abgesichert werden sollte.

Trotzdem sind auch heute noch diverse Client-Systeme im Handel, die lediglich WEP und keine weiteren Sicherheitsmechanismen unterstützen (z. B. manche Barcode Scanner und VoIP over WLAN Handsets). Die Beschaffung solcher Geräte kann aus dem Blickwinkel der Sicherheit in keinster Weise empfohlen werden.

Allerdings sind in der Praxis Altlasten oft nicht vermeidbar, und daher müssen Planer und Betreiber eines WLAN durchaus noch damit rechnen, dass WEP als Verschlüsselungsmethode noch berücksichtigt werden muss. Dies bedeutet nicht, dass in einem solchen „Worst Case“ zwangsläufig alle WLAN-Clients im Sinne eines kleinsten gemeinsamen Nenners lediglich mit WEP abgesichert werden können. Parallel können durchaus leistungsfähigere Sicherheitsinfrastrukturen betrieben werden, wie sie im Kapitel 8 beschrieben werden. Trotzdem verkompliziert dies den Aufbau der Sicherheitsinfrastruk-

tur für das WLAN, und potentiell bestimmt stets das schwächste Glied das insgesamt erreichbare Sicherheitsniveau.

Auch wenn die durch WEP erzielte Absicherung des WLAN recht gering ist, sollte nicht darauf verzichtet werden, sofern Sicherungsmaßnahmen durch die Risikolage des WLAN erforderlich und Alternativen nicht möglich bzw. nicht angemessen sind.

| Funktion | Verfahren | Bewertung | Kommentar |
|---|---|---|---|
| Authentifizierung | Open System Authentication | -- | Sogenannte Null-Authentifizierung, d.h. es wird hier tatsächlich keine Authentifizierung durchgeführt |
| | Shared Key Authentication | -- | Challenge-Response-Verfahren, das allerdings Daten für einen Angriff gegen WEP liefert |
| Integritätsprüfung | CRC32 | -- | Nur zur Erkennung von übertragungsbedingten Bitfehlern geeignet |
| Verschlüsselung | WEP | -- | Entschlüsselung ohne Schlüsselkenntnis und Reverse Engineering der Schlüssel möglich |
| "++" = sehr gut, "+" = gut, "0" = akzeptabel, "-" = mangelhaft, "--" = ungenügend | | | |

Tabelle 1: Ursprüngliche Verfahren in IEEE 802.11 im Überblick

# 4 Einsatz von Firewall-Techniken im WLAN

Da Firewall-Techniken sich beim Schutz der Infrastruktur vor Angriffen aus dem Internet bewährt haben, scheint es zunächst naheliegend zu sein, diese Mechanismen auch zum Schutz vor Angriffen einzusetzen, die vom WLAN ausgehen.

Firewall-Techniken werden hier allgemein als (mehr oder weniger) intelligente Filtermechanismen betrachtet, die grundsätzlich auf allen Protokollebenen von Layer 2 aufwärts operieren können.

Für die Erörterung dieses Themenfelds werden zunächst Access Control Lists (ACLs) auf Layer 2 betrachtet, die im WLAN-Bereich durchaus häufig eingesetzt werden (Kapitel 4.1). Es wird sich allerdings zeigen, dass hiermit nur ein vergleichsweise geringer Schutz erreicht werden kann. Daher wird anschließend in Kapitel 4.2 untersucht, welche Möglichkeiten traditionelle Paketfilter als Abschluss des Distribution Systems bieten. Diese Betrachtungen ergeben zunächst, dass sich auf diese Weise „nur“ die Angriffsfläche reduzieren lässt. Es gibt jedoch Fälle, in denen der Einsatz trotzdem sinnvoll ist. Wenn sich nun ein unberechtigter Zugang zur Infrastruktur mit einer Firewall nicht in jedem Fall blockieren lässt, muss über einen Schutz auf Anwendungs- und Server-Level nachgedacht werden (Kapitel 4.3). Hier werden auch der Einsatz von Application Level Gateways betrachtet und Techniken zur Intrusion Detection und Intrusion Prevention diskutiert. Abbildung 9 fasst die zugrundeliegende Architektur zusammen.

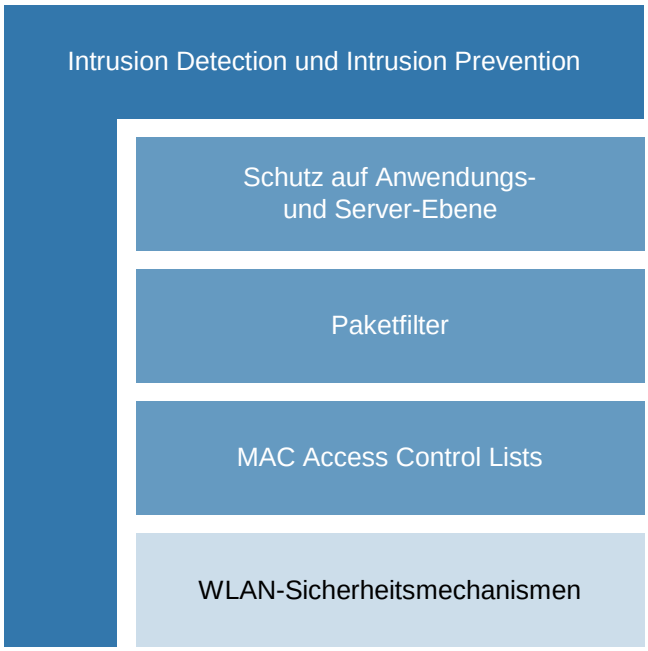



Abbildung 9: Firewall-Techniken zur ergänzenden Absicherung primär von WEP

Falls in einem WLAN Clients betrieben werden müssen, die lediglich WEP (im schlimmsten Fall noch nicht einmal dies) unterstützen, sind Firewall-Techniken und verwandte Methoden oft die einzigen Mittel, die eingesetzt werden können, um eine zusätzliche Absicherung zu WEP zu schaffen.

Beispiele für Clients mit solch eingeschränkten technischen Fähigkeiten können unter anderem bei WLAN Handsets für Voice over IP und bei drahtlosen Barcode Scannern, die im Bereich der Lagerhaltung und Logistik häufig anzutreffen sind, gefunden werden. In der Praxis ist die Unterstützung einer heterogenen Client-Landschaft eine typische Problemstellung für den Aufbau der WLAN-Sicherheitsinfrastruktur.

## 4.1 Access Control Lists auf Layer 2

Die Idee ist naheliegend: Einem Client wird die Kommunikation über einen Access Point mit der dahinterliegenden Infrastruktur nur dann gestattet, wenn dessen MAC-Adresse in einer Zugangskontrollliste (ACL, Access Control List) eingetragen ist. Natürlich wird man ab einer gewissen WLAN-Größe (im Sinne der Anzahl von Clients und Access Points) eine solche Liste nicht mehr lokal auf den Access Points pflegen, sondern die Liste zentral auf einem Server hinterlegen wollen. Als Protokoll bietet sich hier unmittelbar RADIUS an, wobei die MAC-Adresse des Clients bei Anfragen als User-Name behandelt wird. Wenn ein Client sich am Access Point assoziieren möchte, stellt der Access Point zunächst eine RADIUS-Anfrage mit der MAC-Adresse des Clients als User-Name. Der RADIUS-Server prüft, ob er den Nutzer (also die MAC-Adresse) kennt und beantwortet die Anfrage entsprechend. Bei einer positiven Antwort vom RADIUS Server gestattet der Access Point die weitere Kommunikation des fraglichen Clients (Abbildung 10).

Obwohl dieser Mechanismus nicht in IEEE 802.11 festgelegt ist, wird er von vielen Access Points unterstützt.

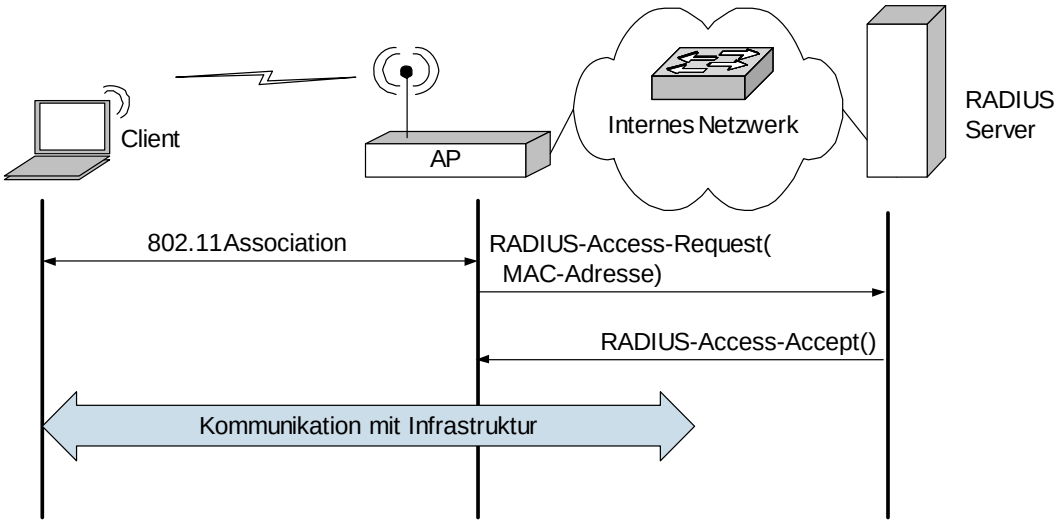



Abbildung 10: MAC-Adressen-Authentifizierung

Bei einem Ausfall der Kommunikation mit dem RADIUS-Server kann sich kein Client neu in das WLAN einbuchen.

Der RADIUS-Server stellt einen sogenannten „Singe Point of Failure“ dar und muss bei entsprechend hoher Verfügbarkeitsanforderung redundant ausgelegt werden.

Am Access Point können hierzu die Adressen von üblicherweise zwei RADIUS-Servern konfiguriert werden. Antwortet der erste Server nicht auf eine Anfrage, wird es beim zweiten Server versucht.

So simpel dieses Verfahren ist, es hat einige Schwächen:

Die Feststellung, ob ein Eintrag in der Access Control List tatsächlich noch zu einem existierenden WLAN-Adapter gehört oder das Gerät schon längst defekt und bereits ausgemustert ist, kann mit der Zeit immer schwieriger werden. Nun könnte man – fast sogar mit Recht – argumentieren, dass dies eine Unterlassungssünde im Bereich des Configuration Managements und des Change Managements sei. Allerdings ist es gerade für derartige Massenartikel nicht einfach, hier die Übersicht zu behalten, insbesondere durch die Vielzahl von verschiedenen Adapter-Typen (vom USB Stick bis zum im Gerät eingebauten Adapter). Unmöglich kann diese Aufgabe beispielsweise für international operierende Organisationen werden, die etwa für Besucher aus anderen Niederlassungen eine Kommunikation über

das WLAN gestatten. Es besteht einfach die Gefahr, entweder für einen wichtigen Besucher zu vergessen, dessen WLAN-Karte in dem RADIUS-Server zu erfassen, oder den entsprechenden Eintrag nicht zu entfernen, obwohl der betreffende Besucher nie wieder zurückkehrt. Die Konsequenz ist eine langsam aber (fast) sicher steigende Anzahl von nicht mehr gültigen Einträgen in der Liste.

Hinzu kommt, dass LAN-Adapter grundsätzlich mit einer „beliebigen" MAC-Adresse konfiguriert werden können, auch wenn jeder LAN-Adapter eine eindeutige auf dem Adapter eingebrannte MAC-Adresse (die sogenannte Burned-in Address) hat. Ein Angreifer auf ein WLAN zeichnet einfach mit einem Protokollanalysator die MAC-Adressen von Clients im WLAN auf. Verlässt ein Client die Funkzelle, die durch einen der beobachteten Access Points aufgespannt wird, konfiguriert der Angreifer seinen Adapter einfach mit der entsprechenden MAC-Adresse des Clients (MAC Address Spoofing) und kann sich am Access Point assoziieren und in das Distribution System hinein kommunizieren.

Es wird lediglich geprüft, ob eine MAC-Adresse als solche authentisch ist. Es wird keine Garantie gegeben, dass sich hinter der MAC-Adresse auch der erwartete Adapter verbirgt.

In diesem Sinne ist der Gewinn an Sicherheit durch diese Methode natürlich als fragwürdig zu bewerten. Trotzdem kann nicht jedermann automatisch ohne ein gewisses Quantum an Fachwissen diese Hürde überspringen. Außerdem bedeutet dieser Mechanismus auch für den versierten Angreifer ein wenig Arbeit, sodass trotz aller Bedenken Zugriffslisten mit MAC-Adressen nach wie vor oft in der Praxis anzutreffen sind.

Ein interessanter Problembereich ist allgemein das Roaming zwischen Standorten und damit verbunden die Fragestellung, ob ein zentraler RADIUS-Server, der alle Standorte bedient, aufgebaut wird oder ein RADIUS-Server pro Standort. Im ersteren Fall ist die Verfügbarkeit der WAN-Strecken zum zentralen Server mit zu berücksichtigen. Im zweiten Fall ist zu überlegen, ob eine Synchronisation der Server notwendig ist, damit die MAC-Adresse des Clients eines Besuchers von einem anderen Standort automatisch akzeptiert wird, oder ob eine Prozedur, bei der die fragliche MAC-Adresse manuell lokal vor Ort eingepflegt wird, an dieser Stelle ausreicht. Letzteres ist oft sinnvoll, wenn der Standortwechsel eines WLAN-Adapters vergleichsweise selten geschieht.

Eine ACL auf Layer 2 ist als schwacher Sicherheitsmechanismus einzustufen, der lediglich als flankierende Maßnahme unter besonderen Rahmenbedingungen noch in Betracht gezogen werden sollte (siehe Kapitel 8).

## 4.2 Paketfilter

Der Übergang zwischen Distribution System und dem eigentlichen LAN stellt einen natürlichen Kontrollpunkt („Single Point of Control") zwischen dem WLAN als unsicherem Bereich und dem abzusichernden Bereich (LAN-Infrastruktur) dar.

Ein Paketfilter (Firewall) kann an diesem Punkt den Kommunikationsverkehr analysieren, Anomalien erkennen und aufzeichnen sowie bei Bedarf entsprechende Alarme senden. Gerade die Funktion der Aufzeichnung von Ereignissen ist essentiell, da es nicht nur darauf ankommt, einen Angriff abzuwehren, sondern auch darauf, ihn zu dokumentieren. Es wird unterschieden zwischen statischen (stateless) Paketfiltern und dynamischen (stateful) Paketfiltern, die den Kontext eines Pakets erkennen und so verbindungsorientiert arbeiten können.

Das zugehörige Regelwerk für einen Paketfilter ist vergleichsweise simpel: In Abhängigkeit von der Quell-IP-Adresse dürfen nur gewisse Ziel-IP-Adressen erreicht und nur gewisse Dienste (d. h. TCP/UDP-Ports) genutzt werden. Pakete, die nicht diesen Regeln entsprechen, werden verworfen.

Diese Maßnahme verkleinert zunächst lediglich die Angriffsfläche, da nur noch dedizierte Dienste und Ziele erreichbar sind. Die freigeschalteten Ziele und Dienste bleiben aber ohne weitergehende Mechanismen auch für einen Angreifer weiterhin erreichbar.

Die notwendigen Funktionen werden praktisch von jedem Paketfilter angeboten. Wireless Switches, die eine Zentralisierung von WLAN- und Mobilitätsfunktionen von den Access Points hin zum Distribution System ermöglichen (siehe auch Kapitel 9 und 10), bieten ebenfalls oft eine Paketfilter-Funktion. Dies stellt eine weitere Option dar, deren Funktionsumfang im Vergleich zu einer „echten“ Firewall im Einzelfall bewertet werden sollte.

Der Einsatz einer Firewall bietet allerdings auch weitergehende Möglichkeiten, denn eine Firewall kann Abweichungen vom normalen Protokollablauf feststellen. Diverse Firewalls auf Paketfilter-Basis sind inzwischen zusätzlich mit verschiedenen Filtern gegen „Standard-Attacken“ auf Session- und Anwendungsebene ausgestattet. Hier muss zwischen dem Investitionsaufwand und der erreichbaren Sicherheit abgewogen werden.

Zu beachten ist bei dieser Architektur, dass die Firewall ein zentraler Verkehrsknotenpunkt ist, wie in Abbildung 11 illustriert. Der Ausfall der Firewall führt zwangsläufig zu einem Ausfall der Kommunikation im gesamten WLAN.

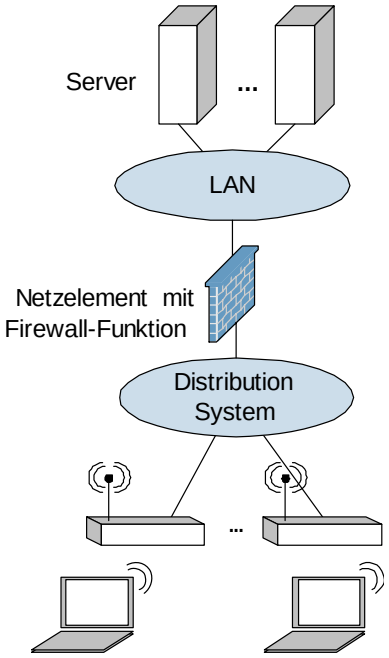



Abbildung 11: Abschluss des Distribution System durch eine Firewall

Die Firewall sollte daher bei entsprechenden Verfügbarkeitsanforderungen redundant ausgelegt sein.

Die Redundanz basiert üblicherweise auf dem Hot-Standby-Prinzip. Eine Firewall ist produktiv (Master-Modus), und eine zweite Firewall im Standby-Modus überwacht den Master. Bei Störungen am Master übernimmt der Standby dessen Funktion (Failover). Für diese Funktion kann das Virtual Router Redundancy Protocol (VRRP) oder eine Herstellerlösung zum Einsatz kommen. Damit bei einem Failover nicht nur die aktiven Netzverbindungen auf Layer 3 umgeschaltet werden, sondern auch der Status der höheren Protokolle, muss der Standby genau denselben internen Zustand haben wie der Master. Hierzu dient ein State Synchronization Protocol. Dieses Protokoll ist herstellerspezifisch und läuft üblicherweise auf einem dedizierten Link zwischen den Firewalls.

Die Firewall muss weiterhin geeignet dimensioniert sein, um den kumulierten Verkehr aller Clients im WLAN bedienen zu können. Dies muss insbesondere bei einer geplanten Nutzung von IEEE 802.11g bzw. IEEE 802.11a berücksichtigt werden, da hier mit höheren Nettodatenraten zu rechnen ist.

Insgesamt kommt eine Firewall als Schutzmechanismus für den Zugang zu Infrastruktur-Ressourcen über ein WLAN primär dann in Frage, wenn bedingt durch die WLAN-Anwendung und die Produktsituation am Markt die Notwendigkeit besteht, Clients mit limitierten technischen Möglichkeiten (WEP) zu betreiben. Dies ist z. B. bei diversen Barcode Scannern und VoIP Handsets der Fall.

## 4.3 Schutz auf Server- und Anwendungsebene

Beim Einsatz einer Paketfilter-Firewall bleibt die Bedrohungslage durch offene Ports und hierüber erreichbare Server bestehen. Dies ist darin begründet, dass die Initiierung einer Kommunikationsbeziehung bei den meisten Anwendungen vom Client ausgeht, und dieser liegt bei einem WLAN (analog zum Remote Access über das Internet) nun einmal im unsicheren Bereich.

In Abhängigkeit von dem sich ergebenden Risiko müssen also noch weitergehende Sicherheitsmaßnahmen umgesetzt werden. Dies ist insbesondere der Fall, wenn im WLAN nicht nur Spezialanwendungen über dedizierte Protokolle genutzt werden, sondern auch auf (kritische) Standardprotokolle wie z. B. HTTP und telnet zurückgegriffen wird.

Weitergehende Schutzmaßnahmen können dann nur auf Anwendungs- und Server-Ebene greifen. Es ist dabei insbesondere nach dem jeweiligen Stand der Technik sicherzustellen, dass ein Angriff verhindert wird, der eine Übernahme eines Servers erlaubt. Folgende Maßnahmen, die allerdings vergleichsweise aufwändig sind, können in dieser Situation in Betracht gezogen werden:

- **Härtung:** Die über das WLAN erreichbaren Server werden geeignet gehärtet. Unter anderem wird dabei sichergestellt, dass das System nach dem aktuellen Stand gepatcht und parametriert ist sowie nicht genutzte Dienste deaktiviert sind. Dies ist insbesondere empfehlenswert, wenn Standardanwendungsprotokolle über das WLAN genutzt werden und für gewisse Softwarestände der eingesetzten Betriebssysteme bereits eine Palette von Angriffstechniken bekannt ist.
- **Application Proxy**: Die Firewall-Architektur wird um einen Application Proxy für die Anwendung ergänzt. Dieser Proxy analysiert das Anwendungsprotokoll und ist in der Lage, unerlaubte Pakete und Protokollsequenzen zu filtern. Für proprietäre Anwendungsprotokolle bedeutet dies allerdings in der Regel einen gewissen zusätzlichen Entwicklungsaufwand.
- **Intrusion Detection System**: Die Firewall-Architektur wird um ein Intrusion Detection System (IDS) ergänzt, das Angriffsmuster erkennen kann. Da die Erkennung auf bekannten Angriffsschemata basiert, muss ein IDS für proprietäre Anwendungsprotokolle zusätzlich angelernt werden. In diesem Zusammenhang muss auch auf Wireless IDS hingewiesen werden, die unmittelbar die Luftschnittstelle eines WLAN beobachten und bei Feststellung etwa eines fremden Access Points einen Alarm auslösen können. Diese Werkzeuge werden noch in Kapitel 10 diskutiert.
- **Isolierung des Servers**: Alternativ kann der entsprechende Server an ein isoliertes VLAN angeschlossen werden, das ausschließlich vom WLAN erreichbar ist, oder an eine DMZ der Firewall.

## 4.4 Bewertung und Zusammenfassung

Firewall-Techniken dienen bei der Absicherung eines WLAN primär der Verkleinerung der Angriffsfläche.

Firewall-Mechanismen, die über die reine Paketfilterfunktion hinausgehen, können einen zusätzlichen Schutz geben.

Das Problem beim Einsatz von Firewall-Techniken zum Schutz eines WLAN liegt primär darin begründet, dass der Client, der einen Dialog initiiert, im unsicheren Bereich (hier im WLAN) liegt. Hier ist es wichtig, die Analogie zu Remote-Access-Lösungen (insbesondere IP-VPN) zu beachten.

Firewall-Techniken sollten also eher eine ergänzende Funktion zu eigentlich wirksamen Sicherheitsmechanismen für das WLAN haben, etwa um Verkehrsflüsse zu kontrollieren und zu steuern.

Wichtig sind Firewall-Techniken insbesondere, wenn einfache WLAN-Clients eingesetzt werden müssen, für die keine erweiterten (über WEP hinausgehenden) Sicherheitsmechanismen angeboten werden. Beispiele sind Barcode Scanner, VoIP Handsets aber auch Drucker. In diesen Fällen kann der Einsatz von Firewall-Techniken tatsächlich die einzig sinnvolle Maßnahme zur Ergänzung von WEP sein.

# 5 Einsatz von VPN zur Absicherung des WLAN

Genauso wie der Remote Access eines Clients über das Internet auf die eigene Infrastruktur mit einem IP-basierten Virtual Private Network (VPN) geeignet abgesichert werden kann, ist es möglich, die Kommunikation über ein WLAN zu schützen. Ob der Zugriff auf interne Ressourcen über ein WLAN erfolgt oder über das Internet, macht aus dem Blickwinkel eines IP-VPN keinen Unterschied. Der Aufbau ist vergleichsweise einfach, die Protokolle standardisiert, die Technik ist in der Praxis bewährt und es gibt genügend Produkte auf dem Markt. Im einfachsten Fall wird die IP-VPN-Lösung, die man beispielsweise bereits zur Anbindung von mobilen Mitarbeitern einsetzt, für die Absicherung des WLAN noch einmal verwendet.

Dies gilt grundsätzlich genauso für VPN, die auf dem Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS)[8] aufbauen. Solche sogenannten SSL-VPNs nutzen ebenfalls größtenteils standardisierte Protokolle, die sich seit vielen Jahren in der Praxis bewährt haben, sind aber tatsächlich ein vergleichsweise neues Thema, da die Protokolle und Techniken in einer neuen Form und Kombination zur Anwendung kommen. Es gibt mittlerweile ebenfalls eine große Anzahl verfügbarer Produkte, die sich bzgl. der eingesetzten Techniken und damit im Funktionsumfang und den mit ihnen realisierbaren Lösungen erheblich unterscheiden.

Bis zur Verfügbarkeit von Produkten mit Wi-Fi Protected Access war ein VPN tatsächlich auch die einzige Alternative, ein sicheres WLAN aufzubauen, wollte man nicht auf herstellerspezifische WLAN-Erweiterungen zurückgreifen. Insbesondere IP-VPN sind entsprechend häufig noch in aktuellen WLAN-Installationen anzutreffen. Aufgrund der Tatsache, dass SSL-VPN-Produkte noch nicht allzu lange am Markt verfügbar sind, findet man sie bisher sowohl in Remote-Access-Szenarien als auch in WLAN-Installationen vergleichsweise selten. Daher wird im Folgenden schwerpunktmäßig auf IP-VPN eingegangen und lediglich bei Bedarf auf die entsprechende Lage bei SSL-VPN hingewiesen. Detailliertere Informationen zum Thema VPN sind im Anhang dieses Dokuments aufgeführt.

## 5.1 Architektur

Grundidee ist der Abschluss des Distribution System durch ein VPN-Gateway. Das WLAN (mit Access Points und Distribution System) bildet das unsichere Transportnetz, über das durch einen entsprechend verschlüsselten Tunnel zwischen Client und VPN-Gateway ein gesicherter Kommunikationskanal etabliert werden kann.

Die Kommunikation über das WLAN hinaus mit der weiteren Infrastruktur geschieht ausschließlich über das VPN-Gateway. Der Aufbau des Tunnels muss dabei an eine geeignet starke Authentifizierung der Kommunikationspartner geknüpft sein.

Abhängig von den eingesetzten Techniken und Produkten steht hierzu eine große Anzahl verschiedener Authentifizierungsmethoden zur Verfügung. Smartcards und Token gehören derzeit zu den sichersten Authentifizierungswerkzeugen, da sie in einer geeigneten Form die Authentifizierungsmerkmale Besitz und Wissen vereinen. Token generieren üblicherweise Einmalpasswörter (One Time Password, OTP) und haben gegenüber Smartcards den Vorteil, dass keine technische Kommunikationsschnittstelle zum Client (Smartcard-Reader, Software) erforderlich ist. Allerdings sind sie nur schwierig in populäre Verzeichnisdienste zu integrieren, sodass es derzeit meist auf eine von der Betriebssystemanmeldung verschiedene, zusätzliche Authentifizierung hinausläuft. Im Gegensatz dazu

[8] TLS ist der aktuell in RFC 2246 standardisierte „Ersatz“ für SSL 3.0. Die beiden Protokolle entsprechen einander im Wesentlichen, sind infolge einiger Unterschiede in der Spezifikation jedoch nicht kompatibel zueinander. Die meisten aktuellen Produkte unterstützen beide Protokolle; insofern erscheint es aus Sicht der Applikation, die SSL/TLS nutzt – hier eine VPN-Lösung – gerechtfertigt, die Begriffe synonym zu verwenden. Da sich SSL im allgemeinen Sprachgebrauch eingebürgert hat, wird dieser Begriff im Folgenden verwendet.

bieten manche Smartcard-Lösungen mit der Integration in einen Verzeichnisdienst (implizite und automatische Abbildung von Smartcard-Zertifikaten zu Nutzern) nicht nur eine Authentifizierung bei RAS/VPN, sondern auch eine Anmeldung an lokale Rechner, eine Authentifizierung bei Zugriff auf entfernte Ressourcen (Kerberos) und eine Anmeldung über IEEE 802.1X (siehe Kapitel 6).

Abbildung 12 zeigt die grundsätzliche Architektur im Überblick. Das VPN-Gateway kann als Modul einer ggf. eingesetzten Firewall oder als separate Hardware realisiert sein. Werden im WLAN ausschließlich VPN-fähige Clients eingesetzt, spricht nichts dagegen, lediglich ein (geeignet gehärtetes) VPN-Gateway zu verwenden und auf eine dedizierte Firewall zu verzichten.

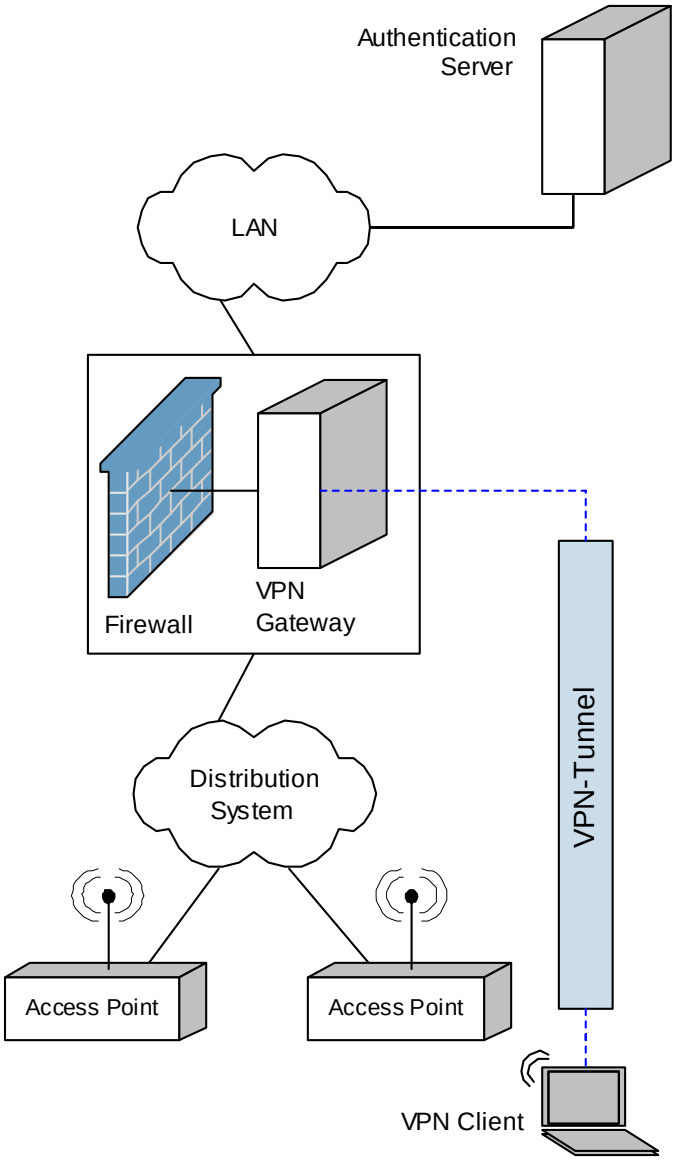



Abbildung 12: Absicherung des WLAN mit einem VPN

Als wesentlicher Standard für den Aufbau eines IP-VPN hat sich IPSec durchgesetzt.

Die Verschlüsselung der Daten geschieht oft noch mit 3DES (Triple Data Encryption Standard) unter Verwendung von mindestens 128 Bit Schlüssellänge (netto 112 Bit), bei aktuelleren Implementierungen in der Regel 192 Bit (netto 168 Bit). Der Einsatz moderner Verfahren, wie der Advanced Encryption Standard (AES), ist allerdings bevorzugt zu empfehlen.

IPSec sieht lediglich eine gegenseitige Authentifizierung der Kommunikationspartner auf Systemebene vor; die Identität des Benutzers wird nicht geprüft.

Es gibt allerdings Situationen, in denen die Authentifizierung auf Systemebene nicht genügt und eine Authentifizierung des Nutzers erforderlich ist. Hier sind verschiedene Ansätze zur Lösung des Problems denkbar und zum Teil durch Hersteller von VPN-Produkten realisiert worden, allerdings werden hierdurch mangels einheitlichem Standard erneut Inkompatibilitäten geschaffen. Das aktuelle Lösungsspektrum reicht von der Smartcard-basierten Kopplung der Systemidentifikation an den Benutzer über Erweiterungen des Internet-Key-Exchange-Protokolls (IKE), Verwendung ineinander geschachtelter Tunnelmechanismen bis zur nachgelagerten Authentifizierung jenseits des VPN-Tunnels, z. B. an einer Firewall. Alle Ansätze weisen sowohl Vor- als auch Nachteile auf. Ein Beispiel ist die Verwendung von L2TP innerhalb einer mit IPSec gesicherten Kommunikationsbeziehung, wie sie in RFC 3193 spezifiziert ist (siehe [L2TP01] und Kapitel 15.3.7.).

## 5.2 Verfügbarkeit

Da der gesamte Verkehr durch das VPN-Gateway fließt, bildet das VPN-Gateway einen „Single Point of Failure“ und muss bei entsprechenden Verfügbarkeitsanforderungen redundant ausgelegt werden.

Das VPN-Gateway kann dabei als Modul einer Firewall realisiert werden (siehe Kapitel 4.2). In diesem Fall ist die Redundanz der Firewall gleichbedeutend mit der Redundanz des VPN-Gateways. Dies ist typisch für ein IP-VPN. Bei SSL-VPN stellt dies noch eher die Ausnahme dar, üblicherweise sind die Gateways bislang in Form einer zusätzlichen Komponente (Appliance oder Server) verfügbar – es zeichnet sich aber ab, dass Firewall-Hersteller in naher Zukunft SSL-VPN-Module für ihre Produkte anbieten werden.

Wird dagegen das VPN-Gateway als separates Netzelement, z. B. in einer DMZ der Firewall, installiert, so muss die Redundanz für dieses Netzelement separat betrachtet werden. Ein dynamisches Redundanzverfahren erfordert (analog zur Diskussion der Firewall-Redundanz) eine Synchronisation der internen Zustände zwischen den redundanten VPN-Gateways, wenn bei einem Failover die bestehenden VPN-Tunnel aufrecht erhalten werden sollen. Hierzu dient ein State Synchronization Protocol, das insbesondere die Zustände der kryptografischen Automaten von dem aktiven VPN-Gateway zum Backup VPN-Gateway übertragen muss. Diese Information ist hochsensibel und der Übertragungsweg muss geeignet abgesichert sein. Das State Synchronization Protocol ist herstellerspezifisch und läuft üblicherweise auf einer dedizierten Verbindung zwischen den VPN-Gateways. Bedingt durch diesen Aufwand wird in der Praxis oft auf ein solches vollständiges Failover verzichtet, um den Preis von abbrechenden Kommunikationsbeziehungen beim Wechsel.

Die Failover-Entscheidung kann bei einem dynamischen Redundanzprotokoll durch VRRP oder durch proprietäre Mittel erfolgen. Alternativ kann ein VPN-Gateway auch als hochverfügbarer Server Cluster realisiert werden.

Kann auf die Forderung einer transparenten Übergabe bestehender VPN-Tunnel zwischen den redundanten VPN-Gateways verzichtet werden, wird der State Synchronization Link (und die zugehörige Synchronisationssoftware) nicht benötigt. In diesem Fall bricht der VPN-Tunnel bei Ausfall des vom Client angesprochenen VPN-Gateways zwar ab, jedoch reicht es für den Client den VPN-Tunnel neu aufzubauen, denn er wird automatisch zum zweiten VPN-Gateway geleitet.

Manche VPN Clients unterstützen die Konfiguration mehrerer VPN-Gateways. Ist ein Tunnelaufbau zu einem Gateway nicht erfolgreich, so versucht der VPN Client automatisch einen Tunnelaufbau zum nächsten VPN-Gateway in der Liste. Eine solche Lösung kann grundsätzlich auch eingesetzt werden.

## 5.3 Leistung und Skalierbarkeit

Das VPN-Gateway muss die kumulierte Nutzlast zwischen Distribution System und LAN transportieren. Der Verkehr von und zu allen WLAN Clients muss zwangsläufig das VPN-Gateway passieren. Bei einer ungenügenden Dimensionierung kann es hier zu einem Engpass und damit verbundenen Einbußen hinsichtlich der Verfügbarkeit kommen.

In vielen Anwendungsbereichen kann nicht a priori ausgeschlossen werden, dass zukünftig eine Verkehrsbelastung auftritt, die vom VPN-Gateway einen Durchsatz von deutlich mehr als 200 MBit/s erfordert. Eine solche hohe Verkehrsbelastung des VPN-Gateways ergibt sich typischerweise bei größeren WLAN-Installationen mit einer entsprechend hohen Anzahl von Access Points und Clients.

Hier ist die Verschlüsselungsleistung besonders kritisch, da komplexe Berechnungen für jedes Paket stattfinden. Werden an dieser Stelle keine entsprechend leistungsfähigen Appliances eingesetzt, kann die Installation eines Clusters mit Lastverteilung in Betracht gezogen werden.

Falls die weitere Entwicklung des WLAN-Kommunikationsverkehrs nicht genügend genau vorausgesagt werden kann, ist der Einsatz einer flexibel skalierbaren Lösung entscheidend, die es erlaubt, zunächst eine Lösung mit einer vergleichsweise geringeren Durchsatzleistung zu implementieren, die bei steigendem Bedarf schrittweise ausgebaut werden kann.

## 5.4 Verwundbarkeiten und Bedrohungen

Sowohl IP- als auch SSL-VPNs sind nach heutigem Erkenntnisstand als sicher anzusehen, sofern das System geeignet konfiguriert ist und die eingesetzten Werkzeuge und Prozesse einen sicheren Betrieb ermöglichen.. Insbesondere bei IP-VPNs werden größtenteils weit verbreitete, lange erprobte Techniken eingesetzt, die sich in der Praxis bestens bewährt haben. Selbstverständlich kann es aufgrund von Implementierungsfehlern einzelner Hersteller trotzdem zu Schwachstellen und somit Angriffspunkten kommen. Nach derzeitigen Erkenntnissen ist – abgesehen von den oben genannten allgemeinen Gefahren – nicht mit speziellen WLAN-spezifischen Verwundbarkeiten und Bedrohungen zu rechnen.

Es muss allerdings auf einen kritischen Bereich hingewiesen werden:

In der Zeit zwischen Aktivierung des WLAN-Adapters bis zum Aufbau des VPN-Tunnels bzw. nach dem Abbau des Tunnels bis zum Abbau der WLAN-Verbindung ist ein Client für kurze Zeit verwundbar. Diese Phase kann ein Angreifer benutzen, um Schwachstellen im Client auszunutzen.

Ein VPN Client sollte daher auch für den WLAN-Einsatz zusätzlich mit einer Personal Firewall (vgl. auch Kapitel 12) geschützt werden.

Je nach Produkt ist die Firewall-Funktion oft schon Bestandteil der VPN Client Software. Beim Einsatz einer Personal-Firewall im WLAN-Bereich ist allgemein darauf zu achten, das lokale Subnetz, in dem sich der Nutzer im WLAN befindet, als nicht vertrauenswürdig zu klassifizieren. Weiterhin sollte der VPN Client die Unterbindung eines sogenannten Split Tunneling unterstützen. Ein Split Tunnel gestattet die gleichzeitige Kommunikation mit Stationen über den VPN-Tunnel und mit Stationen im Transport Netz. Im WLAN-Fall bedeutet dies eine Kommunikation außerhalb des VPN-Tunnels mit anderen Stationen im Distribution System oder bei einem Hotspot auch mit Stationen im öffentlichen Internet. Dies kann zur Backdoor für Angreifer werden.

## 5.5 Vergleich zwischen IP-VPN und SSL-VPN

Für die Absicherung eines WLAN ist ein IP-VPN mit IPSec grundsätzlich als sicherer als die heute marktgängigen SSL-VPN[9] einzustufen, da die gesamte über das VPN-Gateway abgewickelte Kommunikation geschützt ist. Übliche SSL-VPN hingegen schützen „lediglich" die Kommunikation ausgewählter Applikationen. Auch im Bereich des Client-Schutzes bietet IPSec wesentliche Vorteile; SSL-VPN sind hier prinzipbedingt im Nachteil, da sie auf einem höheren OSI-Layer arbeiten.

Allerdings können sich SSL-VPN durch eine Reihe von Eigenschaften von IP-VPN absetzen und zwar genau an den Stellen, an denen IP-VPN Restriktionen aufweisen. Beide Lösungsansätze – IPSec wie auch SSL – weisen offenkundig sowohl Stärken als auch Schwächen auf:

- IPSec bietet sehr sicheren volltransparenten Netzzugriff. Damit ist der Nutzer hinsichtlich der Auswahl seiner Anwendungen nicht weiter eingeschränkt. Nachteilig sind die vergleichsweise aufwändige Administration und die eingeschränkte Client-Auswahl. Weiterhin kann der Einsatz von NAT zu Problemen führen, da z. B. die IP-Adresse in der Berechnung kryptografischer Prüfsummen berücksichtigt werden kann. Die in diesem Falle einsetzbaren Techniken, wie NAT Traversal, werden im Anhang in Kapitel 15.3.6 beschrieben.
- Gängige SSL-VPN-Lösungen sind in der Regel „clientless", d. h. meist ist abgesehen von einem geeigneten Webbrowser kein gesondert zu installierender Client notwendig. Hieraus resultiert auch eine weitreichende Betriebssystem-Unabhängigkeit. Diese Lösungen sind daher günstiger zu administrieren und flexibler im Einsatz. Allerdings bindet man sich oft mit dem eingesetzten Produkt an bestimmte nutzbare Applikationen. Spätere Erweiterungen sind hier problematisch. Außerdem kann eine adäquate Sicherheit bei Nutzung fremder Client-Systeme nicht garantiert werden.

Abhängig vom konkreten Anwendungsfall und von den jeweiligen Rahmenbedingungen kristallisiert sich meist eine der beiden Techniken als die Methode der Wahl heraus. Die Entscheidung hängt von einer Vielzahl von Faktoren ab. Dazu zählen beispielsweise:

- Welche Art von Zugriff wird benötigt?

  Bei permanentem Zugriff auf alle verfügbaren Ressourcen, d. h. einem transparenten Szenario, bietet sich IPSec als Methode der Wahl an, während bei nur sporadischer Nutzung einzelner Anwendungen, etwa bei mobilen Nutzern, SSL Vorteile bietet – vorausgesetzt, die jeweilige Anwendung lässt sich per SSL-VPN abbilden.

- Sind die Anwender eigene Mitarbeiter?

  Werden ausschließlich eigene Mitarbeiter versorgt, lässt sich dies auf Basis standardisierter IPSec-basierter Lösungen mit zentralem Management bei maximaler Sicherheit realisieren. Kommen auch andere Nutzer in Betracht, so sollte SSL favorisiert werden, um die Notwendigkeit der speziellen Clients zu vermeiden; diese bedingen kaum abzuschätzende Problemfelder im Betrieb.

- Wie kritisch ist der Vertraulichkeitsschutz?

  Bei hohen Anforderungen an Verschlüsselungsstärke und Authentifizierungsstandard ist IPSec zu empfehlen.

---

[9] Praktisch alle kommerziellen SSL-VPN-Produkte basieren auf Terminal-Server-Ansätzen, die ausgewählte Anwendungen per Browser-Interface nutzbar machen (vgl. auch Kapitel 15.4); von diesem Ansatz wird im Folgenden ausgegangen. Darüber hinaus existieren auch Ansätze transparenter VPN auf SSL-Basis (z. B: OpenVPN), die dann ähnlich wie IPSec-basierte Lösungen einzustufen sind. Generell ist der Begriff „SSL-VPN" aktuell sehr unscharf definiert.

- Wie kritisch sind die Ressourcen, auf die zugegriffen wird?

  Auf kritische Ressourcen sollte nicht von Clients mit undefiniertem Sicherheitsstandard zugegriffen werden; das gilt sowohl für die jeweiligen Zielsysteme als auch für die ggf. übertragenen Informationen. Für solche Einsatzfälle verbietet sich SSL quasi von selbst.

- Wie versiert sind die Anwender im Umgang mit der Technik?

  Je weniger Erfahrung die Anwender im Umgang mit der eingesetzten Technik haben, desto einfacher sollte die Handhabung des Clients sein. Hier bietet die SSL-Lösung durch Einsatz der gewohnten Browsertechnologie enorme Vorteile gegenüber spezialisierten IPSec-VPN-Clients.

Bei der Planung des Einsatzes ist außerdem zu berücksichtigen, wie wichtig eine schnelle Einsatzfähigkeit bzw. eine spätere Skalierbarkeit der Lösung sind.

SSL-basierte Lösungen lassen sich in aller Regel schneller ausrollen – schließlich wird meist kein Client benötigt – als IPSec-VPN. Allerdings bindet man sich mit dem eingesetzten Produkt an bestimmte nutzbare Applikationen. Spätere Erweiterungen sind hier problematisch, während IPSec durch den Zugriff auf Netzwerkebene wesentlich mehr Flexibilität bietet.

## 5.6 Bewertung und Zusammenfassung

Die Verwendung eines IP-VPN (eine geeignete Authentifizierung und Verschlüsselung auf dieser Ebene vorausgesetzt) kann grundsätzlich zum Schutz der WLAN-Übertragung empfohlen werden.

Das VPN-Gateway ist allerdings den Durchsatzanforderungen entsprechend zu dimensionieren und je nach zu erzielender Verfügbarkeit redundant auszulegen.

Ein VPN eignet sich zunächst vor allem für den Schutz von WLAN, die noch mit älteren Access Points ausgestattet sind, welche sich nicht auf WPA bzw. IEEE 802.11i aufrüsten lassen. In vielen Fällen besteht der Wunsch, ein bereits erfolgreich eingesetztes VPN-Produkt auch im WLAN weiter zu nutzen und so den zusätzlichen Konfigurationsaufwand für IEEE 802.11i oder WPA zu vermeiden. Es gibt auch Situationen, in denen Clients eingesetzt werden müssen, für die aktuell noch keine Möglichkeit besteht, sie auf IEEE 802.11i bzw. WPA aufzurüsten, jedoch eine VPN-Lösung verfügbar ist[10].

Ein weiterer Vorteil bei der Verwendung eines VPN für den WLAN-Schutz ist die Tatsache, dass sich die Absicherung nicht nur auf die Luftschnittstelle (d. h. zwischen Client und Access Point) sondern auch auf das Distribution System erstreckt. In manchen Bereichen ist es aus baulichen Gründen nicht möglich, einen Access Point versteckt zu installieren (etwa oberhalb einer Zwischendecke), sondern nur sichtbar, z. B. an einer Wand. In öffentlich zugänglichen Bereichen, die mit einem WLAN versorgt sind, ist damit das Problem eines unberechtigten Zugangs zum Access Point verbunden. Neben dem Diebstahlrisiko besteht hier Gefahr, dass ein Angreifer versucht, an einem zugänglichen Access Point einen Weg in die Infrastruktur über den Ethernet-Anschluss des Access Points zu finden. Der Schutz durch WEP, WPA und IEEE 802.11i erstreckt sich nur auf die Luftschnittstelle, und der Ethernet-Anschluss wird nicht weiter berücksichtigt. Bei der Verwendung eines VPN ist es unerheblich, ob sich der Angreifer an der Luftschnittstelle oder an einem Port des Distribution Systems befindet, denn der schützende Tunnel reicht vom Client bis zum VPN-Gateway.

Mit der steigenden Verfügbarkeit von WPA-zertifizierten und IEEE 802.11i-konformen Produkten, ist es nicht unwahrscheinlich, dass der Einsatz von VPN zur Absicherung eines WLAN entsprechend zurückgehen wird.

[10] Es kann natürlich auch der umgekehrte Fall eintreten.

# 6 Wi-Fi Protected Access und IEEE 802.11i

Die im Kapitel 3 genannten Sicherheitslücken haben in IEEE 802.11 im Mai 2001 zur Gründung der „Task Group i“ geführt, die an einer neuen Sicherheitslösung für WLAN gearbeitet hat. Die entsprechende Spezifikation wurde im Juni 2004 verabschiedet (siehe [IEEE04a]) und wird in Kapitel 6.1 vorgestellt. Da der WLAN-Markt eine standardisierte Lösung schneller benötigte, hat die Wi-Fi Alliance im ersten Quartal 2003 als eigenen Sicherheitsstandard Wi-Fi Protected Access (WPA) veröffentlicht (siehe [WPA04]). Seit Ende August 2003 ist WPA Bestandteil der Wi-Fi-Zertifizierung, und eine stetig wachsende Anzahl von Produkten unterstützt inzwischen WPA. WPA ist zwar aufwärtskompatibel zu IEEE 802.11i, enthält aber zunächst nur eine gewisse Auswahl von Elementen des IEEE-Standards. Kapitel 6.2 stellt WPA und den Zusammenhang mit IEEE 802.11i vor.

An dieser Stelle sei nochmals auf das Problem der unsicheren Standardkonfigurationen (siehe auch Kapitel 3), mit denen WLAN-Geräte oft ausgeliefert werden, hingewiesen. WPA und IEEE 802.11i sind meist nicht als Voreinstellung konfiguriert.

## 6.1 Konzepte in IEEE 802.11i

Folgende Anforderungen standen bei der Spezifikation von IEEE 802.11i im Vordergrund:

- Datenpakete müssen authentifiziert sein und nicht nur verschlüsselt.
- Ein Schlüssel wird nur für ein Paket benutzt.
- Pakete müssen eine verschlüsselte Sequenznummer tragen.
- Kommunikationspartner müssen sich gegenseitig authentifizieren.

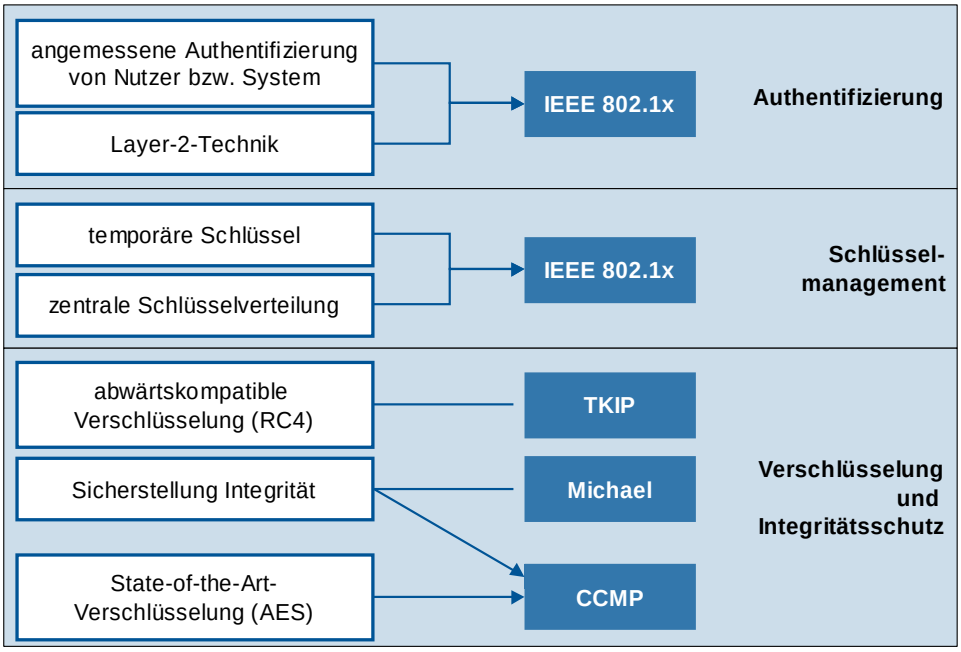



Abbildung 13: Bausteine in IEEE 802.11i im Überblick

Ein Kernproblem der verbesserten Sicherheitslösung stellt die Abwärtskompatibilität dar. Soll es möglich sein, ein bestehendes WLAN-System gemäß dem Standard von 1999 (siehe Kapitel 3) nachträglich mit dem neuen Standard aufzurüsten, darf höchstens ein Update der Firmware erfolgen. Die Konsequenz wäre in diesem Fall, dass weiterhin RC4 genutzt wird.

Es wurden also zwei Verschlüsselungsverfahren festgelegt: Das Temporary Key Integrity Protocol (TKIP) basiert als abwärtskompatible Lösung nach wie vor auf WEP, es beseitigt jedoch die wesentlichsten Schwächen. Für TKIP ist in IEEE 802.11i das Problem der mangelhaften Integritätsprüfung in WEP durch den Einsatz eines zusätzlichen Verfahrens (als Michael bezeichnet) gelöst worden. TKIP zusammen mit Michael ist als temporäre Lösung zu verstehen. Das zweite Verfahren (CCMP[11]), welches auf einer modernen Verschlüsselungsmethode basiert und langfristig tragbar ist, erfordert neue Hardware.

Für die Authentifizierung und das Schlüsselmanagement wurde in IEEE 802.11i auf einen anderen Standard zurückgegriffen, nämlich auf IEEE 802.1X (siehe [IEEE04b]). Ein WLAN, das ausschließlich Assoziationen erlaubt, deren Kommunikation durch die in IEEE 802.11i spezifizierten neuen Sicherheitsmechanismen geschützt wird, bezeichnet der Standard IEEE 802.11i als Robust Security Network (RSN). Erkennbar ist ein RSN dadurch, dass im Beacon Frame der potentielle Einsatz von WEP nicht angezeigt wird, sondern lediglich die im Folgenden vorgestellten Methoden TKIP und CCMP.

Abbildung 13 zeigt die Bausteine, aus denen IEEE 802.11i zusammengesetzt ist, im Überblick. Diese Bausteine werden in den Kapiteln 6.1.1 und 6.1.2 kurz vorgestellt. Kapitel 6.1.3 diskutiert den Einfluss höherwertiger Sicherheitsmechanismen auf die Leistung bei einem Handover.

### 6.1.1 Verschlüsselung und Integritätsschutz

Durch TKIP werden primär die bisher bekannten Schwächen bei der Auswahl und Erzeugung der Startwerte für RC4 bereinigt. Wesentliche Elemente in TKIP sind: Pro Paket wird ein neuer Schlüssel durch Anwendung einer Hash-Funktion auf einem geheimen symmetrischen Sitzungsschlüssel, dem IV und einer Paketsequenznummer erzeugt, um das Problem des bisher statischen WEP-Schlüssels zu umgehen. Der Sitzungsschlüssel wird seinerseits aus einem gemeinsamen Schlüssel erzeugt, dem sogenannten Pairwise Master Key (PMK). Abbildung 14 zeigt das Verfahren im Überblick. Die Mechanismen zur Schlüsselverwaltung und –erzeugung werden im folgenden Kapitel 6.1.2 beschrieben.

Ein zusätzlicher Message Integrity Check (MIC, als „Michael“ bezeichnet), der neben den Nutzdaten auch die Quell- und Zieladressen des MAC-Pakets berücksichtigt und verschlüsselt übertragen wird, sorgt für die Fälschungssicherheit. Die Verwendung von Michael in TKIP ist bereits kritisiert worden. Der Standard fordert eine Beschränkung auf weniger als zwei MIC-Fehler pro Minute. Sobald Michael mehr als eine Verletzung der Integrität feststellt, werden als Konsequenz für eine Minute alle Übertragungsversuche der zugehörigen MAC-Adresse ignoriert und eine Neuaushandlung der Schlüssel ist anschließend erforderlich. Auf diese Weise sollen die weiteren Versuche einer Paketfälschung in Grenzen gehalten werden. Wichtig ist in diesem Zusammenhang noch die Feststellung, dass zunächst der CRC ausgewertet wird und der Wert des IV passen muss, bevor Michael aktiv wird. So kann weitgehend ausgeschlossen werden, dass es sich um einen zufälligen Übertragungsfehler handelt, sondern es muss von einer bewussten Manipulation, also von einem Angriff ausgegangen werden.

Dieser Mechanismus eignet sich allerdings für einen Angriff vom Typ Denial of Service (DoS), indem ein Paket der angegriffenen Station aufgezeichnet wird, der Inhalt geeignet manipuliert wird und das Paket anschließend wieder auf das WLAN an den originalen Empfänger übertragen wird. Dieser wird eine Integritätsverletzung feststellen und die Quelladresse zeitweise sperren.

[11] CCMP ist eine Abkürzung für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Dieses Verfahren wird weiter unten genauer beschrieben.

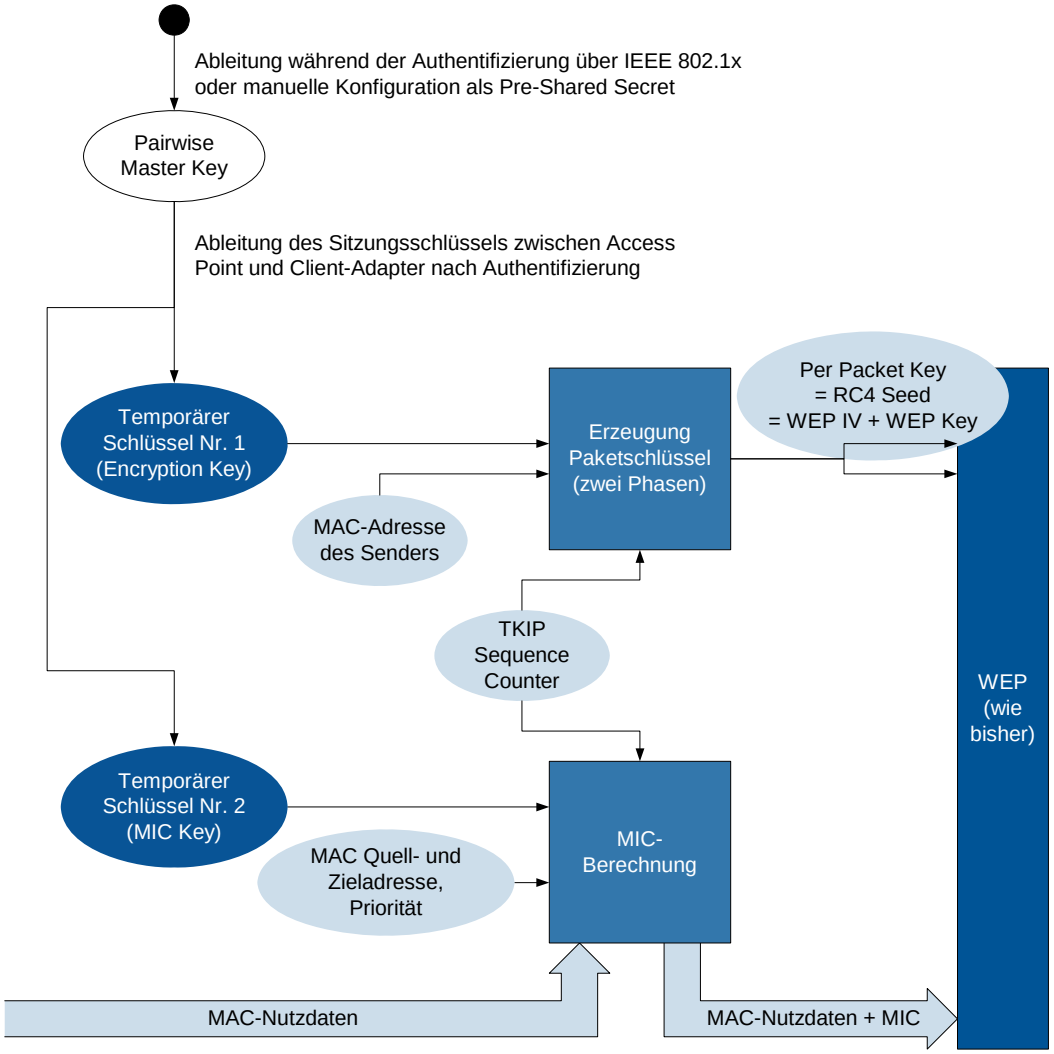



Abbildung 14: Aufbau von TKIP (vereinfacht)

In WLAN können Angriffe vom Typ DoS nie vermieden werden, denn ein Störsignal kann einfach, effektiv und jederzeit erzeugt werden[12].

Daher sollte die Schwäche der Verwendung von Michael in TKIP durch die zeitweise Sperrung einer Station, die eine Integritätsverletzung verursacht hat, nicht überbewertet werden. Wichtig ist dagegen,

12 Es kann zwischen physikalischen und logischen Störsignalen unterschieden werden.

Bei einem physikalischen Störsignal wird auf dem physikalischen Übertragungskanal, auf dem eine Station bzw. ein Access Point operiert, bewusst eine Interferenz durch ein Fremdystem (z. B. Bluetooth bei einem WLAN bei 2,4 GHz) oder durch ein anderes WLAN-System ausgestrahlt. Am Empfänger einer Station des so gestörten WLAN überlagern sich Nutz- und Störsignal. Ist die Feldstärke des Störsignals genügend groß, können so Paketverluste provoziert bzw. der Kanalzugriff künstlich in die Länge gezogen werden.

Bei einem logischen Störsignal werden bewusst Pakete auf MAC-Ebene induziert. Hierbei handelt es sich typischerweise um ungesicherte Managementpakete, die insbesondere nicht verschlüsselt und nicht hinsichtlich ihrer Authentizität und Integrität geprüft werden. Das Ergebnis ist oft eine Denial-of-Service-Attacke, die beispielsweise eine Deassoziierung einer Station bewirkt und die auf diese Weise ihre Verbindung zum Netz verliert. Bedauerlicherweise beseitigt auch IEEE 802.11i diese Schwäche nicht.

dass eine Feststellung der Verletzung der Integrität durch Michael als Angriffsversuch gewertet wird, der sofort mit hoher Wichtigkeit an das Netzmanagement zu berichten ist.

Die Entschlüsselung funktioniert prinzipiell ähnlich unter Umkehrung der Operationsrichtungen. Damit der Empfänger auch den Paketschlüssel, der zur Verschlüsselung beim Sender verwendet wurde, zur Entschlüsselung erzeugen kann, überträgt TKIP einen weiteren Initialisierungsvektor der Länge 32 Bit. Es werden also zwei Initialisierungsvektoren pro Paket übertragen: einer mit 24 Bit für WEP (mit einer effektiven Länge von 16 Bit) und einer mit 32 Bit für TKIP, in Summe also 48 Bit. Die effektive Schlüssellänge liegt nach wie vor bei 104 Bit, da als Basis WEP verwendet wird. Abbildung 15 zeigt den Aufbau eines TKIP-Pakets. Im Vergleich zu WEP werden 12 Byte pro Paket zusätzlich für TKIP übertragen und damit insgesamt pro Paket 20 Byte für die Absicherung der Übertragung.

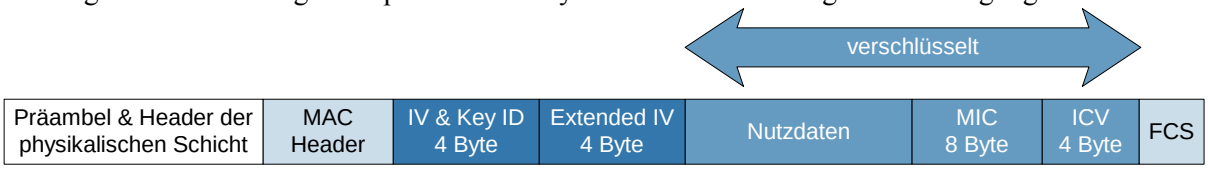



Abbildung 15: Format eines TKIP-Pakets

TKIP wird als temporäre Lösung zur Unterstützung bereits bestehender WLAN verstanden. Da TKIP auf der bestehenden „WEP-Hardware“ aufsetzt, müssen wesentliche Funktionen in Software realisiert werden. Daher zeigt ein WLAN mit TKIP in der Praxis einen etwas geringeren Durchsatz als ein WLAN mit WEP. Hier muss man mit einem Verlust von 5 % bis 10 % rechnen.

Als langfristige Lösung sieht 802.11i den Einsatz des Advanced Encryption Standard (AES, siehe [DaRi99]) in einem speziellen Modus CCMP vor. CCMP steht für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Hierbei wird nicht direkt der Klartext mit AES verschlüsselt, sondern der Wert eines Zählers. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Zähler, wie in Abbildung 16 illustriert. Außerdem wird die Methode Cipher Block Chaining (CBC) zur Integritätssicherung der Daten verwendet. Zur Schlüsselverwaltung und -verteilung wird wieder IEEE 802.1X vorausgesetzt. Die in IEEE 802.11i verwendete Schlüssellänge beträgt 128 Bit.

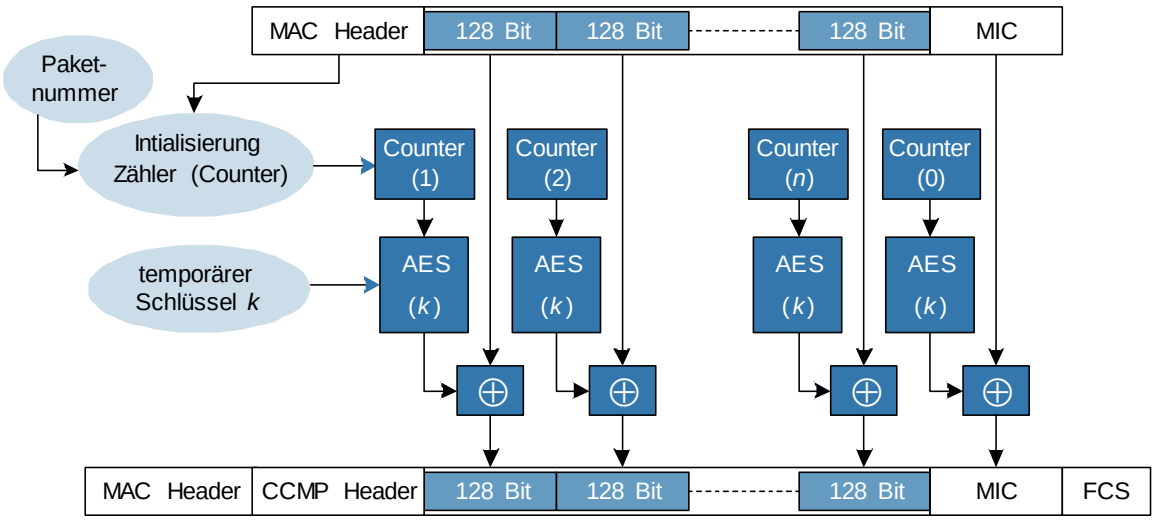



Abbildung 16: Verwendung von AES in IEEE 802.11i (vereinfacht)

Für CCMP werden pro Paket 16 Byte Daten übertragen, davon 8 Byte für die Integritätsprüfung, wie in Abbildung 17 gezeigt. Das Format ist (bis auf die nicht mehr notwendigen WEP-Daten) analog zu TKIP aufgebaut.

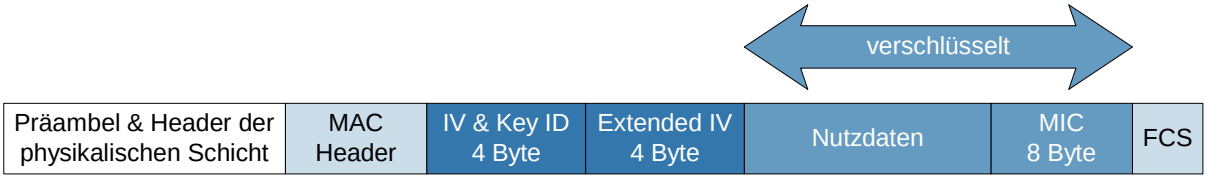



Abbildung 17: Format eines CCMP-Pakets

### 6.1.2 Erzeugung der Schlüssel

TKIP und CCMP sind symmetrische Verfahren, und die Kommunikationspartner müssen daher einen gemeinsamen Schlüssel konfiguriert haben. Dieser Schlüssel wird, wie bereits in Abbildung 14 gezeigt, als Pairwise Master Key (PMK) bezeichnet.

Es stellt sich nun zunächst die Frage, wie der Pairwise Master Key (PMK) auf die beteiligten Stationen gelangt.

Hierzu sind zwei Möglichkeiten vorgesehen:

- **Statische Schlüssel**: Der PMK kann (analog zu WEP) manuell als ein statischer Schlüssel, als Pre-Shared Key (PSK) bezeichnet, auf Access Points und Clients konfiguriert werden. Es besteht meist die Möglichkeit den gemeinsamen geheimen Schlüssel auch über Passwörter festzulegen. Diese Passwörter werden über Hash-Funktionen in den PMK umgerechnet. Hat ein solcher PSK eine zu geringe Komplexität (im Sinne der Länge des Schlüssels und der Zufälligkeit der Zeichen), ist er anfällig gegenüber Wörterbuch- bzw. Dictionary-Attacken. Daher sollten diese Passwörter eine hohe Komplexität und eine Länge von mindestens 20 Stellen besitzen (siehe [IEEE04a]). Ab einer gewissen Größe eines WLAN ist das Ausrollen eines neuen Schlüssels mit erheblichen Problemen verbunden.
- **Dynamische Schlüssel**: Eine höhere Sicherheit kann ein Mechanismus zur Schlüsselverwaltung und -verteilung bieten, der dafür sorgt, dass regelmäßig und insbesondere nach einer erfolgreichen Authentifizierung des WLAN-Clients am Access Point ein neuer Schlüssel (PMK) bereitgestellt wird. Für diese Schlüsselverwaltung und -verteilung greift IEEE 802.11i auf den Standard IEEE 802.1X zurück. Dieser Standard ist ursprünglich zur portbasierten Netzzugangskontrolle in kabelbasierten Netzen entworfen worden. Grundsätzliche Idee in IEEE 802.1X ist, dass die Freischaltung eines Netzports erst dann erfolgt, wenn der Nutzer sich erfolgreich dem Netz gegenüber authentifiziert hat. Die Authentifizierung erfolgt also auf Schicht 2. Damit so etwas überhaupt funktioniert, spezifiziert IEEE 802.1X eine Schnittstelle zwischen Client, Netzelement und einem Authentifizierungssystem. Diese Schnittstelle basiert auf dem Extensible Authentication Protocol (EAP) und einer Adaptierung dieses Protokolls für die Übertragung auf Layer 2 in LAN (als EAP over LAN, EAPOL bezeichnet). Hand in Hand geht damit die Festlegung einer Funktion zur Schlüsselverwaltung und -verteilung.

In 802.11i wird zur Authentifizierung von Client und Access Point auf die Authentifizierung gemäß IEEE 802.1X verwiesen, welche damit die bisherige Authentifizierung in IEEE 802.11 ersetzt. Die Frage der Authentifizierung für den WLAN-Zugang wird von der Standardisierung der WLAN-Übertragung entkoppelt.

IEEE 802.1X und EAP werden im Kapitel 7 im Detail beschrieben.

Für die Verschlüsselung und Integritätsprüfung wird der PMK nicht direkt verwendet, sondern es werden aus dem PMK temporäre Schlüssel für die Sitzung aus dem PMK abgeleitet. Für TKIP funktioniert dies folgendermaßen:

- In einem ersten Schritt wird aus dem 256 Bit langem PMK ein Pairwise Transient Key (PTK) der Länge 512 Bit durch Anwendung eines speziellen Zufallszahlengenerators (Pseudo Random Function, im Standard mit PRF-X bezeichnet) ermittelt. Die Parameter für die Funktion PRF-X sind neben dem PMK und einer im Standard festgelegten String-Konstante die MAC-Adressen von Access Point bzw. Authenticator und Client bzw. Supplicant sowie die im Rahmen des EAPOL Key Exchange ausgetauschten Zufallszahlen „ANonce“ und „SNonce“ (siehe Kapitel 7.1 und hier insbesondere Abbildung 25). Diese Operation wird auf beiden Seiten (Access Point und Client) identisch durchgeführt. Das Ergebnis ist ein gemeinsamer PTK, wie Abbildung 18 illustriert.
- Der PTK wird in vier Schlüssel der Länge 128 Bit aufgeteilt. Die vom PTK abgeleiteten Schlüssel MK und EK werden für die nachfolgende verschlüsselte Übermittlung (hier nicht dargestellt) eines Group Transient Key (GTK) zum Client benutzt. Die Schlüssel TK1 und TK2 werden in TKIP als Encryption Key und MIC Key zur Verschlüsselung und Integritätssicherung der „normalen“ Unicast-Kommunikation verwendet (siehe Abbildung 14). Der verschlüsselt übermittelte GTK ist wiederum in eine Group Key Hierarchy einzuordnen (Abbildung 19). Die davon abgeleiteten Group TKs sind die Basis für die Verschlüsselung von Multicast- und Broadcast-Nachrichten.

Bei der Verwendung von CCMP wird kein zusätzlicher Schlüssel für die Erzeugung des MIC benötigt. Die Längen der Transient Keys verkürzen sich entsprechend um 128 Bit, wie in Abbildung 20 gezeigt.

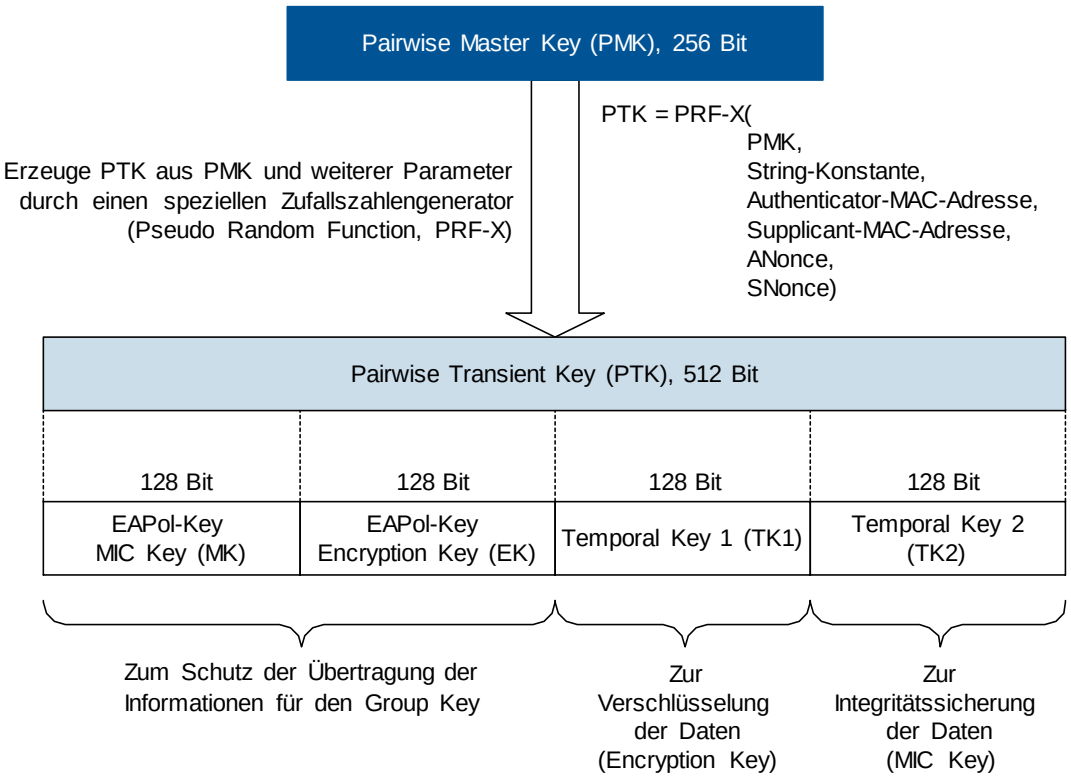



Abbildung 18: Pairwise Key Hierarchy für TKIP

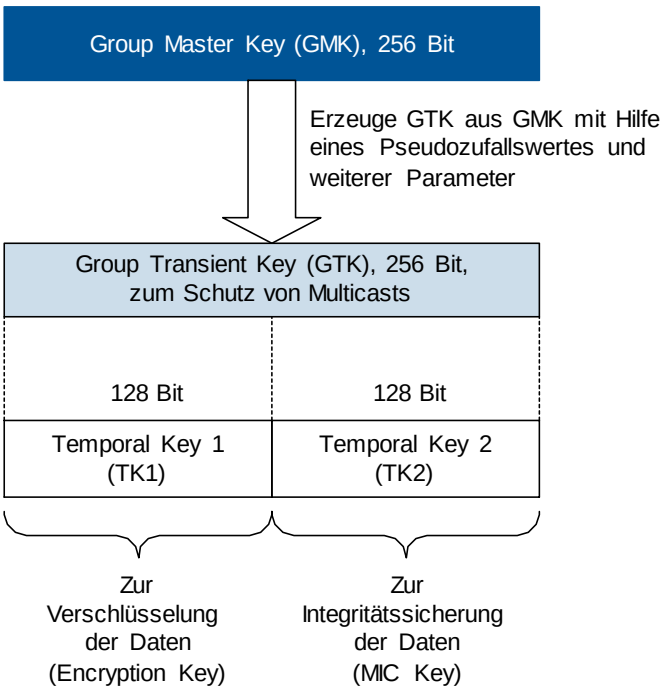



Abbildung 19: Group Key Hierarchy für TKIP

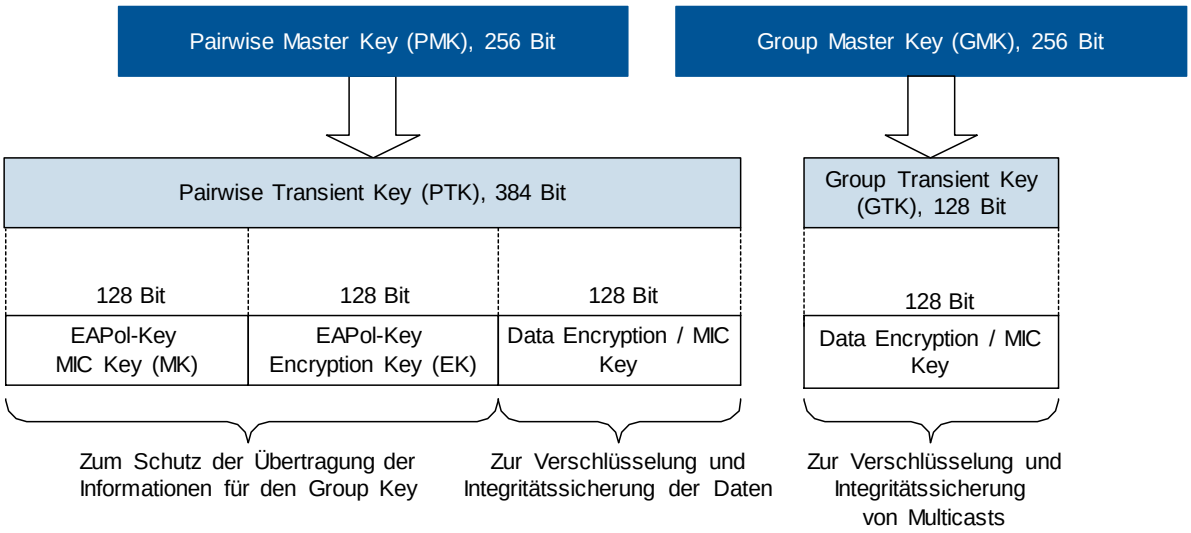



Abbildung 20: Pairwise Key Hierarchy (links) und Group Key Hierarchy (rechts) für CCMP

### 6.1.3 Arbeiten mit Pre-Shared Keys

Sofern auf den Einsatz einer Authentifizierung nach IEEE 802.1X verzichtet wird, ist der Pairwise Master Key (PMK) in Clients und Access Points manuell als Pre-Shared Key einzustellen. Der PMK weist, wie in Abbildung 18 dargestellt, eine Länge von 256 Bit auf. Damit einem Anwender die Einrichtung eines Schlüssel erleichtert wird, schlägt der Standard IEEE 802.11i ein spezielles Verfahren vor, das den PMK aus einer beliebigen Zeichenkette generiert. Diese Zeichenkette wird der Anwender

aus Worten seiner Sprache sowie Ziffern und Zeichen erzeugen und eingeben. Üblicherweise wird er einen Satz („Passphrase“) formulieren, der leicht zu merken ist.

Gemäß IEEE 802.11i wird der PMK über eine Funktion[13] erzeugt, die folgende Parameter als Eingangwerte erhält:

- Passphrase mit 8 bis 63 Zeichen; 64 Zeichen dürfen wegen einer möglichen Verwechselung mit einem direkt als Hexadezimalzahlen eingegebenen PMK nicht verwendet werden
- Service Set Identifier (SSID)
- Länge des SSID
- Zahl der Durchläufe
- Schlüssellänge

Die Funktion wird in [RSA99] beschrieben. Es handelt sich um einen Pseudozufallszahlen-Generator, der insgesamt 4096 mal durchlaufen wird.

Wegen des beschränkten Wertebereichs weist eine typische Passphrase nur ca. 2,5 Bits „Sicherheit“ pro Zeichen aus. Die genannte Funktion erzeugt einen PMK, dessen Sicherheits-Äquivalent 2,5-mal die Zahl der Zeichen in der Passphrase zuzüglich 12 Bit beträgt. Die Autoren von IEEE 802.11i weisen darauf hin, dass man erst bei einer Passphrase von mehr als 20 Zeichen eine gewisse Sicherheit gegenüber Dictionary-Attacken erwarten kann.

### 6.1.4 Handover

Unabhängig, ob TKIP oder CCMP eingesetzt wird, durch die Möglichkeit einer Authentifizierung mit IEEE 802.1X und durch die Verwendung von verschlüsselten Sequenznummern wird eine kryptografische Session zwischen Client und Access Point etabliert. Das hat Auswirkungen auf die Mobilität, insbesondere beim Handover zwischen zwei Access Points. Im IEEE 802.11-Standard von 1999 erfolgt einfach eine neue Assoziation und WEP-Authentifizierung am neuen Access Point. Das geht in der Regel schnell genug, ohne dass höhere Protokolle etwas davon spüren und ohne dass eine Kommunikation zwischen den Access Points erforderlich ist. Mit 802.11i bzw. allgemein mit IEEE 802.1X ist der Aufwand ungleich höher. Bei einem Handover besteht hier grundsätzlich die Gefahr, dass es für die Anwendung bei einem Zellwechsel zu einem Leistungsengpass und damit zu einem Verfügbarkeitsproblem kommt.

IEEE 802.11i sieht daher für eine Anmeldung an einem Access Point drei verschiedene Varianten vor:

- **Vollständige Authentifizierung**: Wenn ein Client sich an einem Access Point anmeldet, erfolgt ein kompletter Aufbau der Security Association. Wird IEEE 802.1X verwendet, bedeutet dies eine vollständige Authentifizierung, die Übertragung des PMK über EAP zum Client und das Erzeugen eines PTK über die in Kapitel 7.1 in Abbildung 25 gezeigte Sequenz (einem sogenannten 4-Way-Handshake).
- **Caching**: Access Point und Client merken sich einen PMK und speichern ihn auch dann noch, wenn der Client bereits die Funkzelle verlassen hat. An einem neuen Access Point wird weiterhin eine komplette Authentifizierung durchgeführt. Kehrt der Client jedoch in eine bereits besuchte Zelle zurück, liegt dort der PMK bereits vor, und die Authentifizierung muss nicht mehr durchgeführt werden. Lediglich ein neuer PTK muss über den bereits erwähnten Mechanismus erzeugt werden (Abbildung 25), was mit einem deutlich geringeren Aufwand verbunden ist.
- **Pre-Authentication**: Hier wird einem Client gestattet, simultan zu mehreren Access Points eine Assoziation aufzubauen. Die Idee ist dabei, dass eine Authentifizierung an einem potentiellen neuen Access Point „auf Verdacht“ durchgeführt werden kann, bevor der Client den Datentransfer am alten Access Point abbricht und auf einen neuen Access Point umschaltet. Der Client führt also

13 *PSK* = PBKDF2(*PassPhrase*, *ssid*, *ssidLength*, 4096, 256)

die Authentifizierung vor (genauer gesagt sogar unabhängig) von dem eigentlichen Handover durch. Hierzu muss es gestattet sein, dass ein Client an mehreren Access Points assoziiert ist, was streng genommen im Widerspruch zum alten Standard IEEE 802.11 von 1999 steht. Solange ein Client tatsächlich zu einem Zeitpunkt nur über einen Access Point Daten überträgt, stellt dies aber kein Problem dar.

Ursprünglich wurde in der Arbeitsgruppe zu IEEE 802.11i diskutiert, den Standard IEEE 802.11F für die Verbesserung der Leistung bei einem Handover zu nutzen. Letztendlich wurden geeignete Informationselemente aber weder in IEEE 802.11i noch in IEEE 802.11F spezifiziert. Die Verwendung eines IAPP für die Verbesserung des Verhaltens bei einem Handover (selbst wenn es gemäß IEEE 802.11F geschieht) stellt daher einen herstellerspezifischen Mechanismus dar, der in verschiedenen Varianten in WLAN-Produkten anzutreffen ist.

Die Erweiterung IEEE 802.11i hat Auswirkungen auf die Interoperabilität mit Geräten nach dem alten Standard IEEE 802.11 in der Auflage von 1999. Ein Access Point nach IEEE 802.11i darf durchaus gleichzeitig mit Geräten nach dem alten Standard und mit Geräten nach IEEE 802.11i kommunizieren. Dies gilt jedoch nicht für Clients. Hier gilt entweder IEEE 802.11i oder WEP, jedoch nicht beides gleichzeitig. Zusätzlich ist ein Mechanismus in IEEE 802.11i enthalten, der eine Client-Konfiguration vorsieht, welche ausschließlich die erweiterten Sicherheitsmechanismen erlaubt und die Kommunikation mit einem Access Point nach dem alten Standard IEEE 802.11 explizit verbietet. Dies erlaubt (scheinbar, siehe Kapitel 8.3) einerseits die sanfte Migration zu den erweiterten bzw. neuen Sicherheitsmechanismen und andererseits die Umsetzung strenger Sicherheitsrichtlinien.

IEEE 802.11i führt die Absicherung von WLAN ausschließlich auf der Luftschnittstelle und damit auf Layer 2 aus. Während der Standardisierungsarbeit wurde die Alternative einer Sicherheit auf Layer 3 (sprich: IP-VPN) intensiv diskutiert, jedoch letztendlich verworfen. Obwohl es auf den ersten Blick sehr attraktiv erscheint, das Thema Sicherheit von WLAN einfach aus dem IEEE-Standard zu entfernen und das Problem den höheren Ebenen zu überlassen, wurde eine andere Entscheidung getroffen. Ein wesentlicher Punkt war dabei das Problem der Leistung und der Skalierbarkeit. Der in IEEE 802.11i spezifizierte Ansatz erfordert lediglich die Verschlüsselung zwischen einem Access Point und den assoziierten Clients. Das in Kapitel 5.3 beschriebene Redundanz- und Durchsatzproblem in größeren WLAN kann hier nicht auftreten, und das System skaliert sich en passant.

## 6.2 Wi-Fi Protected Access

Ende Oktober 2002 hat die Wi-Fi Alliance bekannt gegeben, unter der Bezeichnung Wi-Fi Protected Access (WPA) einen eigenen Standard herauszugeben, der auf IEEE 802.11i basieren und aufwärtskompatibel sein wird. WPA wurde im ersten Quartal 2003 veröffentlicht (siehe [WPA04]).

WPA übernimmt Teile von IEEE 802.11i (siehe Abbildung 21) und konkretisiert Freiheitsgrade in IEEE 802.11i für den praktischen Einsatz. Dies ist zwingend notwendig, um eine Interoperabilität zwischen Herstellern zu ermöglichen. WPA ist seit Ende August 2003 Bestandteil der Wi-Fi-Interoperabilitätstests.

Von IEEE 802.11i hat WPA die für TKIP spezifizierten Erweiterungen bezüglich Initialisierungsvektor, Re-Keying und den Message Integrity Check übernommen. AES wird (noch) nicht berücksichtigt.

WPA unterscheidet zwischen größeren WLAN-Installationen im Unternehmensbereich und kleineren WLAN im privaten und SOHO-Bereich (Small Office / Home Office):

- **WPA-Enterprise**: Für größere WLAN kann die Authentifizierung und Schlüsselverwaltung mit IEEE 802.1X über EAP und RADIUS geschehen.
- **WPA-Personal**: Für kleinere WLAN bleibt es zwar bei Pre-Shared Keys (**WPA-PSK**), die Sicherheit ist jedoch durch TKIP im Vergleich zu WEP auf einem deutlich höheren Niveau.

Die Funktion für ein schnelles und trotzdem sicheres Handover zwischen Access Points wird in WPA zunächst nicht berücksichtigt.

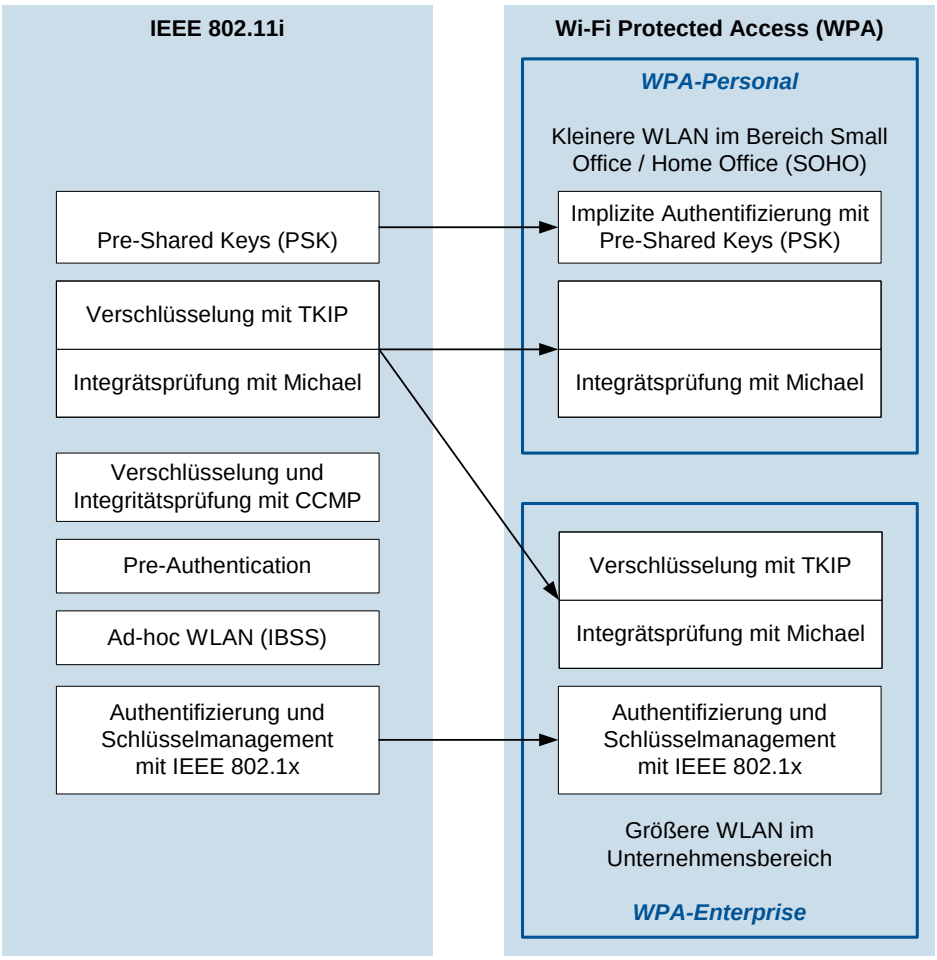



Abbildung 21: Zusammenhang zwischen IEEE 802.11i und WPA

Die erwähnte Handover-Problematik ist für solche WLAN-Anwendungen von Bedeutung, die eine flächendeckende Mobilität ohne nennenswerte Qualitätseinbrüche erfordern. Da WPA zunächst Pre-Authentication ausklammert, muss die Handover-Funktion bei aktiviertem WPA im Einzelfall hinsichtlich der Leistung verifiziert werden.

Es wird generell empfohlen, die geforderte Leistung (im Sinne der Dauer eines Handovers und einer maximalen Paketverlustrate dabei) als Anforderung in WLAN-Planungen und bei der Produktauswahl zu berücksichtigen. Diese Leistung muss auch bei Anwendung von WPA gefordert werden.

Die in WPA umgesetzten Maßnahmen (bzw. die entsprechenden Maßnahmen in IEEE P802.11i) wurden von der internationalen Kryptoanalytiker-Gemeinde genau geprüft. Dabei ist man allgemein zu dem Schluss gekommen, dass unter der Voraussetzung einer geeigneten Konfiguration bereits WPA die soweit bekannten Sicherheitslücken von WEP schließt.

Bei der Verwendung von passwortbasierten Authentifizierungsmethoden (siehe hierzu auch Kapitel 7) ist generell darauf zu achten, dass eine geeignete Passwortkomplexität zugesichert ist. Dies gilt insbesondere für WPA mit Pre-Shared Keys. Zu vermeiden sind durch zu einfache „Passphrases“ generierte und zu kurze Schlüssel (Mindestlänge 20 Zeichen). Für die Authentifizierung über IEEE 802.1X ist weiterhin die Wahl einer angemessen sicheren EAP-Authentifizerungsmethode für die Gesamtsicherheit des WLAN relevant.

Inzwischen hat die Wi-Fi Alliance bereits die Folgeversion von WPA, als WPA2 bezeichnet und verabschiedet. Seit Sommer 2004 werden WLAN-Geräte nach WPA2 zertifiziert. Bis September 2006 ist

die Zertifizierung nach WPA2 noch optional. WPA2 basiert auf IEEE 802.11i und deckt alle zwingenden Anforderungen von IEEE 802.11i ab. Dies beinhaltet insbesondere die Übernahme des spezifischen AES-Modus (CCMP).

Mit AES ist in WPA2 im Vergleich zu RC4 in WPA ein modernes Verschlüsselungsverfahren zu Grunde gelegt worden, das zudem standardisiert ist und durch seine Offenlegung bereits eine Vielzahl von Prüfungen erfolgreich bestanden hat. Der verwendete Modus CCMP gestattet gleichermaßen eine Verschlüsselung auf dem Stand der Technik als auch eine entsprechende Integritätsprüfung. Insbesondere gab es bei der Spezifikation von CCMP für den WLAN-Einsatz keine Rahmenbedingungen, wie die Abwärtskompatibilität zu WEP, welche das Design verkomplizieren und es damit potentiell anfälliger gegenüber Implementierungsfehlern und Angriffen machen. Es muss weiterhin bedacht werden, dass bei TKIP im Vergleich zu CCMP ein geringerer Durchsatz zu erwarten ist. Daher ist WPA2 generell WPA vorzuziehen.

## 6.3 Bewertung und Zusammenfassung

Mit IEEE 802.11i bzw. WPA und WPA2 stehen Mittel zur Verfügung, um ein WLAN auf der Luftschnittstelle adäquat abzusichern. Authentifizierung und Schlüsselmanagement geschehen dabei entweder über IEEE 802.1X oder über Pre-Shared Keys. Statisch konfigurierte Pre-Shared Keys sind nur für sehr kleine WLAN-Installationen geeignet, da der Aufwand des Ausrollens eines neuen Schlüssels bei steigender WLAN-Größe sehr schnell nicht mehr sinnvoll beherrschbar ist. Bei der Authentifizierung über IEEE 802.1X muss beachtet werden, dass die gewählte EAP-Authentifizierungsmethode auch dem angestrebten Sicherheitsniveau angemessen ist und entsprechend konfiguriert wird.

WPA stellt eine Teilmenge von IEEE 802.11i dar, und die Wi-Fi Alliance zertifiziert seit Sommer 2003 WLAN-Produkte hinsichtlich WPA-Konformität und WPA-Interoperabilität. Eine dementsprechend große Anzahl von Produkten ist verfügbar. WPA nutzt TKIP zur Verschlüsselung und das Verfahren Michael zur Integritätsprüfung. TKIP basiert weiterhin auf WEP bzw. RC4, jedoch unter Umgehung deren bekannter Schwächen. IEEE 802.11i und WPA2 spezifizieren mit CCMP eine Verwendung von AES. Generell ist der Einsatz von AES zu bevorzugen, da AES ein Verfahren auf dem Stand der Technik darstellt und hier alle wesentlichen Elemente des Verschlüsselungsverfahrens in Hardware realisiert sind. Die Übertragung von Managementpaketen, die im Rahmen des MAC-Protokollmechanismen von IEEE 802.11 ausgetauscht werden, geschieht allerdings weiterhin ungesichert. Ein Missbrauch dieser Mechanismen wird durch IEEE 802.11i nicht verhindert, und die Bedrohung durch entsprechende DoS-Angriffe besteht weiterhin.

Tabelle 2 zeigt abschließend die Bewertung der Bausteine von IEEE 801.11i bzw. WPA und WPA2 im Überblick.

| Funktion | Verfahren | Bewertung | Kommentar |
|---|---|---|---|
| Authentifizierung | implizite Authentifizierung durch Pre-Shared Key | **0** | Diese Bewertung gilt, sofern der Schlüssel zufällig gewählt ist bzw. aus einem Passwort hoher Komplexität mit einer Länge von mindestens 20 Zeichen erzeugt wird. |
| | IEEE 802.1X | **++** | Schlüsselmanagement und diverse Authentifizierungs-methoden werden unterstützt. Die verwendete Authentifizierungsmethode muss dem zu erreichenden Sicherheitsniveau angemessen gewählt sein. Nur für diesen Fall gilt die angegebene Bewertung. |
| Verschlüsselung (WPA) | TKIP | **+** | TKIP basiert auf WEP. Es erfolgt für jedes Paket eine kryptographische Erzeugung eines Schlüssels.<br>Da TKIP in Software abläuft, kommt es zu Leistungs-einbußen. |
| Integritätsprüfung (WPA) | Michael | **0** | DoS-Angriff ist möglich.<br>Die Länge des MIC beträgt 64 Bit. |
| Verschlüsselung (WPA2) | CCMP | **++** | CCMP verwendet AES. AES erfordert entsprechende Hardware. Die verwendete Schlüssellänge beträgt 128 Bit. Nach dem Stand der Technik ist CCMP als sicheres Verfahren einzustufen. |
| Integritätsprüfung (WPA2) | CBC-MAC | **++** | Bestandteil von CCMP. Die Länge des MIC beträgt 64 Bit. |
| "++" = sehr gut, "+" = gut, "0" = akzeptabel, "-" = mangelhaft, "--" = ungenügend | | | |

Tabelle 2: Bewertung der Elemente von IEEE 802.11i bzw. WPA und WPA2

# 7 Authentifizierung und Schlüsselverwaltung im WLAN mit IEEE 802.1X

In IEEE 802.11i (nach langer Entwicklungszeit im Juni 2004 ratifiziert) wird für die Authentifizierung von Clients und Access Points auf die Authentifizierung gemäß IEEE 802.1X verwiesen, welche damit die bisherige als ausgesprochen unsicher einzustufende WEP-Authentifizierung in IEEE 802.11 ersetzt. In diesem Kapitel wird zunächst der Standard IEEE 802.1X und das für diesen Standard besonders wichtige Extensible Authentication Protocol (EAP) vorgestellt (Kapitel 7.1). Anschließend werden in Kapitel 7.2 die wesentlichen Authentifizierungsverfahren vorgestellt, die über IEEE 802.1X bzw. EAP genutzt werden können. Abschließend werden in Kapitel 7.3 die wesentlichen Aspekte der Integration der WLAN-Authentifizierung in die Benutzerverwaltung diskutiert.

## 7.1 IEEE 802.1X und das Extensible Authentication Protocol

Bei IEEE 802.1X handelt es sich um eine standardisierte Methode zur portbasierten Netzwerkzugangskontrolle (Port based Network Access Control) für LAN, die auf IEEE-802-Standards basieren. Hiermit sind konkret z. B. übliche Ethernet-LAN gemeint sowie auch ausdrücklich WLAN nach IEEE 802.11[14]. Zweck der im Standard beschriebenen Abläufe soll im Wesentlichen sein, Geräten nur dann einen Zugang zum Netzwerk zu gewähren, wenn eine Authentifizierung ergeben hat, dass es sich um bekannte Geräte bzw. Benutzer handelt, die auch wirklich Zugang erhalten sollen. Die Authentifizierung erfolgt also bereits auf Layer 2. Entworfen wurde IEEE 802.1X für Fälle, in denen man ohne großen Aufwand ein Gerät mit einem physikalischen Port des Netzwerkes verbinden kann (was sinngemäß besonders auf WLAN zutrifft), dies aber aus Sicherheitsgründen nicht dazu führen soll, dass das Netzwerk sofort genutzt werden darf. Ein weiterer wichtiger Aspekt bei der Nutzung von IEEE 802.1X für WLAN ist die Möglichkeit, mittels der darunter liegenden Methoden auch eine Schlüsselverwaltung und -verteilung zu erreichen.

### 7.1.1 Aufbau und Grundfunktionen

Damit eine Port-basierte Authentifizierung erfolgen kann, wird innerhalb des IEEE-Standards 802.1X das Extensible Authentication Protocol (EAP, RFC 2284, im Juni 2004 ersetzt durch RFC 3748, siehe [EAP04]) verwendet.

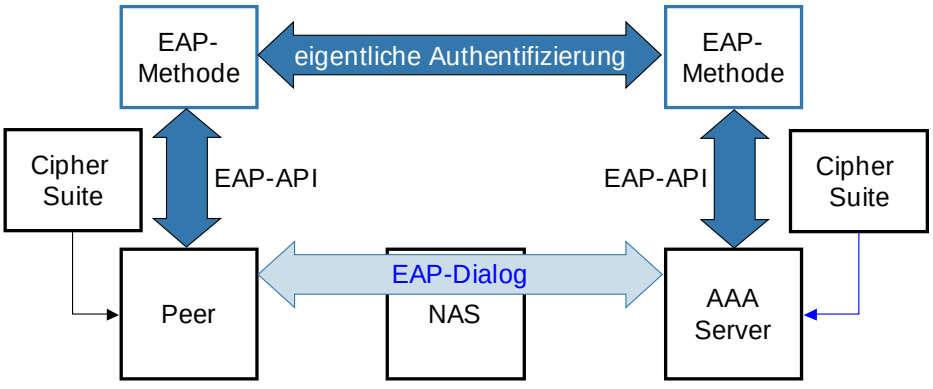



Abbildung 22: Grundkonzept von EAP

[14] Der Standard ist jedoch vom ursprünglichen Konzept her auf Punkt-zu-Punkt-Verbindungen ausgelegt; bei „Shared Media“ sind deren Besonderheiten zu beachten.

Hierbei handelt es sich nicht um ein eigenes Authentifizierungsverfahren, sondern vielmehr um ein Gerüst, in das konkrete Authentifizierungsverfahren, nämlich die EAP-Methoden oder EAP-Typen, eingebettet werden.

Abbildung 22 illustriert das zugrunde liegende Konzept. Ursprünglich für die PPP-Authentifizierung (Point-to-Point Protocol) geschaffen, also z. B. für eine RAS-Einwahl über Modem, wird EAP hier als EAPOL[15] (EAP over LAN) verwendet, um die Authentifizierungsverfahren auch direkt für Layer 2 ohne den Umweg über PPP verfügbar zu machen (Abbildung 23). Damit ist EAP zur Authentifizierung bereits anwendbar, bevor eine Kommunikation auf höherer Protokoll-Ebene stattfinden kann – und genau dies ist für eine portbasierte Zugangskontrolle gewünscht.

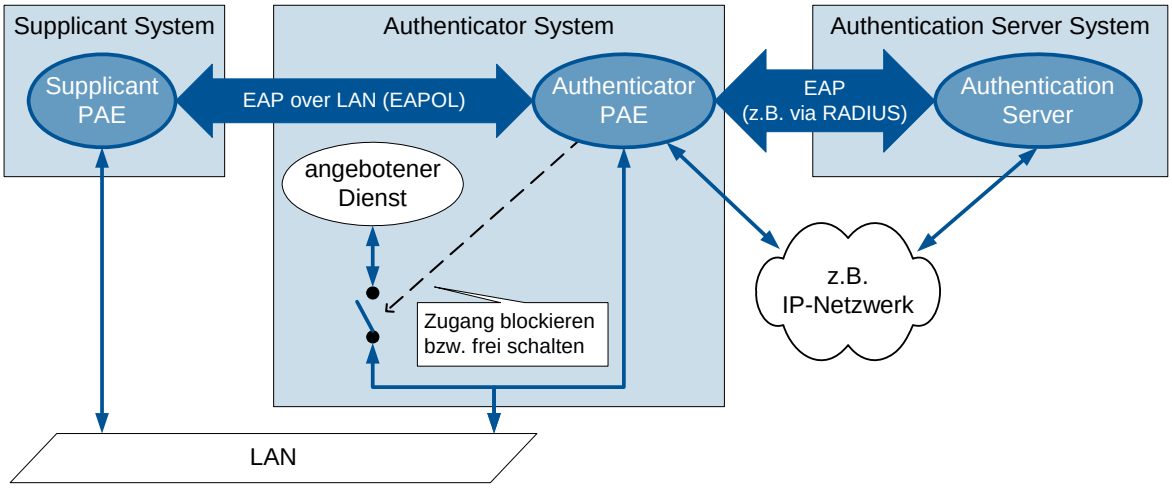



Abbildung 23: IEEE 802.1X und EAPOL

Ein Vorteil von EAP ist unter anderem seine Modularität, sodass es sich relativ leicht um weitere EAP-Methoden (die eigentlichen Authentifizierungsverfahren) erweitern lässt. Zudem ist es für das Gerät, das die Authentifizierung z. B. eines Clients erwünscht, nicht unbedingt erforderlich, die jeweilige Methode selbst zu beherrschen, sondern es kann die EAP-Pakete an den eigentlichen Authentifizierungsserver durchreichen.

Der Standard IEEE 802.1X sagt aber (wie auch IEEE 802.11i) nichts darüber aus, welche tatsächliche EAP-Methode genutzt werden muss[16]. Hier ist man zumindest aus Sicht von IEEE 802.1X frei in der Entscheidung. Durch unzureichende Regulierungsmechanismen ist es in der Vergangenheit zu einem regelrechten Wildwuchs von EAP-Methoden gekommen. Ungefähr 50 EAP-Methoden sind inzwischen bekannt. Für die Anwendung in WLAN sind jedoch nur einige Methoden relevant, die in Kapitel 7.2 näher erläutert werden.

Die zunächst zwei Instanzen (PAEs, Port Access Entities), die an einer Authentifizierung nach IEEE 802.1X teilnehmen, werden als Authenticator und Supplicant bezeichnet. Zusätzlich existiert noch die Rolle des Authentication Server (AS), der aber nicht unbedingt vom Authenticator verschieden sein muss. Da bei WLAN die Access Points häufig in nicht geschützten Bereichen positioniert sind, kommt dort die Speicherung von Benutzerdaten aus Sicherheitsgründen typischerweise nicht in Frage, da

15 EAPOL wird bei der Verwendung in WLAN auch gelegentlich als EAPoW (EAP over Wireless) bezeichnet.

16 Das IEEE hat 2003 gegenüber der IETF EAP Working Group den Wunsch geäußert, für RFC3748 eine EAP-Methode vorzuschreiben, welche die Anforderungen des IEEE für Wireless LANs erfüllt. Als weiterhin einzige vorgeschriebene EAP-Methode ist jedoch in RFC3748 EAP-MD5 genannt. Es wurde aber ein Verfahren beschrieben, mit dem man EAP-Methoden gegenüber spezifischen Anforderungen evaluieren kann und weiterhin werden „Security Considerations“ erörtert, die auch auf WLANs eingehen. Siehe hierzu [EAP05].

physischer Zugriff nahezu immer auch eine Kompromittierbarkeit mit sich bringt. Daher ist in solchen Fällen eine Trennung von Authenticator und AS empfehlenswert. Diese Rollenverteilung kann man mit der RADIUS-Idee vergleichen, bei der ebenfalls drei Parteien unterschieden werden, nämlich der RADIUS-Server (AAA-Server), ein NAS (Network Access Server) und ein NAS-Client (z. B. ein RAS-Client, der sich über VPN einwählt).

Der Supplicant bei 802.1X (z. B. der WLAN-Client, in der Terminologie von EAP auch als Peer bezeichnet) ist diejenige PAE, die den Dienst eines Authenticators (z. B. den eines virtuellen Ports auf einem Access Point) nutzen möchte. Hierzu bedient der Authenticator sich des Authentication Servers (AS), welcher die Überprüfung der vom Supplicant übermittelten Authentifizierungs-Informationen (Credentials) vornimmt (Authentication) und dem Authenticator mitteilt, ob der Zugang gewährt wird (Authorization).

Der Supplicant ist eine Software, die auf dem Client installiert wird. Hierbei sind prinzipiell drei Varianten zu unterscheiden:

- Variante 1: Der Supplicant ist Teil des Betriebssystems und arbeitet mit Kartentreibern beliebiger Hersteller zusammen, sofern die Kartentreiber WPA bzw. WPA2 unterstützen.
- Variante 2: Der Supplicant wird vom Hersteller der Karte mitgeliefert. Bei Installation des Kartentreibers wird der Supplicant – transparent für den Anwender – mit installiert.
- Variante 3: Der Supplicant wird von einem Dritthersteller bezogen und arbeitet mit Kartentreibern beliebiger Hersteller zusammen, sofern die Kartentreiber WPA bzw. WPA2 unterstützen.

Je nach Betriebssystem und verwendeter WLAN-Adapterkarte wird man sich für eine der Varianten entscheiden müssen, wobei die Varianten aus der Sicht der WLAN-Sicherheit gleichwertig sind. Erfahrungsgemäß unterscheiden sich die Varianten jedoch bezüglich der EAP-Methoden, die von ihnen bereitgestellt werden. Die Entscheidung für eine bestimmte EAP-Methode, die zur vorhandenen Umgebung, d. h. AS und evtl. Access Point passt, beeinflusst somit die Entscheidung für eine der genannten Varianten.

Der AS ist oft ein RADIUS-Server, mit dem der Authenticator über „EAP in RADIUS“ (in RADIUS gekapseltes EAP, RFC 3579, siehe [RADI03a]) kommuniziert. Diese Funktion wird inzwischen von diversen RADIUS-Servern unterschiedlicher Hersteller unterstützt. Abbildung 24 zeigt diesen Nachrichtenfluss im Überblick.

Die Verwendung von RADIUS ist jedoch keine Forderung von IEEE 802.1X; die Kommunikationswege zwischen Authenticator und AS werden nicht vorgeschrieben, RADIUS ist jedoch ausdrücklich als ein mögliches Verfahren genannt.

Im Falle von WPA ist gefordert, dass der Access Point RADIUS unterstützt.

Der Authentication Server bzw. RADIUS-Server ist der zentrale Punkt der Infrastruktur, bei dem im Rahmen von IEEE 802.1X letztendlich alle Anfragen zusammenlaufen. Bei Ausfall des Authentication Server ist keine neue Anmeldung am WLAN mehr möglich. Auch ein Handover bzw. Roaming oder eine periodische Re-Authentifizierung des Clients schlagen dann fehl, womit das System für Clients nach kurzer Zeit nicht mehr verfügbar ist Damit stellt das Authentication Server System einen potentiellen Single Point of Failure dar und muss bei entsprechend hoher Verfügbarkeitsanforderung redundant ausgelegt werden.

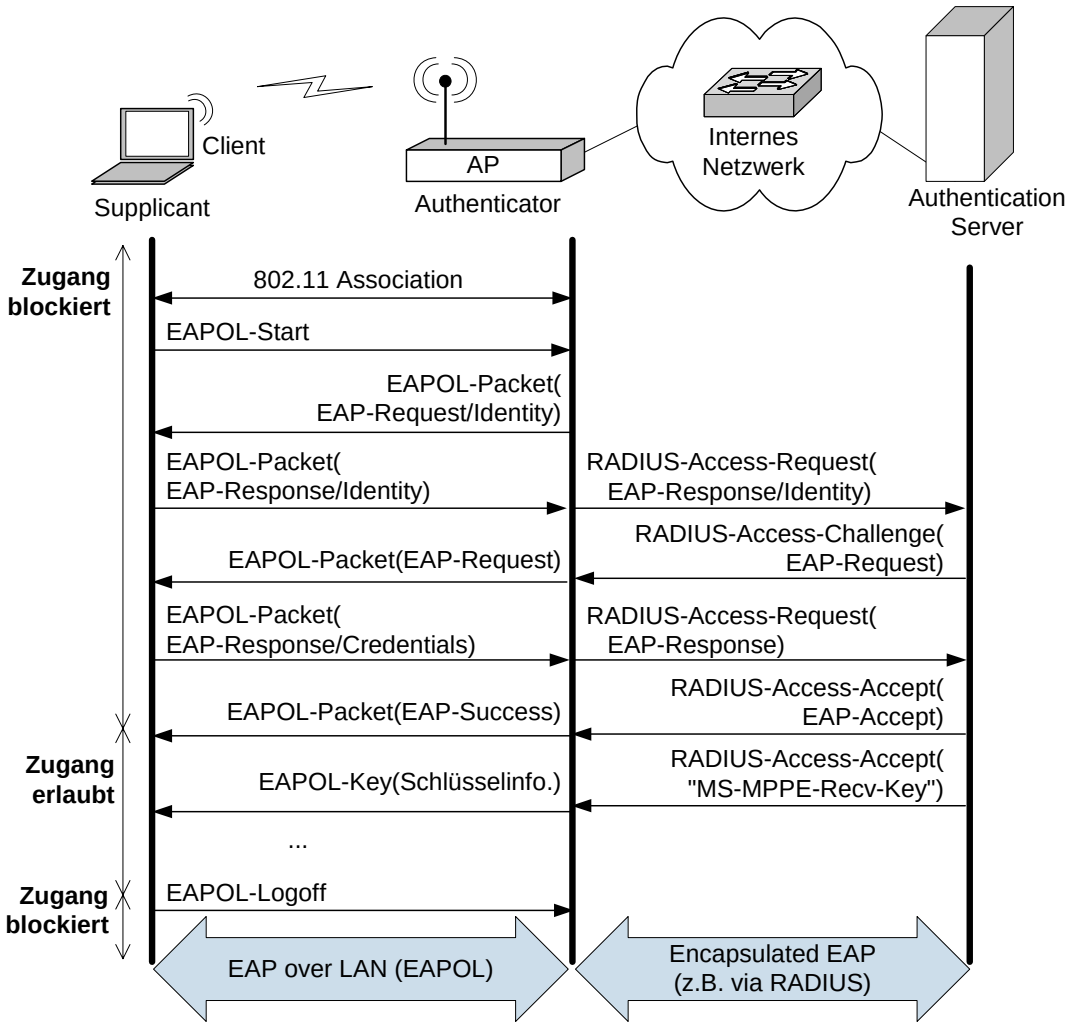



Abbildung 24: EAPOL-Kommunikation, vereinfacht

### 7.1.2 Schlüsselverwaltung und -verteilung

Das im Standard 802.1X beschriebene EAPOL ist dafür ausgelegt, geheime Schlüsselinformationen zum Supplicant (z. B. dem WLAN-Client) zu übertragen (GTK, Group Transient Key) bzw. mit diesem vereinbaren zu können (PTK, Pairwise Transient Key), sofern die benutzte EAP-Methode (siehe Kapitel 7.2) die hierzu erforderlichen Master-Schlüssel (Pairwise Master Key, PMK) liefert, wie in Abbildung 25 gezeigt.

Die Master-Schlüssel können aber auch als Pre-Shared Keys (PSKs) manuell (z. B. WPA-PSK) auf den Komponenten konfiguriert werden[17]. Bei Verwendung von PSKs wird die EAP-Authentifizierung nicht genutzt, EAPOL jedoch kommt für den Austausch von transienten Schlüsseln (PTK, GTK) weiterhin zum Einsatz.

Dieser Austausch von Schlüsselinformationen geschieht durch die in Abbildung 25 gezeigte EAPOL-Key-Sequenz. Bei diesem sogenannten 4-Way-Handshake werden insbesondere zwei Pseudozufallszahlen (ANonce für den Authenticator und SNonce für den Supplicant) über EAPOL ausgetauscht, die

[17] Hier ist darauf zu achten, dass der PSK möglichst zufällig gewählt wird bzw. aus einem Passwort hoher Komplexität mit mindestens 20 Zeichen gebildet wird.

als sitzungsspezifische Parameter in die Funktion zur Ableitung der PTK einfließen, wie in Kapitel 6.1.2 in Abbildung 18 am Beispiel von TKIP bereits illustriert wurde. Diese Möglichkeit ist für eine sichere WLAN-Kommunikation bei WPA und bei IEEE 802.11i erforderlich, um einen statischen Schlüssel wie bei WEP zu vermeiden.

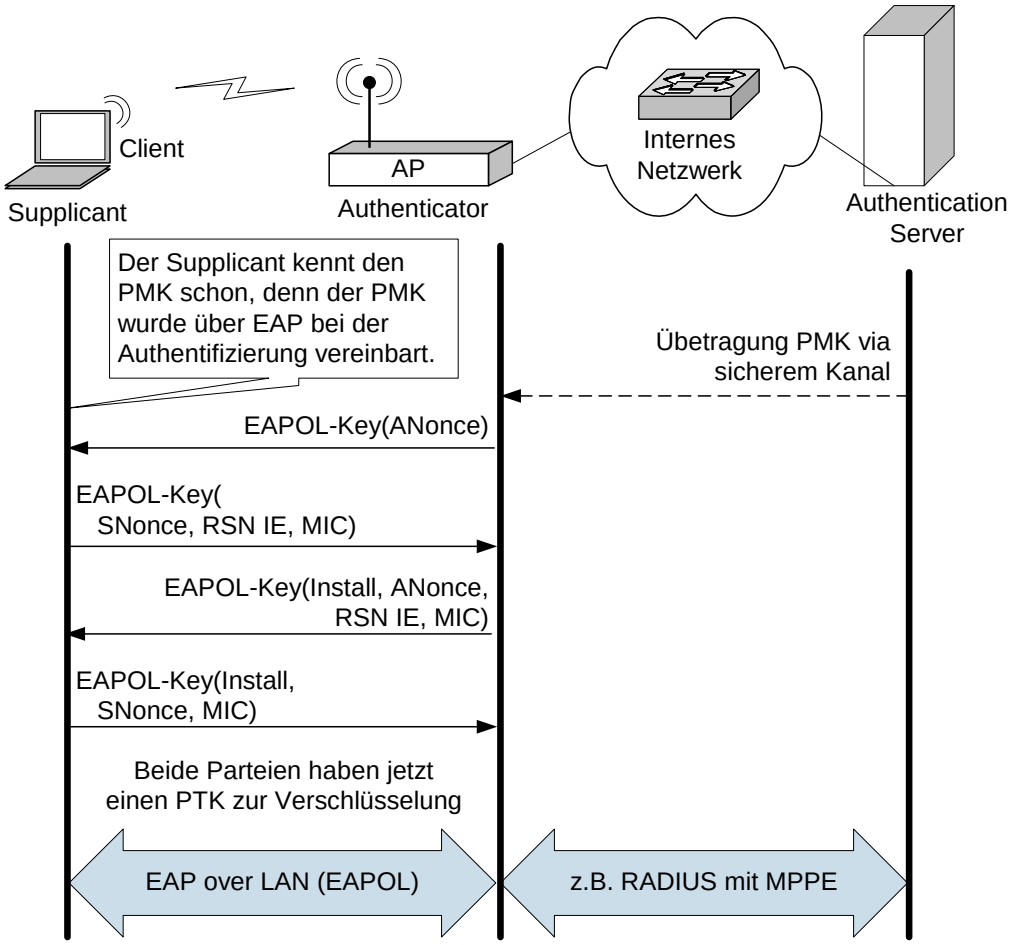



Abbildung 25: PTK-Schlüsselgenerierung über EAPOL Key Exchange

Für den Bereich WLAN kommen nur EAP-Methoden in Frage, die eine geeignete Art von Schlüsselerzeugung unterstützen.

Das Vereinbaren von Schlüsseln über die EAPOL-Key-Nachrichten setzt voraus, dass die beiden EAPOL-Partner über einen PMK (Pairwise Master Key) verfügen, der von der EAP-Methode geliefert werden muss – und zwar derart, dass beide Partner diesen PMK kennen. Die Übermittlung dieses PMK vom AS zum AP kann z. B. über RADIUS-Attribute erfolgen (MPPE-Schlüssel). IEEE 802.1X macht hierzu allerdings keine Vorgaben.

Bei lang andauernden WLAN-Sitzungen ist es sinnvoll, den PMK „aufzufrischen“. Hierzu sieht IEEE 802.1X die Funktion der regelmäßigen Re-Authentifizierung (Reauthentication) vor.

## 7.2 Authentifizierungsverfahren und EAP-Methoden

Die Auswahl eines Authentifizierungsverfahrens (d. h. einer EAP-Methode), welches für IEEE 802.1X verwendet werden soll, hängt unter anderem davon ab, ob die genutzten Client-Typen das Verfahren unterstützen oder entsprechend erweiterbar sind. Weiterhin bestimmt die vorhandene oder gewünschte Infrastruktur zur Benutzerauthentifizierung die Anwendbarkeit einer EAP-Methode. Zu berücksichtigen ist auch, ob das Verfahren Möglichkeiten zur Schlüsselverwaltung und -verteilung bietet. Letzteres ist bei WLAN ein besonders wichtiger Aspekt, wenn es darum geht, Verfahren wie z. B. WPA-TKIP anzuwenden. Folgende Verfahren sind derzeit[18] unter anderem verfügbar:

- EAP-MD5 (RFC 2284 bzw. RFC 3748, EAP Typ 4)
- EAP-OTP (RFC 2284 bzw. RFC 3748, EAP Typ 5)
- EAP-GTC (RFC 2284 bzw. RFC 3748, EAP Typ 6)
- EAP-TLS (RFC 2716, EAP Typ 13)
- EAP-TTLS (IETF Internet Draft, EAP Typ 21)
- EAP-PEAP (RSA, Cisco, Microsoft, IETF Internet Draft, EAP Typ 25)
- EAP-Cisco Wireless (auch LEAP, Herstellerentwurf, Cisco, EAP Typ 17)
- EAP-MSCHAPv2 (Herstellerentwurf, Microsoft, IETF Internet Draft, EAP Typ 26)
- EAP-FAST (IETF Draft, Herstellerentwurf, Cisco, EAP Typ 43)
- EAP-SIM (IETF Internet Draft, Herstellerentwurf, 3GPP, EAP Typ 18)

### 7.2.1 EAP-MD5

Die EAP-Methode MD5 (Message Digest 5, ein Hash-Algorithmus) ist bereits im EAP-Standard selbst beschrieben.

EAP-MD5 (MD5-CHAP als EAP-Methode, Challenge Handshake Authentication Protocol) muss von allen EAP-Standard-konformen EAP-Implementierungen unterstützt werden.

Dies bedeutet nicht automatisch, dass MD5 auch als Authentifizierungsmethode zugelassen ist. Lediglich die technische Möglichkeit muss von der Implementierung zur Verfügung gestellt werden. Welche Authentifizierungsmethode in einer tatsächlichen Umgebung zulässig ist und unter welchen Bedingungen, wird an anderer Stelle festgelegt, typischerweise auf dem RADIUS-Server.

Bei MD5-CHAP wird, vereinfacht gesagt, vom Server unter anderem ein zufälliger Challenge-String an den Client gesendet, der den MD5-Hash aus dieser Nachricht und dem Benutzerkennwort bildet und an den Server zurück übermittelt. Der Server kann diese Operation ebenfalls durchführen und damit prüfen, ob die Gegenstelle das richtige Kennwort kannte. Ist dies der Fall, ist damit der Benutzer authentisch. Hierbei wird der Benutzername (wie bei vielen anderen Verfahren auch) im Klartext übertragen.

Da MD5-CHAP, häufig auch nur kurz CHAP genannt, einige Schwachstellen aufweist (siehe z. B. [MiAr02]) und zudem die beiderseitige Kenntnis eines unverschlüsselten Passwortes erfordert, ist es nach modernen Erkenntnissen kein empfehlenswertes Verfahren.

Weiterhin unterstützt EAP-MD5 keine Schlüsselerzeugung und scheidet daher für die unmittelbare Nutzung in IEEE 802.11i bzw. WPA- und WPA2-Enterprise zunächst aus.

[18] Den EAP-Methoden werden von der IANA die EAP-Typnummern zugeordnet.

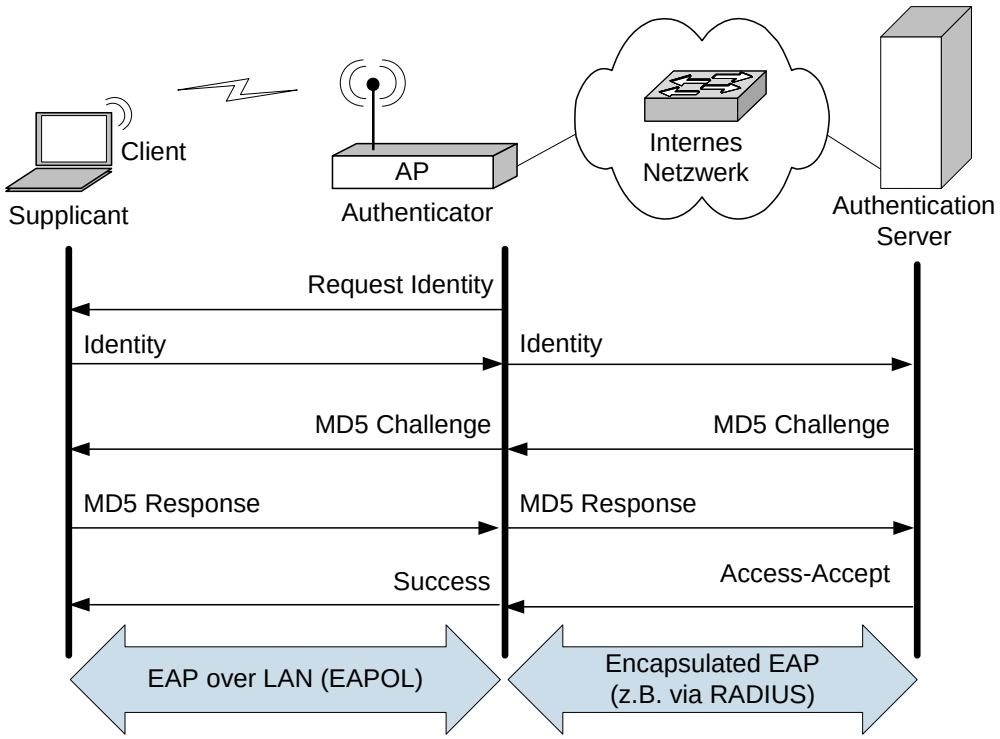



Abbildung 26: EAP-MD5 über IEEE 802.1X

### 7.2.2 EAP-GTC und EAP-OTP

Die EAP-Typen Generic Token Card (GTC) und One-Time Password (OTP) sind ebenfalls bereits im EAP-Standard spezifiziert[19], müssen jedoch nicht zwingend von Implementierungen unterstützt werden.

EAP-GTC ist ein Verfahren, bei dem ein Challenge-String an den Client übertragen wird, woraufhin der Benutzer üblicherweise einen Wert von einer Token Card abliest – teils zeitabhängig oder auch nach Eingabe von Informationen in die Token Card. Der abgelesene Wert kann dann vom Benutzer über einen entsprechenden Dialog eingegeben werden. Hierbei wird oft die Kombination von Wissen und Besitz zur Authentifizierung genutzt, wobei der Benutzer zusätzlich eine nur ihm bekannte PIN eintippt, entweder auf der Token Card selbst oder auf dem Client.

Der Typ OTP wird verwendet, um Benutzer über Einmalpasswörter zu authentifizieren. Dabei wird ein Request vom Authentication Server gesendet, welcher vom Benutzer durch die Eingabe eines Einmalpasswortes beantwortet wird.

Einmalpasswörter oder die Nutzung von Token Cards sind einander konzeptionell ähnlich. Manchmal werden Token Cards zur Bereitstellung von zeitabhängigen einmaligen Passcodes verwendet. Sie gelten – gegenüber gewöhnlichen Kennworten – als sicherer[20], sind aber u. a. anfällig für Attacken vom Typ Man in the Middle (MitM).

Wie die vorgenannte EAP-Methode MD5 unterstützen auch GTC und OTP alleine keine gegenseitige Authentifizierung oder Schlüsselerzeugung. Sie kommen direkt daher nicht in Frage, wenn man unter

19 OTP selbst ist in RFC 2289 und RFC 2243 beschrieben (siehe [OTP98] und [OTP97]).

20 Falls OTP oder GTC lediglich als Transportweg für gewöhnliche Kennworte (nicht Einmalkennworte) verwendet werden, sind die Verfahren jedoch keineswegs als sicher zu erachten. Daher ist gemäß RFC 3748 (EAP) außerhalb von geschützten Tunneln eine solche Verwendung verboten.

Verwendung von 802.1X die Sicherheit in WLAN erhöhen will. Indirekt[21] (d. h. getunnelt über die unten erläuterten Methoden PEAP, TTLS, FAST) finden sie aber durchaus Verwendung.

### 7.2.3 EAP-TLS

Die Methode EAP-TLS ist als einzige außer den in RFC 2284 bereits genannten Methoden bisher als RFC veröffentlicht. Die Tests für eine WPA-Zertifizierung der Wi-Fi-Alliance werden mit dieser EAP-Methode durchgeführt.

EAP-TLS (RFC 2716, siehe [TLS99]) basiert auf der Technik von TLS (Transport Layer Security). Jedoch wird hier nur ein Teil dessen verwendet, was TLS zu leisten im Stande ist, nämlich im Wesentlichen die Authentifizierung, die eine der Voraussetzungen für eine sichere Kommunikation ist.

Bei EAP-TLS wird eine beidseitige Authentifizierung anhand von X.509-Zertifikaten durchgeführt.

Dazu muss der zu authentifizierende Partner beweisen, dass er den privaten Schlüssel kennt, der zu dem öffentlichen Schlüssel gehört, welcher seinem Kommunikationspartner bekannt ist. In einem Zertifikat ist dieser öffentliche Schlüssel enthalten und weiterhin wird mit eben diesem Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA, siehe auch Kapitel 15.6) dafür gebürgt, dass es sich bei dem im Zertifikat genannten Inhaber wirklich um diese Instanz (z. B. eine Person oder ein Gerät) handelt. Wer also zeigen kann, dass er den privaten Schlüssel kennt, ist damit authentifizierbar.

Der Ablauf bei TLS ist vereinfacht wie folgt beschrieben:

Der Client sendet eine Hello Message u. a. mit einer Random-Zeichenkette und Informationen zur Aushandlung von Verschlüsselungsparametern, worauf der Server mit einem Server Hello nebst eigener Certificate Chain (Zertifikatskette, inklusive dem eigenen Zertifikat) antwortet. Dabei fordert der Server auch das Client-Zertifikat an. Der Client überprüft die Certificate Chain und generiert ein Pre-Master Secret, verschlüsselt dieses mit dem öffentlichen Schlüssel des Servers und übermittelt es (Key Exchange) zusammen mit einem mittels privatem Schlüssel signierten Hash der vorhergehenden Kommunikation als Nachweis seiner Authentizität (Certificate Verify). Vom Pre-Master Secret können beide Seiten ein Master Secret ableiten und haben damit ein geteiltes Geheimnis (Shared Key), das TLS-Master Secret. Weiterhin wird das Client-Zertifikat an den Server übermittelt, welches der Server überprüfen kann. Danach schickt der Client eine mit den vorher vereinbarten Parametern verschlüsselte Finished-Nachricht, welche der Server mit einer Finished-Nachricht beantwortet. Da diese Antwort wiederum einen überprüfbaren, signierten Hash der vorherigen Kommunikation beinhaltet, ist somit auch der Server aus Sicht des Clients authentisch.

Der während der Authentifizierungsphase von TLS erzeugte geheime Schlüssel, das TLS-Master Secret (oder auch Master Session Key, MSK), kann bei einer folgenden verschlüsselten Kommunikation (z. B. ein TLS-Tunnel) u. a. zur Erzeugung von Session Keys (mittels der PRF, Pseudo-Random Function, eine in der Kryptografie häufig genutzte Funktion zur Erzeugung von Zufallswerten) verwendet werden. Das TLS-Master Secret wird allgemein als sicher generiert erachtet – korrekt verwendet lassen sich mit seiner Hilfe weitere sichere Schlüssel vereinbaren.

Bei TLS selbst wird daraufhin verschlüsselt kommuniziert, bei EAP-TLS ist mit der Erzeugung des MSK der TLS-spezifische Ablauf beendet; die Parteien sind wechselseitig authentifiziert. Der MSK kann für weitere Zwecke verwendet werden, z. B. als PMK zur Erzeugung von Schlüsseln (PTK) für eine sichere WLAN-Übertragung über TKIP oder CCMP (siehe Kapitel 6). EAP-TLS unterstützt also nicht direkt, wie manchmal beschrieben, die dynamische Erzeugung von Schlüsseln für die WLAN-Kommunikation, sondern die Bereitstellung eines MSK. Die darunter liegende Verschlüsselungsanwendung (im Falle von WLAN also z. B. die TKIP-Umgebung mit EAPOL) muss für eine korrekte Verwendung des MSK sorgen. Für den Einsatz in WLAN-Umgebungen bedeutet dies z. B., dass be-

[21] In den IETF Drafts, welche OTP und GTC als EAP-Methoden näher beschreiben, wird ausdrücklich von der direkten Verwendung über WLAN oder über das öffentliche Internet abgeraten.

sagter Schlüssel auch dem AP bekannt gemacht werden muss, wenn dieser sicher mit dem WLAN-Client kommunizieren will.

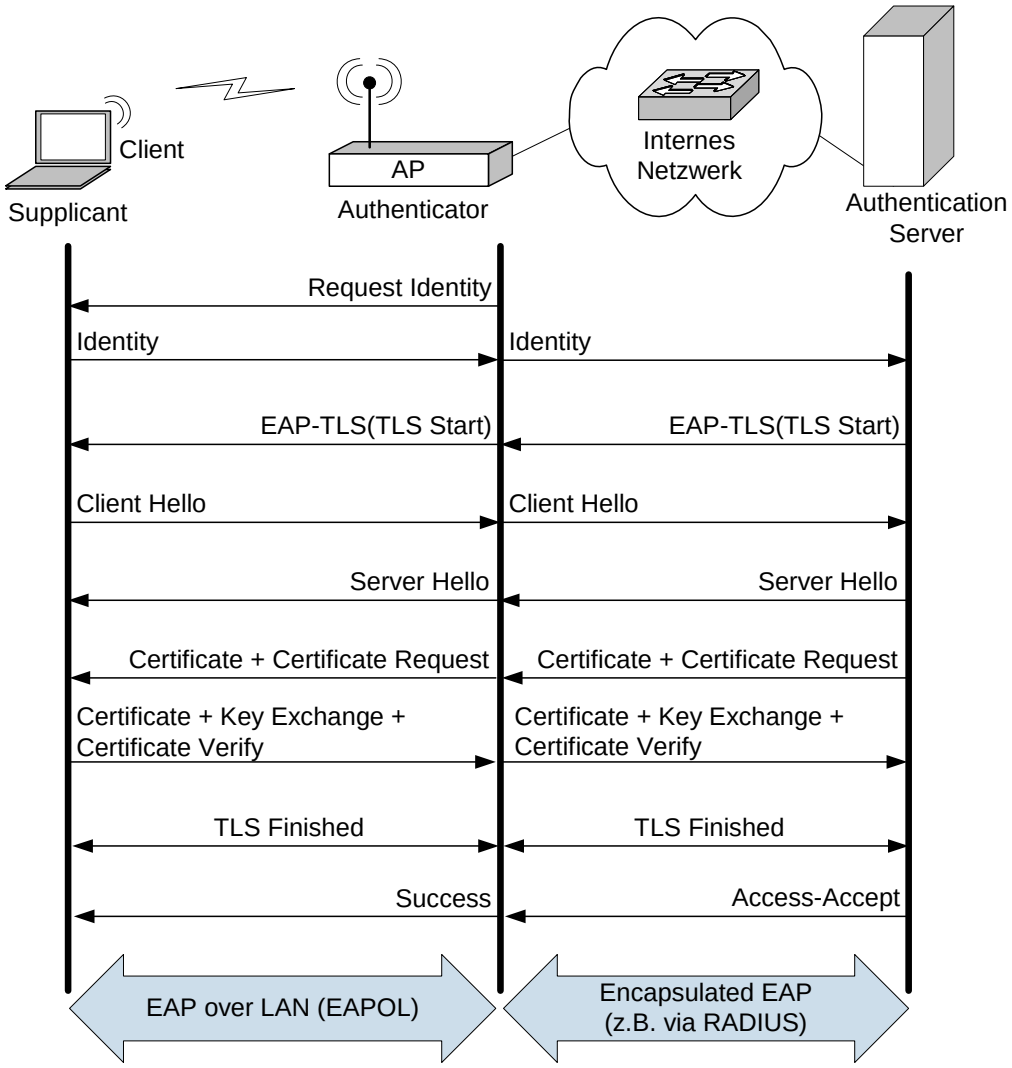



Abbildung 27: EAP-TLS über IEEE 802.1X (vereinfacht)

Ein wichtiger Aspekt bei EAP-TLS ist die Bereitstellung von Zertifikaten: Alle Parteien, die über EAP-TLS authentifiziert werden sollen, müssen dazu ein Zertifikat erhalten. Dies sind für den Bereich WLAN auch alle Clients bzw. alle Benutzer (siehe hierzu auch Kapitel 7.3).

Folglich müssen Verfahren etabliert sein oder werden, die eine entsprechende Zertifikatsverteilung erreichen und die Verwaltbarkeit (z. B. Ausstellung, Rückruf, Erneuerung von Zertifikaten etc.) gewährleisten. Eine solche Public Key Infrastructure (PKI) zu installieren und zu betreiben setzt eine sorgfältige Planung voraus.

### 7.2.4 EAP-TTLS

Ein weiterer EAP-Typ, der bei der IETF als Draft vorliegt (siehe [FBW04]), ist das EAP Tunneled TLS Authentication Protocol (kurz: EAP-TTLS). Bei diesem Verfahren wird der oben beschriebene TLS-Handshake so durchgeführt, dass nur der EAP-Server (also z. B. der RADIUS-Server) authentifi-

ziert wird, der Client jedoch noch nicht. Daher benötigt der Client auch kein Zertifikat, was unter Umständen zu einer erleichterten Implementierung führen kann, besonders falls nicht für alle Client-Typen Zertifikate ausgestellt werden können oder sollen. Da aber im WLAN gerade der Client bzw. der Benutzer authentifiziert werden soll, ist das Verfahren so gestaltet, dass andere Authentifizierungsprotokolle getunnelt werden können, und zwar durch einen TLS-Tunnel (Abbildung 28).

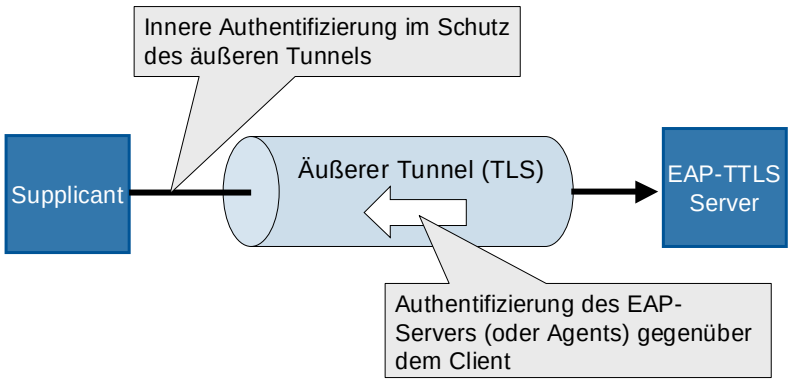



Abbildung 28: Authentifizierung im Tunnel bei EAP-TTLS

Daher wird bei EAP-TLS nicht nur der TLS-Handshake zu Ende geführt, sondern das TLS-Verfahren weitergenutzt, um die TLS-verschlüsselte Verbindung zwischen dem Client und dem Authentication Server (oder einem Authentication Agent) zu etablieren. In diesem verschlüsselten Tunnel können nun andere Methoden wie z. B. GTC benutzt werden –auch weniger sichere, da die übermittelten Daten durch TLS geschützt werden. Im Tunnelinneren können sowohl ältere Standardprotokolle verwendet werden (wie PAP, CHAP, MSCHAP, siehe Anhang in Kapitel 15) als auch wiederum EAP-Methoden. Das Tunnelende bildet ein EAP-TTLS-Server, der nicht notwendigerweise auch der AS für das innere Protokoll sein muss: Er kann selbst als Authentication Agent wiederum Client eines weiteren Servers sein, der nur das innere, ggf. ältere, Protokoll unterstützt. Auch bei TTLS wird Schlüsselmaterial (MSK) erzeugt und auch hier muss (z. B. über RADIUS-Attribute) dieses Schlüsselmaterial zum Authenticator (also zum Access Point) gelangen.

### 7.2.5 EAP-PEAP

Wie auch EAP-TTLS ist Protected EAP (kurz: PEAP) ein Schlüsselmaterial erzeugendes Verfahren, bei dem zunächst über TLS der Server über ein Zertifikat authentifiziert wird und dann ein verschlüsselter TLS-Tunnel zwischen dem Client und dem PEAP-Server genutzt wird, um in diesem Tunnel andere Methoden zur Authentifizierung des Benutzers anzuwenden (analog zu Abbildung 28).

Wie bei EAP-TTLS ist auch bei EAP-PEAP eine Trennung von Authentication Agent und AS möglich, sodass der PEAP-Server ein anderes Gerät sein kann als der AS zur Benutzerauthentifizierung. Bei EAP-PEAP sind innerhalb des Tunnels im Unterschied zu EAP-TTLS allerdings nur EAP-Methoden zulässig, z. B. EAP-MSCHAPv2, EAP-TLS (beide u. a. bei Microsoft verwendet) oder EAP-GTC (u. a. Cisco).

EAP-PEAP wurde einige Male von RSA Security, Cisco und Microsoft als Internet Draft veröffentlicht, erlangte zwar nie Standard-Status, ist aber durch die Integration in MS Windows XP weit verbreitet. PEAP ist also ein herstellerspezifisches Verfahren, durch seine XP-Integration und die Verfügbarkeit auch für Windows 2000 jedoch ein Quasi-Standard.

Besonders für die Microsoft-basierten Umgebungen ist die Kombination von EAP-PEAP mit EAP-MSCHAPv2 interessant. MSCHAPv2 ist eine bei Windows-Clients häufig genutzte PPP-Authentifizierungsmethode, die besonders gut zu den Microsoft-Lösungen zur Benutzerverwaltung (z. B. den Domänen) passt. Es handelt sich um ein Challenge/Response-Verfahren zur Benutzerauthentifizierung über User-Name und Passwort-Hash. PEAP mit EAP-MSCHAPv2 lässt sich z. B.

über einen RADIUS-Server, der an das Active Directory oder an eine NT4-Domäne gekoppelt ist, mit nur geringem Aufwand in einer Microsoft-Umgebung implementieren.

Unter anderem bedingt durch die breite Basis installierter Windows-Clients ist bei EAP-PEAP die Interoperabilität auch bei WLAN-Produkten unterschiedlicher Hersteller häufig gegeben.

Bei EAP-PEAP muss für die Authentifizierung des Servers für diesen ein Zertifikat zur Verfügung gestellt werden. Dies erfordert eine PKI (siehe auch Kapitel 15.6), jedoch ist der administrative Aufwand zur Verteilung von Zertifikaten bei PEAP und bei EAP-TTLS (Zertifikate nur serverseitig) deutlich geringer als z. B. bei EAP-TLS (Zertifikate für beide Seiten).

Aus kryptografischer Sicht ist zu beanstanden, dass PEAP, ebenso wie EAP-TTLS, zur Sicherung des äußeren Tunnels nur die Identität des Servers prüft, die des Clients dagegen eben in diesem Schritt noch nicht. Dies bietet aber nicht das gleiche Sicherheitsniveau wie ein Authentifizierungsverfahren, welches direkt die Identität beider Seiten überprüft. Aus diesem Grund rät auch RFC 3748 (EAP) von einer solchen getunnelten Lösung ab, sofern andere Verfahren genutzt werden können.

Von der Version PEAPv2 wird erwartet, dass die denkbare MitM-Attacke[22] (Man in the Middle) durch weitere Verbesserungen ausgeschlossen ist (siehe [PSS04]). Falls dieses Ziel erreicht wird, ist PEAPv2 durchaus als sicheres Protokoll einzuschätzen. Auch PEAPv1 ist in den meisten praktischen Anwendung nicht pauschal als unsicher zu bewerten. Es ist auf jeden Fall Verfahren wie CHAP oder MSCHAP vorzuziehen, welche allerdings auch nur selten direkt zur (herstellerspezifischen) Authentifizierung bei WLANs Anwendung finden, da sie für IEEE 802.1X nicht genutzt werden können.

Ob die potentielle Angreifbarkeit von PEAP und TTLS über MitM-Attacken für den jeweiligen Einsatzzweck relevant ist, bleibt aber im Einzelfall zu entscheiden – für höchste Sicherheitsansprüche sollten PEAP und TTLS als Tunnel für weniger starke innere Authentifizierungsverfahren vermieden werden.

### 7.2.6 LEAP oder EAP-Cisco Wireless

Als erstes EAP-Verfahren für die WLAN-Verwendung unter IEEE 802.1X wurde von Cisco LEAP (Lightweight EAP) entwickelt, das auch EAP-Cisco Wireless oder kurz EAP-Cisco genannt wird.

Bei LEAP handelt es sich um ein proprietäres Verfahren, das jedoch auch zusammen mit WPA einsetzbar ist. Ursprünglich wurde es von Cisco nicht offen gelegt.

Durch Analyse der übertragenen Daten wurde es aber rekonstruiert und im Internet öffentlich gemacht (siehe z. B. [Mac01]. LEAP authentifiziert den Client und den Authentication Server über User-Namen und Passwort-Hash, wobei durch Verwendung eines modifizierten MS-CHAPv2 besonderer Wert auf die Interoperabilität mit Microsoft-Umgebungen gelegt wurde. Entsprechend lässt sich der zugehörige RADIUS-Server z. B. an ein Active Directory koppeln.

Das Verfahren wird durch die starke Verbreitung von Cisco-Produkten im WLAN-Bereich häufig eingesetzt, ist jedoch (wie allerdings viele passwortbasierte Verfahren) anfällig für so genannte Wörterbuch-Attacken. Diese Angreifbarkeit wird zwar durch das Verwenden von starken Passwörtern relativiert, oft sind jedoch kryptografisch starke Benutzer-Passwörter nicht ohne weiteres umsetzbar, sodass derartige Verfahren weniger zu empfehlen sind[23]. Da viele der Produkte, die LEAP unterstüt-

---

22 Um die MitM-Attacke durchführen zu können, sind allerdings einige Randbedingungen erforderlich, die in der Praxis derzeit häufig nicht gegeben sind – unter anderem die Verwendbarkeit desselben Authentifizierungsverfahrens sowohl innerhalb aus auch außerhalb von Tunneln. Gute kryptografische Verfahren sollten allerdings auch unter diesen ungünstigen Randbedingungen sicher bleiben, sonst ist dies als eine Schwachstelle anzusehen, selbst wenn diese aus aktueller Sicht noch recht theoretisch ist. Weiterhin wird bei strikter Prüfung der Server-Zertifikate die Umsetzung der MitM-Attacke deutlich erschwert.

23 Es wurde im Internet bereits ein Werkzeug veröffentlicht, welches die genannte Schwäche ausnutzen kann.

zen, auch EAP-PEAP beherrschen oder sich entsprechend erweitern lassen, ist eine Alternative in diesem Fall u. a. der Umstieg auf EAP-PEAP in Kombination z. B. mit EAP-MSCHAPv2. Eine neuere Alternative ist die Verwendung des weiter unten erwähnten EAP-FAST.

Nachteilig an LEAP ist auch die Abhängigkeit des Protokolls von den APs selbst: Bei reinen EAP-Methoden ist dies nicht gegeben; bei LEAP muss man jedoch für die Access Points Produkte einsetzen, die LEAP auch explizit unterstützen. Begründet ist diese Abhängigkeit, die vom Standard IEEE 802.1X so nicht vorgesehen ist, unter anderem dadurch, dass LEAP bereits vor der Verabschiedung des Standards verfügbar war.

LEAP ist nach Stand der Technik als ein „Auslaufmodell“ anzusehen, das in der Vergangenheit einen guten Kompromiss zwischen Sicherheit und Administrierbarkeit bot.

Für neue WLAN-Installationen sollte LEAP wegen seiner Schwächen nicht mehr in Betracht gezogen werden, da mit IEEE 802.11i ein flexiblerer Standard zur Verfügung steht, der auch sicherere Verfahren unterstützt.

### 7.2.7 EAP-FAST

EAP-FAST (Flexible Authentication via Secure Tunneling, EAP-Typ 43) wurde von Cisco als Nachfolger von LEAP vorgesehen und ist als Draft[24] bei der IETF veröffentlicht, siehe [CMS05].

Das Verfahren soll für die bei LEAP genannte Wörterbuch-Attacke nicht anfällig sein. Auch bei EAP-FAST wird wie bei EAP-PEAP die Tunnel-Technik von TLS eingesetzt, um ein anderes Verfahren in diesem Tunnel zu schützen.

Im Unterschied zu bisher üblichen TLS-basierenden Methoden wird jedoch bei EAP-FAST ein symmetrisches Verfahren zur Authentifizierung eingesetzt, sodass keine Zertifikate notwendig sind, weder auf Client- noch auf Server-Seite. Damit aber dennoch die gewünschte und wichtige gegenseitige Authentifizierung möglich ist, muss ein anderes gemeinsames Geheimnis für diesen Zweck auf dem Client und dem Server bekannt gemacht werden – es handelt sich also um eine Authentifizierung über pre-shared keys, unter EAP-FAST Teil der so genannten PAC-Informationen (Protected Access Credential). Um diese Information sicher zu verteilen, sieht Cisco einen manuellen Weg vor und einen Automatismus, der z. B. bei der Erstinstallation verwendet werden kann, falls eine sichere Netzwerkumgebung gegeben ist. Eine erwähnenswerte Funktion ist auch die Möglichkeit, einmal verteilte PAC-Informationen innerhalb von EAP-FAST selbst aktualisieren zu können, sodass ein automatisierter Schlüsselwechsel stattfinden kann.

Durch eine kryptografische Verbindung zwischen dem Tunnel und der inneren Methode bietet EAP-FAST konzeptionell nicht die Angriffsflächen wie z. B. EAP-PEAP. Da bei EAP-FAST der Tunnel selbst bereits beidseitig authentifiziert ist, sind die diskutierten MitM-Attacken hier praktisch nicht mehr relevant. EAP-FAST ist daher auch nicht zu denjenigen Tunnel-Verfahren zu zählen, von denen RFC 3748 abrät.

Aus aktueller Sicht ist demnach das Verfahren vom Aufbau her als sicher zu bezeichnen, sofern die Verteilung der PACs ebenfalls sicher gestaltet werden kann. Fundiertere Aussagen zur Sicherheit eines Verfahrens lassen sich im Allgemeinen jedoch erst nach längerer Betriebszeit machen.

Interessant ist EAP-FAST zunächst für Nutzer, die bisher WLAN-Produkte von Cisco in Kombination mit Microsoft und dem Active Directory unter Verwendung von LEAP einsetzten: Eine Modernisierung hin zu EAP-FAST ist hier relativ unkompliziert möglich.

---

[24] Da die Anforderungen an neue EAP-Methoden durch RFC3748 verschärft wurden, werden seit dessen Veröffentlichung erst nach einem Review durch einen Experten neue EAP-Typnummern vergeben. EAP-FAST genügt aber bereits erweiterten Anforderungen von RFC3748 und nimmt für sich in Anspruch, alle im RFC vorgesehenen Sicherheitsziele zu erreichen.

### 7.2.8 EAP-MSCHAPv2

Bei EAP-MSCHAPv2 handelt es sich um die Integration von MS-CHAPv2 in die EAP-Umgebung. Der Vorschlag für diese EAP-Methode ist im Jahre 2004 wieder neu als Draft veröffentlicht worden (siehe [KaPa04]). Die Methode ist noch kein RFC Standard, ist unter MS Windows XP aber bereits implementiert und ist auch für Windows 2000 verfügbar, also dementsprechend weit verbreitet.

Derzeit ist EAP-MSCHAPv2 (innerhalb von PEAP) bei Microsoft das Standardverfahren, wenn nicht mittels Zertifikaten authentifiziert werden soll – unter anderem bedingt durch die Tatsache, dass die Technik sehr gut zu einer MS Active Directory-Umgebung (AD) passt. Hierbei kann der Client authentifiziert werden, ohne dass Anpassungen an dem Verzeichnisdienst AD notwendig wären. Das Verfahren MS-CHAPv2 und damit auch die entsprechende EAP-Methode setzen u. a. voraus, dass der Verzeichnisdienst einen so genannten Password Hash (und nicht notwendigerweise das Kennwort selbst) kennt. Das genau ist beim Active Directory und auch bereits unter Windows NT 4.0 der Fall.

Da bereits eine Reihe von Tunnelverfahren für die Authentifizierung über EAP-Methoden existiert (PEAP, TTLS, FAST), wird EAP-MSCHAPv2 auch zukünftig eine wichtige Rolle spielen – auch für Wireless LANs. Innerhalb solcher Tunnel, besonders z. B. innerhalb von EAP-FAST, ist der Einsatz des Verfahrens daher nach heutigem Kenntnisstand sinnvoll und sicher, auch wenn MS-CHAPv2 alleine (ohne sichere Tunnel) aus heutiger Sicht für nicht gesicherte Netzwerkverbindungen nicht empfehlenswert ist.

### 7.2.9 EAP-SIM und EAP-AKA

Die aus dem Mobilfunk bekannten SIM-Karten (Subscriber Identity Module) sind die Grundlage für die Methode EAP-SIM (EAP-Typ 18, siehe [HaSa04]). Das Verfahren wurde auf Anregung des 3rd Generation Partnership Project (3GPP), das als Herstellergremium für die technische Entwicklung der GSM- und UMTS-Standardfamilie verantwortlich zeichnet, durch Nokia als Draft veröffentlicht. SIM-Karten sind Smartcard-ähnliche Geräte u. a. mit kryptografischen Funktionen, die es erlauben, einen Teilnehmer anonym und Mobilfunknetz-übergreifend zu authentifizieren. Ähnliches gilt auch für U-SIM-Karten (Universal Subscriber Identity Module, UMTS SIM), die bei dem Verfahren EAP-AKA (Authentication and Key Agreement[25], EAP-Typ 23, siehe [ArHa04]) verwendet werden. USIM wurde für UMTS (Universal Mobile Telecommunications System) definiert.

Bei EAP-SIM und EAP-AKA besteht grundsätzlich die Möglichkeit, die Mobilfunk-Roaming-Infrastruktur zur Authentifizierung von einem anderen Netz aus, z. B. von einem WLAN aus, zu nutzen. Bei der Anbindung eines WLAN an ein Mobilfunknetz ist außerdem eine Vereinheitlichung der Abrechnung über den Betreiber des Mobilfunknetzes erreichbar. EAP-SIM und EAP-AKA sind für die Authentifizierung in Hotspots von Interesse.

EAP-AKA ist u. a. wegen besserer kryptografischer Verfahren und längerer Schlüssel als sicherer zu erachten als EAP-SIM und wird innerhalb des Draft zu EAP-SIM sogar empfohlen, falls die entsprechende Infrastruktur zur Verfügung steht. Beide EAP-Methoden unterstützen das Generieren von Schlüsselinformationen (Key Derivation) sowie die gegenseitige Authentifizierung[26].

---

25 Die Methode EAP-AKA basiert auf UMTS AKA. EAP-Methoden sind aber nicht mit den Authentifizierungsverfahren im Mobilfunk zu verwechseln oder mit diesen identisch.

26 Die Authentifizierung mittels SIM im Mobilfunkbereich unterstützt jedoch selbst keine gegenseitige Authentifizierung. UMTS AKA bietet diese Funktion bereits.

## 7.3 Integration in die Benutzerverwaltung

In vielen Fällen wird es gewünscht sein, eine einheitliche Umgebung aufzubauen, in der die Wireless-Nutzer an demselben System authentifiziert und autorisiert werden sollen wie die Nutzer im LAN. Zunächst gilt es also festzustellen, ob eine solche Kopplung gewünscht ist. Wenn dies der Fall ist, so ist bei der Produktauswahl zu beachten, dass mindestens die Kombination aus Client-Betriebssystem, Supplicant, Access Point, Wireless Distribution System, Authentication Server, der Verbindung von AS zur Benutzerverwaltung und der Benutzerverwaltung selbst die maßgebliche Wirkkette darstellt. Es sind also im Allgemeinen nicht ausschließlich die EAP-Methoden relevant, sondern ggf. nahezu alle beteiligten Komponenten.

Wichtig ist in diesem Zusammenhang auch die Unterscheidung von Benutzer- und Computerauthentifizierung: Von einer Benutzerauthentifizierung wird gesprochen, falls eine WLAN-Verbindung erst erfolgreich aufgebaut werden kann, wenn ein Benutzer am Client-System angemeldet ist und sich gegenüber der IEEE 802.1X-Umgebung authentifizieren kann. Dies kann durch Eingeben von Informationen wie Kennwort oder Smartcard-PIN oder durch automatisches Nutzen solcher Informationen geschehen. Benutzername und Kennwort können beispielsweise automatisch geschickt werden oder über den privaten Schlüssel im Zugriff des Nutzers, z. B. über ein Zertifikat, wird automatisch dessen Identität bewiesen.

Beim Vergleich mit den üblichen Verfahren im LAN fällt aber auf, dass dort normalerweise der Ablauf etwas anders ist: Ein Client verbindet sich mit einem Port des Netzes (z. B. durch Einschalten des PCs), das Betriebssystem initialisiert beim Hochfahren seinen TCP/IP-Stack und führt z. B. DHCP durch, um eine IP-Konfiguration zu erhalten. Danach wird der Rechner einige Kommunikation im Netzwerk durchführen, um z. B. im Falle eines MS Windows-Systems Richtlinien für den Computer anzufordern, die er dann umsetzt – und zwar noch bevor irgendein Benutzer angemeldet ist.

Wenn all dies nun statt in einem kabelgebundenen LAN im Wireless LAN, abgesichert durch IEEE 802.1X, passieren soll, so kann diese Kommunikation nur dann erfolgen, wenn nicht der Benutzer, sondern der Computer sich über EAP authentifizieren kann. IP-Pakete werden ja erst dann von dem AP weitergeleitet, wenn der Port in den Zustand „authenticated“ bzw. freigeschaltet wurde (siehe Abbildung 23). Unter Windows XP beispielsweise ist genau dies möglich und standardmäßig auch so konfiguriert: Das System versucht, sich als Computer zu authentifizieren, wenn die WLAN-Verbindung aktiviert werden soll und kein Nutzer angemeldet ist. Dies setzt allerdings voraus, dass der Authentication Server auch einen „Benutzer“ dieses Namens authentifizieren kann. Dies ist z. B. bei Verwendung des Active Directory von Microsoft der Fall: Hier ist der Computer selbst ein sog. Security Principal, der in der Domäne einen Account und auch ein Kennwort hat (das er selbst verwaltet und ändert). Ein System (kein Nutzer) wird sich aber nur dann erfolgreich im WLAN authentifizieren können, wenn solche Voraussetzungen erfüllt sind.

Zur Geräteauthentifizierung ist es also z. B. erforderlich, dass ein RADIUS-Server, der die Identitätsprüfung vornimmt, über die gewählte EAP-Methode entweder selbst oder in Zusammenarbeit mit dem Verzeichnisdienst, den er nutzt, den Computer überhaupt authentifizieren und autorisieren kann.

Bei der Diskussion um die Fähigkeit zur Integration verschiedener Produkte und Verfahren in die bestehende oder aufzubauende Infrastruktur zur Benutzerverwaltung darf aber auch ein gewissermaßen „dezentraler“ Ansatz nicht außer Acht gelassen werden: Nämlich gerade die beabsichtigte Trennung der Benutzerverwaltung von WLAN, RAS oder VPN-Verbindungen von den Verwaltungsstrukturen innerhalb des LAN.

Bei klassischen, Firewall-basierenden VPN oder RAS-Zugängen beispielsweise wird dieser Weg oft beschritten, mit dem Effekt, dass das Thema „Schutz des Netzwerkes nach außen“ meist unter die Verwaltungshoheit einer anderen Abteilung fällt als das Thema „Sicherheit innerhalb des Netzwerkes“. Aus sicherheitstechnischer Sicht spricht auch einiges für diesen Ansatz, denn die immer weiter wachsende Komplexität der zu bewältigenden Aufgaben hat auch eine Fehleranfälligkeit – technische wie menschliche – zur Folge. Ebenso bringt die Abhängigkeit vieler Funktionen von der Verfügbarkeit einer Reihe von zentralen Diensten Risiken mit sich.

Ein Beispiel für eine Lösung, die eine Trennung von Port-basierter Netzwerkzugangskontrolle und LAN-Benutzerverwaltung verfolgt, wäre die Verwendung von Tokens zur Anmeldung über IEEE 802.1X, und zwar gegen einen RADIUS-Server, der mit einer getrennten Datenbank zur Benutzerverwaltung zusammenarbeitet. Dies kann ggf. auch dieselbe Datenbank sein, welche für Firewall-basierende VPN oder RAS-Einwahl benutzt wird. Der Preis dieser Lösung ist allerdings dann meist die fehlende Möglichkeit für ein Single Sign-on, was Benutzer oft als unangenehm empfinden. Es bleibt in diesem Falle also bei dem oft zitierten Kompromiss zwischen Sicherheit und Komfort.

## 7.4 Bewertung und Zusammenfassung

Für den Nutzer von IEEE 802.11i, WPA oder WPA2 liegt die eigentliche Tücke in IEEE 802.1X verborgen. Über IEEE 802.1X werden Authentifizierung und Schlüsselmanagement abgewickelt. IEEE 802.1X ist allerdings „nur“ ein Authentifizierungs-Framework, das eine standardisierte Schnittstelle für ein Authenticator System (z. B. ein Access Point) spezifiziert, über welche die Authentifizierung zwischen Client (Supplicant in der Terminologie von IEEE 802.1X) und Authentication Server abgewickelt werden kann. Hierzu wird EAP, das eigentlich für PPP spezifiziert wurde, für die Anwendung im LAN (d. h. auf Layer 2) adaptiert.

Allerdings ist EAP ebenfalls ein Authentifizierungs-Framework. Die eigentliche Authentifizierung geschieht über eine sogenannte EAP-Methode, d. h. ein Authentifizierungsprotokoll, das sich an die Rahmenbedingungen von EAP hält. Bedingt durch gewisse organisatorische Schwächen in der Standardisierung konnte es bei den EAP-Methoden zu einem durchaus als kritisch einzustufenden Wildwuchs kommen. Eine Vielzahl von EAP-Methoden existieren, davon diverse ohne Nummer oder ohne offengelegte Spezifikation. Die wenigsten EAP-Methoden haben den Status eines RFC.

Für die Anwendung im WLAN ist zunächst essentiell, dass die EAP-Methode in der Lage ist, Schlüsselmaterial bereit zu stellen. EAP-MD5 fällt beispielsweise damit aus. Wird an die Authentifizierung die Forderung gestellt, dass beide Kommunikationspartner sich mit einem vergleichsweise hochwertigen Mechanismus gegenseitig authentifizieren, ist oft EAP-TLS die EAP-Methode der Wahl. Da die Authentifizierung über X.509-Zertifikate erfolgt, ist der Einsatz von EAP-TLS mit der Verfügbarkeit einer PKI verbunden.

Als Alternativen bieten sich mit Einschränkungen EAP-Methoden an, die zunächst einen äußeren Tunnel etablieren und im Schutz dieses Tunnels eine (ggf. schwächere) innere Authentifizierung des Clients durchführen. EAP-PEAP ist eine solche EAP-Methode. Diesem (und ähnlichen) Verfahren wird allerdings eine Anfälligkeit für MitM-Angriffe vorgehalten. EAP-FAST operiert zwar auch mit einem äußeren Tunnel und innerer Authentifizierung, baut jedoch den äußeren Tunnel auf eine andere Weise auf, die (zumindest nach dem heutigen Stand) keine Anfälligkeit MitM-Angriffen gegenüber zeigt.

Tabelle 3 zeigt zusammenfassend einige der für WLAN relevanten EAP-Methoden im Vergleich.

| EAP-Methode | LEAP | PEAP | EAP-TLS |
|---|---|---|---|
| Innere EAP-Methode | | MSCHAPv2 | |
| Single Sign-On (MS Active Directory) | ja | ja | ja |
| Passwortänderung innerhalb der Sitzung | nein | ja | nicht anwendbar |
| LDAP-Unterstützung | nein | nein | ja |
| Zertifikat für RADIUS-Server notwendig | nein | ja | ja |
| Client-Zertifikat notwendig | nein | nein | ja |
| Anfälligkeit gegenüber Dictionary-Attacken | ja | nein | nein |
| Anfälligkeit gegenüber MitM-Attacken | nein | ja | nein |
| Aufwand von Planung und Implementierung | niedrig | mittel | "hoch" |

Tabelle 3: Exemplarischer Vergleich von EAP-Methoden[27]

[27] Die Wertung „hoch“ für EAP-TLS in der Tabelle ist mit Absicht in Anführungszeichen gesetzt worden. Es ist zwar unbestreitbar, dass die Anfangsphase des Aufbaus einer PKI mit einem gewissen Aufwand verbunden ist. Ist aber diese Infrastruktur schon vorhanden (z. B. weil sie für den Remote-Zugang per VPN implementiert wurde), kann sich der Aufwand für die Umsetzung von EAP-TLS durchaus als niedrig erweisen.

# 8 Kombination und Koexistenz von Sicherheitsmechanismen

Es ist in der Praxis oft nicht möglich, ein WLAN mit einer einzelnen spezifischen Technik zu schützen. Man ist dann gezwungen, mehrere Techniken geeignet zu kombinieren bzw. eine Koexistenz verschiedener Techniken zu gestatten.

Typische Gründe hierzu sind:

- **Heterogene Client-Landschaften:**

  Die Einsetzbarkeit von Sicherheitsmechanismen wie WPA oder VPN ist auch durch die verwendeten Client-Betriebssysteme bestimmt. Oft ist es sogar so, dass eine gewisse WLAN-Funktion zunächst in Access Points zur Verfügung gestellt wird und erst später für Clients. Dabei werden Betriebssysteme meist gemäß ihrer Verbreitung unterstützt. Für gewisse Betriebsysteme bzw. Versionen kann es passieren, dass eine Funktion erst sehr spät oder sogar nie umgesetzt wird. Als Beispiel sei hier DOS erwähnt. Dieses Betriebssystem ist aus dem Büroalltag bereits seit einigen Jahren verschwunden. Trotzdem gibt es in den Bereichen Produktion und Logistik noch auf DOS basierende Entwicklungen und zugehörige Produkte. Für DOS gibt es allerdings weder einen Supplicant für IEEE 802.1X noch Aktivitäten zur Unterstützung von WPA.

- **Nutzer- und Anwendungsgruppen mit unterschiedlichen Sicherheitsanforderungen:**

  Das nutzbare Frequenzspektrum für ein Funksystem ist generell eine knappe Ressource. Für flächendeckende WLAN wird daher oft eine physikalische WLAN-Infrastruktur geschaffen, die gemeinsam von allen Parteien genutzt wird. Dabei kann es durchaus vorkommen, dass auf der gemeinsamen Infrastruktur unterschiedliche Sicherheitsanforderungen zu berücksichtigen sind. Dies ist beispielsweise der Fall, wenn auf einer WLAN-Infrastruktur neben dem Zugriff für Mitarbeiter auf interne Ressourcen auch die Möglichkeit bestehen soll, Gästen einen eingeschränkten Zugang (etwa zum Internet) zu liefern.

- **Migration von einer Sicherheitstechnik zu einer anderen:**

  Im Rahmen einer Migration zu einer anderen Technik zur Absicherung eines WLAN muss in den allermeisten Fällen für einen gewissen Zeitraum ein Parallelbetrieb von alter und neuer Technik möglich sein. Nicht selten bedeutet dies eine längere Koexistenz einer vergleichsweise unsicheren mit einer sichereren Technik.

Diese Aspekte führen automatisch in die Thematik der Trennung unterschiedlicher Benutzergruppen im WLAN, die in Kapitel 8.1 diskutiert wird. Dass sich WEP, Firewall-Techniken und VPN durchaus positiv ergänzend kombinieren lassen, wird in Kapitel 8.2 beschrieben. Allerdings werden Produkte nach WPA bzw. IEEE 802.11i vermehrt eingesetzt. Mit der Koexistenz zu anderen Techniken sind hier jedoch spezielle Probleme verbunden, die insbesondere eine Migration zu IEEE 802.11i bzw. WPA erschweren (siehe Kapitel 8.3).

## 8.1 Trennung von Benutzergruppen

Grundsätzlich kann die Trennung von Benutzergruppen auf der physikalischen Ebene, auf Layer 2 oder auf Layer 3 und höher stattfinden. Die Trennung von Nutzergruppen oberhalb von Layer 2 führt zwangsläufig zu VPN-Techniken, ggf. in Kombination mit Firewall-Mechanismen, wie sie bereits diskutiert wurden. Daher werden im Folgenden lediglich die Trennung auf Layer 1 und auf Layer 2 betrachtet.

### 8.1.1 Trennung auf physikalischer Ebene

Einem Access Point wird genau eine Benutzergruppe zugeordnet, die dann über den SSID identifiziert wird[28].

Die Trennung im Bereich des Distribution Systems erfolgt entweder über physikalisch getrennte LAN (d. h. es wird pro Nutzergruppe ein eigenes Distribution System realisiert), oder sie erfolgt über unterschiedliche VLAN auf einer physikalischen LAN-Infrastruktur.

Nachteilig wirken sich die Kosten dieser Lösung aus, da für jede Nutzergruppe eigene Access Points beschafft werden müssten.

Vorteilhaft bei der Trennung auf physikalischer Ebene erscheint zunächst die Tatsache, dass die Trennung vollständig geschieht. Leider wird dieser Vorteil durch das Shared Medium Funk und durch die verfügbare Bandbreite relativiert:

Eine Trennung auf physikalischer Ebene erfordert eine genügende Anzahl von überschneidungsfreien Kanälen, sofern keine geografische Trennung zwischen den Benutzergruppen vorgenommen werden kann. Dies setzt der Skalierbarkeit einer solchen Lösung erhebliche Grenzen.

Bei DSSS und OFDM bei 2,4 GHz besteht das Problem, dass die Bandbreite eines Systems lediglich drei interferenzfreie Systeme (konfiguriert auf die Kanäle 1-7-13 bzw. für FCC-Adapter auf 1-6-11) an einem Ort erlaubt. Weiterhin muss beachtet werden, das bei 2,4 GHz der genutzte Frequenzbereich ein ISM-Band ist. Störungen durch fremde Systeme (z. B. Bluetooth, Bewegungsmelder oder Mikrowellenherde) oder andere WLAN können hier nicht ausgeschlossen werden.

Eine Lösung zur Trennung zweier Benutzergruppen auf physikalischer Ebene mit nur drei überschneidungsfreien Kanälen bei 2,4 GHz ist nicht zu empfehlen, da die Gesamtverfügbarkeit des WLAN auf diese Weise gesenkt wird. Erst der Einsatz von IEEE 802.11a/h in Kombination mit IEEE 802.11b/g erlaubt eine bessere physikalische Trennung von Nutzergruppen, da mit reinem IEEE 802.11a weitere vier und mit IEEE 802.11h sogar bis zu 19 weitere Kanäle zur Verfügung stehen.

Der Standard IEEE 802.11h wurde im September 2003 verabschiedet, und seit Frühjahr 2005 zertifiziert die Wi-Fi Alliance auch Produkte nach IEEE 802.11h.

### 8.1.2 Trennung auf Layer 2

Der Grundgedanke bei der Trennung auf Layer 2 ist der Aufbau einer flächendeckenden Infrastruktur, die für alle Nutzergruppen gemeinsam genutzt wird. Die Trennung der Nutzergruppen erfolgt dann je nach Lösung bereits logisch auf der Luftschnittstelle bzw. im Access Point oder sogar erst im Distribution System.

Folgende Alternativen sind technisch möglich:

- **Dynamische VLAN-Zuweisung in Switches des Distribution Systems**: Diese Funktion wird von manchen Herstellern von Switches angeboten. Hierbei wird die VLAN-Zugehörigkeit anhand der Quell-MAC-Adresse eines Pakets, welches an einem Port anliegt, bestimmt. Dabei wird, neben den Ports an denen das VLAN möglich sein soll, eine Tabelle mit denjenigen MAC-Adressen angegeben, die zu diesem VLAN gehören.
- **Policy-based VLAN-Zuordnung mit IEEE 802.1X**: Über IEEE 802.1X kann prinzipiell auch die VLAN-Zugehörigkeit eines Clients in Abhängigkeit der gewählten Authentifizierungsmethode bestimmt werden. Ob und wie WLAN-Ausrüster diese Funktion im Rahmen von WPA implementieren werden, ist zur Zeit noch nicht bekannt.

[28] Genauer gesagt: Einem Radioteil im Access Point wird eine Benutzergruppe zugeordnet, da manche Hersteller den Einbau von zwei Radioteilen unterstützen.

- **Wireless VLAN durch SSID-VLAN-Mapping**: Auf einem Access Point werden mehrere SSIDs konfiguriert. Jeder SSID kann von einem Client in einem Probe Request angefragt werden, und eine Assoziation mit dem Access Point erfolgt ohne Änderung gemäß IEEE 802.11. Im Access Point gibt es eine durch den Administrator spezifizierte Tabelle, welche die Zuordnung zwischen SSID und VLAN ID vornimmt. Typischerweise können so maximal 16 Wireless VLAN konfiguriert werden. Dem Broadcast SSID entspricht meist das Default VLAN (ID 1). Auf dem Ethernet Port des Access Points findet dann VLAN Tagging statt. Abbildung 29 illustriert das Prinzip. Jedem SSID (und damit jedem VLAN) können eigene Sicherheitseinstellungen, d. h. Authentifizierung und Verschlüsselung, zugewiesen werden. Dieser Mechanismus eines Wireless VLAN ist bereits von einigen Herstellern implementiert worden.

Bis auf die VLAN-Zuordnung über IEEE 802.1X handelt es sich bei den drei Alternativen um herstellerspezifische Techniken. Dies betrifft entweder die Access-Point-Infrastruktur bei Wireless VLAN oder die (Access) Switches im Distribution System.

Bei der Gestaltung des Distribution System muss die Entscheidung getroffen werden, wo die verschiedenen VLAN wieder entkoppelt werden. Aus der Sicherheitsperspektive sollte eine frühzeitige physikalische Entkopplung auf separate LAN-Komponenten in Betracht gezogen werden[29]. Je nach Sicherheitsanforderung kann dies bereits im Distribution System (ggf. sogar am Access Switch) oder erst in dem Netzelement geschehen, das den Abschluss des Distribution System und den Übergang zur weiteren LAN-Infrastruktur bildet.

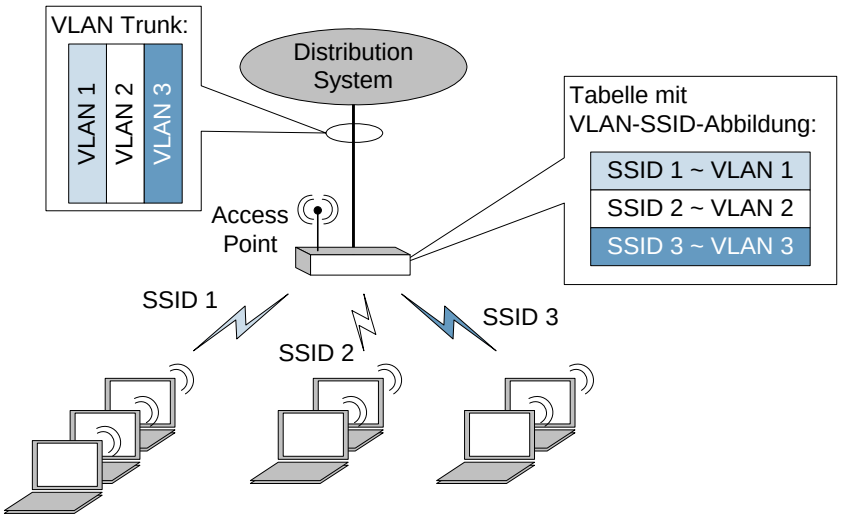



Abbildung 29: Prinzip der Wireless VLAN

## 8.2 Kombination von WEP, Firewall-Techniken und VPN

Ein IP-VPN ist zum Schutz des WLAN-Zugangs nur geeignet, wenn die entsprechenden VPN-Clients für alle (jetzt und künftig) eingesetzten Client-Systeme verfügbar sind. Diese Methode ist daher nicht allgemein anwendbar für heterogene Client-Landschaften, in denen Clients eingesetzt werden, die lediglich WEP unterstützen.

29 Das IT-Grundschutzhandbuch (siehe [GSHB04]) bemerkt in diesem Zusammenhang im Gefährdungskatalog unter G.298 zur Sicherheit von VLAN unter anderem: „VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind."

Eine solche Lösung ist generell nicht erstrebenswert. Auf der Luftschnittstelle ist die WEP-basierte Kommunikation schließlich nach wie vor angreifbar.

Wie bereits erwähnt, gibt es allerdings in der Praxis Rahmenbedingungen, die zu einem (temporären) Mischbetrieb führen können. In diesem Fall findet man oft eine Architektur, die eine Kombination aus dem Firewall-basierten Ansatz und einer VPN-Lösung darstellt und so zwei Benutzergruppen auf einer gemeinsamen WLAN-Funkabdeckung realisiert. Der Grundgedanke ist dabei recht einfach: Nur Verkehr, der über das VPN-Gateway zum LAN fließt, erhält uneingeschränkten Zugang, da am VPN-Gateway eine entsprechend starke Authentifizierung von Client bzw. Nutzer möglich ist. Der gesamte andere Verkehr erhält nur Zugriff auf dedizierte Dienste und Server (hier muss natürlich wieder der Schutz auf Server- und Anwendungsebene greifen). Abbildung 30 zeigt dieses Konzept am Beispiel von IPSec. Ein interessanter Seiteneffekt ergibt sich bei der Nutzung von Wireless Switches. Typischerweise unterstützen diese Wireless Switches eine VPN-Gateway-Funktion.

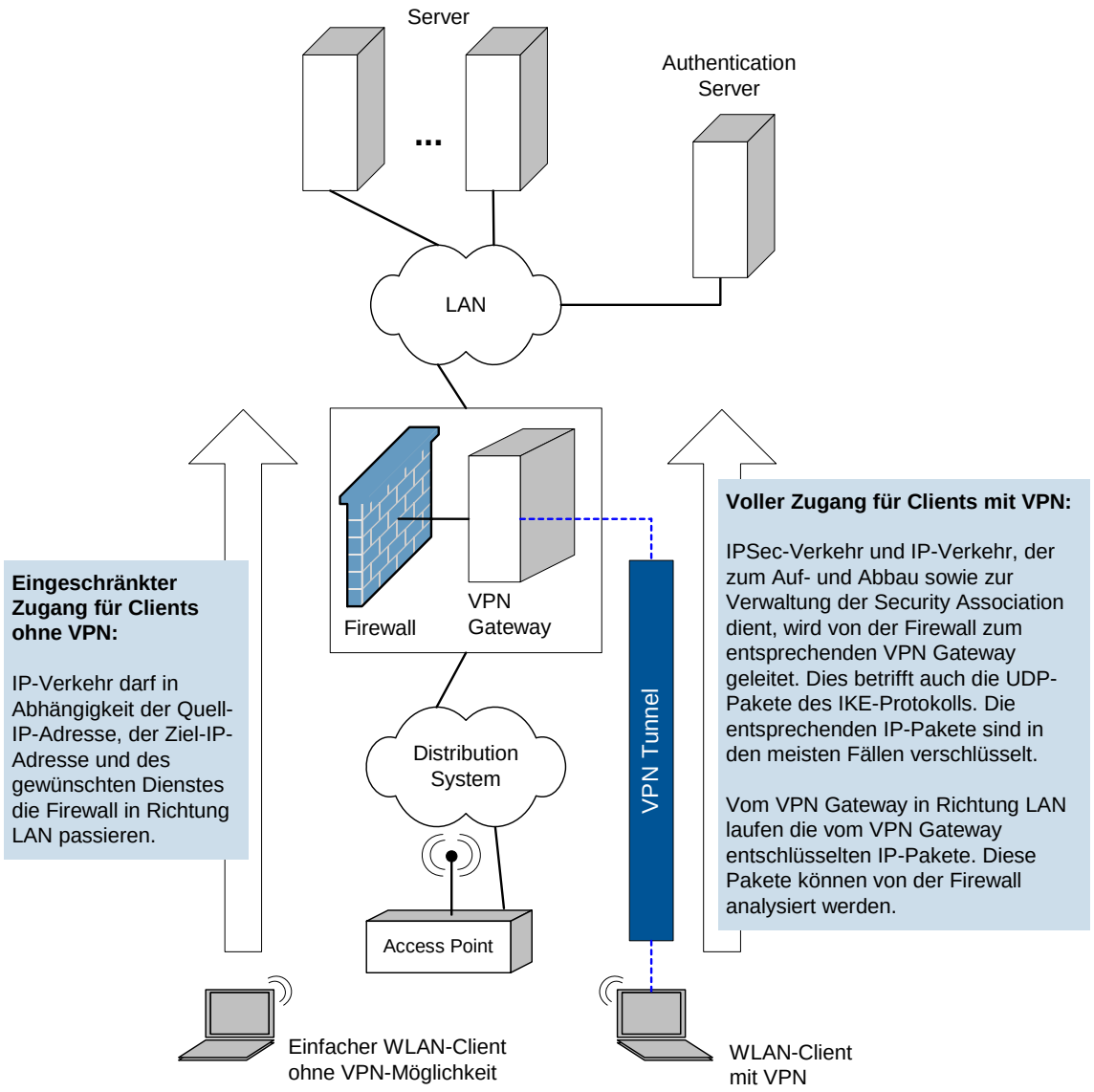



Abbildung 30: Realisierung von zwei Nutzergruppen mit unterschiedlichen Zugriffsrechten mit einem IP-VPN am Beispiel von IPSec

Diese Kombination eignet sich beispielsweise für Szenarien, die flächendeckend für Produktions- und Logistikanwendungen eine WLAN-Infrastruktur vorsehen, die auch für Büroanwendungen genutzt werden soll.

## 8.3 Migration zu WPA und IEEE 802.11i

Die Migration eines bestehenden WLAN zu WPA bzw. IEEE 802.11i sollte nach Möglichkeit in einem Schritt geschehen. Ist dies nicht möglich, muss für den Migrationszeitraum eine Koexistenz bisheriger Sicherheitsmechanismen und WPA bzw. IEEE 802.11i möglich sein. Je nach verwendeten Client-Systemen muss in manchen Fällen hier ein vergleichsweise großer Zeitraum kalkuliert werden.

Im Folgenden wird von WPA bzw. IEEE 802.11i unter Verwendung von IEEE 802.1X ausgegangen, d. h. Pre-Shared Keys werden nicht unmittelbar berücksichtigt.

Die zentrale Forderung ist zunächst: Die eingesetzten Access Points müssen auf der Luftschnittstelle einen Mischbetrieb von IEEE 802.11i und dem bisherigen Sicherheitsmechanismus (z. B. WEP) unterstützen. Ein WLAN, das einen solchen Mischbetrieb gestattet, wird in IEEE 802.11i als Transition Security Network (TSN) bezeichnet.

Das Problem in diesem Mischbetrieb liegt vereinfacht in der Tatsache, dass ohne weitergehende Maßnahmen keine signifikant höhere Sicherheit im WLAN erreicht wird, solange noch ein einziger nicht migrierter Client im Netz ist. In diesem Sinne ist das Erreichen eines höheren Sicherheitsniveaus durch IEEE 802.11i eine „Alles-oder-Nichts-Situation“.

Die Ursache ist die fehlende Unterstützung der Trennung von Benutzergruppen auf der Luftschnittstelle und im Distribution System.

Zur Illustration des Problems sei angenommen, dass ein WLAN mit WEP auf WPA migriert werden soll. Die entsprechenden Access Points werden aufgebaut und für den Mischbetrieb konfiguriert.

Auf der Luftschnittstelle ist die WEP-basierte Kommunikation natürlich nach wie vor angreifbar, die WPA-Kommunikation jedoch nicht (eine hochwertige Authentifizierung bzw. strenge Password Policy vorausgesetzt). Die WEP-Nutzergruppe darf weiterhin nur auf dedizierte Dienste und Ziele über eine Firewall zugreifen. Weiterhin sei nun angenommen, dass alle Server, die über WEP erreichbar sind, geeignet gehärtet wurden und auf Anwendungsebene keine Angriffsmöglichkeiten bestünden. Es wäre nun ein Fehler, den WPA-Nutzern einfach einen freien Zugang zur Infrastruktur zu erlauben. Da beide Nutzergruppen lediglich auf der Luftschnittstelle unterschieden werden und ihre Pakete in das Distribution System ohne weitere Trennung gelassen werden, kann eine Firewall nachträglich nicht verlässlich unterscheiden, wer zu welcher Gruppe gehört. Würde beispielsweise die Quell-IP-Adresse als Kriterium genutzt, um zu entscheiden, ob ein Client als WPA-Nutzer freien Zugang oder als WEP-Client eingeschränkten Zugang erhält, so könnte ein Angreifer versuchen, den Layer-2-Kontext eines WEP-Clients zu stehlen, um Zugang zum Distribution System zu erlangen und den IP-Kontext eines WPA-Clients zu nehmen, um trotz Firewall freien Zugang zur LAN-Infrastruktur zu erhalten.

Um diesem möglichen Angriff geeignet begegnen zu können, muss die Nutzergruppe, zu der ein Client gehört, über den Access Point hinaus auch im Distribution System bekannt sein, d. h. eine Nutzergruppentrennung auf Layer 2 ist notwendig.

Mit dieser Thematik beschäftigte sich Kapitel 8.1. Dieses Problem gilt auch bei Migration eines WLAN mit WEP-Verschlüsselung und sogar bei einem WLAN, das mit einem VPN abgesichert ist, und zu IEEE 802.11i migriert wird. Abbildung 31 zeigt eine typische Migrationsarchitektur, die sich generell auch für eine Koexistenz zwischen IEEE 802.11i und anderen Sicherheitsmechanismen eignet. Dabei werden die verschiedenen Nutzergruppen auf Wireless VLAN abgebildet. Ein Wireless VLAN erlaubt lediglich den Zugang über IEEE 802.11i und wird von den Clients genutzt, die schon zu IEEE 802.11i migriert wurden. Ein anderes Wireless VLAN wird den „alten“ noch nicht migrierten Clients zugeordnet. Gegebenenfalls sind noch weitere Nutzergruppen (beispielsweise Gäste) zu berücksichtigen. Die Wireless VLAN werden mit den jeweiligen Sicherheitseinstellungen für die betei-

ligten Nutzergruppen auf den Access Points konfiguriert. Im Laufe der Migration wird das Wireless VLAN für die „Altlasten“ immer weniger genutzt, bis es schließlich aus der Konfiguration entfernt werden kann. An dieser Stelle sei aber nochmals darauf hingewiesen, dass eine solche Architektur, die einen Mischbetrieb verschiedener Sicherheitsmechanismen im WLAN gestattet, nur als Notlösung verstanden werden sollte. Dabei sind die Dauer dieses Mischbetriebs und das während der Migrationsphase akzeptable Sicherheitsniveau entscheidend für die Sicherheitsmaßnahmen, die während der Migrationsphase greifen müssen. Nach Möglichkeit sollte eine homogene Struktur, die ein WLAN konsistent z. B. mit IEEE 802.11i absichert, angestrebt werden.

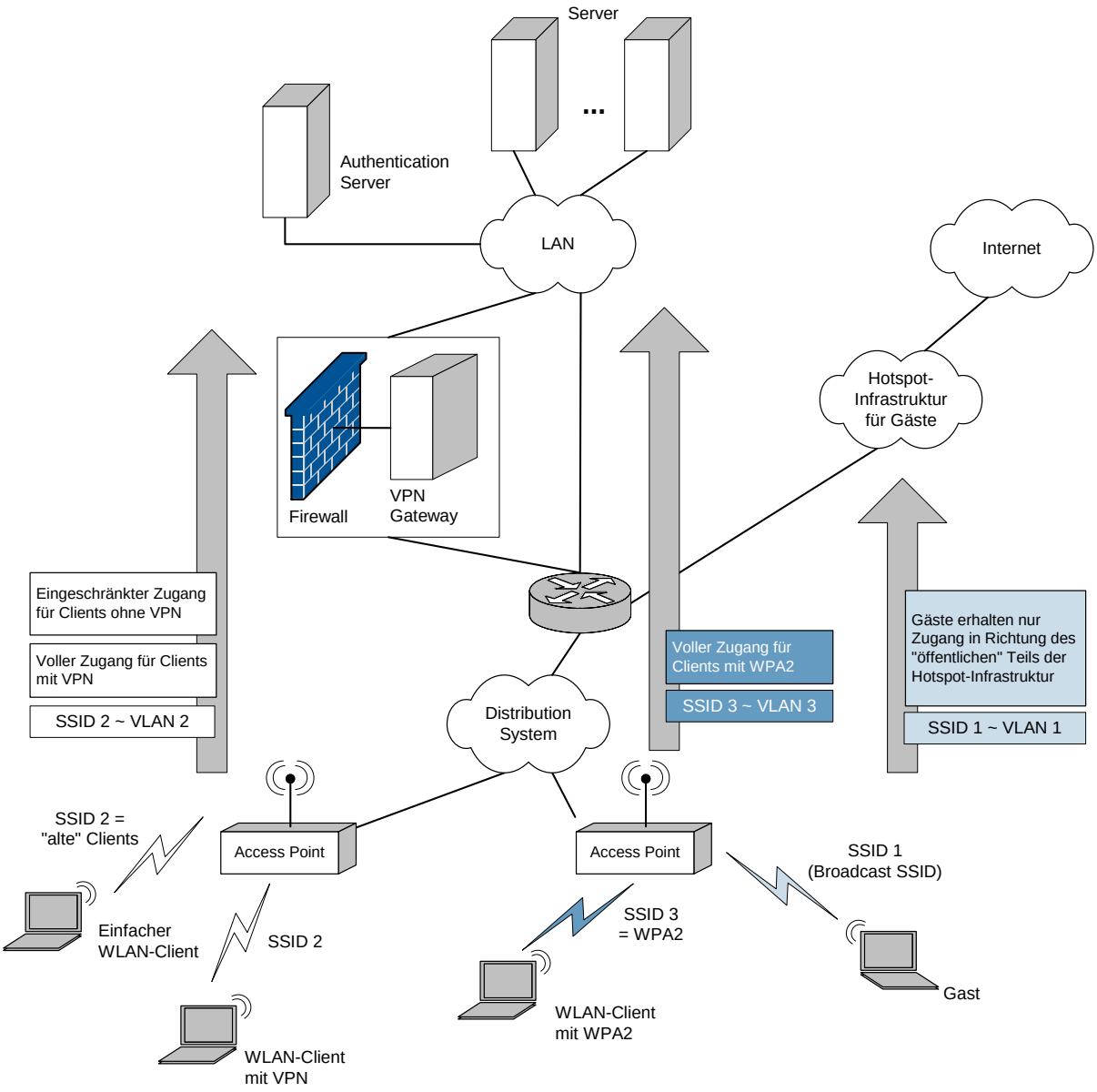



Abbildung 31: Migrationsarchitektur unter Verwendung von Wireless VLAN

# 9 Auswirkungen der Mobilität auf die Sicherheitsinfrastruktur

Die Sicherheitsinfrastruktur in einem WLAN muss auch auf die mobilitätsspezifischen Eigenheiten in einem WLAN abgestimmt sein. Dies betrifft die folgenden Funktionen:

- Layer 2 Roaming: Hier ist der zusätzliche Aufwand durch eine erneute Authentifizierung am Access Point zu berücksichtigen. Dieser zusätzliche Aufwand verlängert die Zeit, die während des Zellwechsels nicht zur Übertragung von Nutzdaten zur Verfügung steht. Je nach Anwendung, z. B. bei der Sprachübertragung, können diese Totzeiten als unangenehm empfunden werden. Diese Aspekte und insbesondere das Inter Access Point Protocol wurden bereits in Kapitel 6 diskutiert.
- Layer 3 Roaming: Wird das Distribution System als geswitchtes Layer-3-Netz derart aufgebaut, dass benachbarte Access Points zu unterschiedlichen IP-Subnetzen gehören, müssen beim Zellwechsel zusätzliche Effekte auf Layer 3 beachtet werden, die in Kapitel 9.1 erörtert werden.
- Roaming zwischen WLAN-Installationen: Das WLAN muss hier mit Besuchern (etwa von einem anderen Standort) umgehen. Dabei geht es primär um die Frage der Authentifizierung, da im besuchten WLAN zunächst nicht automatisch davon ausgegangen werden kann, dass in den lokalen Benutzerdatenbanken der Besucher mit seinen zugehörigen Authentifizierungsinformationen verzeichnet ist. Diesen Aspekt betrachtet Kapitel 9.2.

## 9.1 Mobilität auf Layer 3

Aus einer Sicherheitsperspektive ist die Strukturierung des Distribution Systems in mehrere Broadcast-Domänen bzw., äquivalent hierzu formuliert, das transparente Roaming zwischen Distribution Systems auf Layer 3 aus den folgenden Gründen von Interesse:

- Die Verkleinerung der Broadcast-Domänen verringert das Risiko einer zu großen Broadcast-Last. Zusätzlich können zuverlässige Redundanzmechanismen mit schnellen Failover-Zeiten (z. B. OSPF) eingesetzt werden. Beides wirkt sich positiv auf die Verfügbarkeit aus.
- Das Versorgungsgebiet kann durch mehrere IP-Subnetze geografisch strukturiert werden und durch eine entsprechende Auswahl und Konfiguration des Routing-Protokolls können Verkehrsflüsse gelenkt und kontrolliert werden. Dies schränkt die potentielle Angriffsfläche im WLAN im Sinne der über das WLAN erreichbaren Ziele ein.

Hierfür steht allerdings nur eine ausgesprochen limitierte Anzahl möglicher Techniken zur Verfügung. Zu nennen sind der Einsatz von DHCP, von Mobile IP bzw. von spezifischen Tunnelmechanismen (typischerweise eine Funktion von sogenannten Wireless Switches).

### 9.1.1 Offline-Mobilität mit DHCP

Geschieht beim Handover im WLAN ein Wechsel von einem IP-Subnetz in ein anderes, so ist damit zumindest die Vergabe einer neuen IP-Adresse und der Verlust aller Kommunikationsbeziehungen, die mit der bisherigen IP-Adresse verknüpft waren, wie z. B. TCP-Verbindungen, verbunden (Abbildung 32).

Manche Betriebssysteme (bzw. deren Implementierung des IP-Protokoll-Stacks) sind in der Lage, einen solchen Wechsel des IP-Subnetzes festzustellen und durch einen DHCP-Request einen neuen IP-Kontext aufzubauen. Manche Anwendungen benötigen keine permanente TCP-Verbindung, sondern bauen sie bei Bedarf auf (z. B. Web-Browser) und würden daher den Subnetzwechsel im WLAN unter Umständen nicht bemerken.

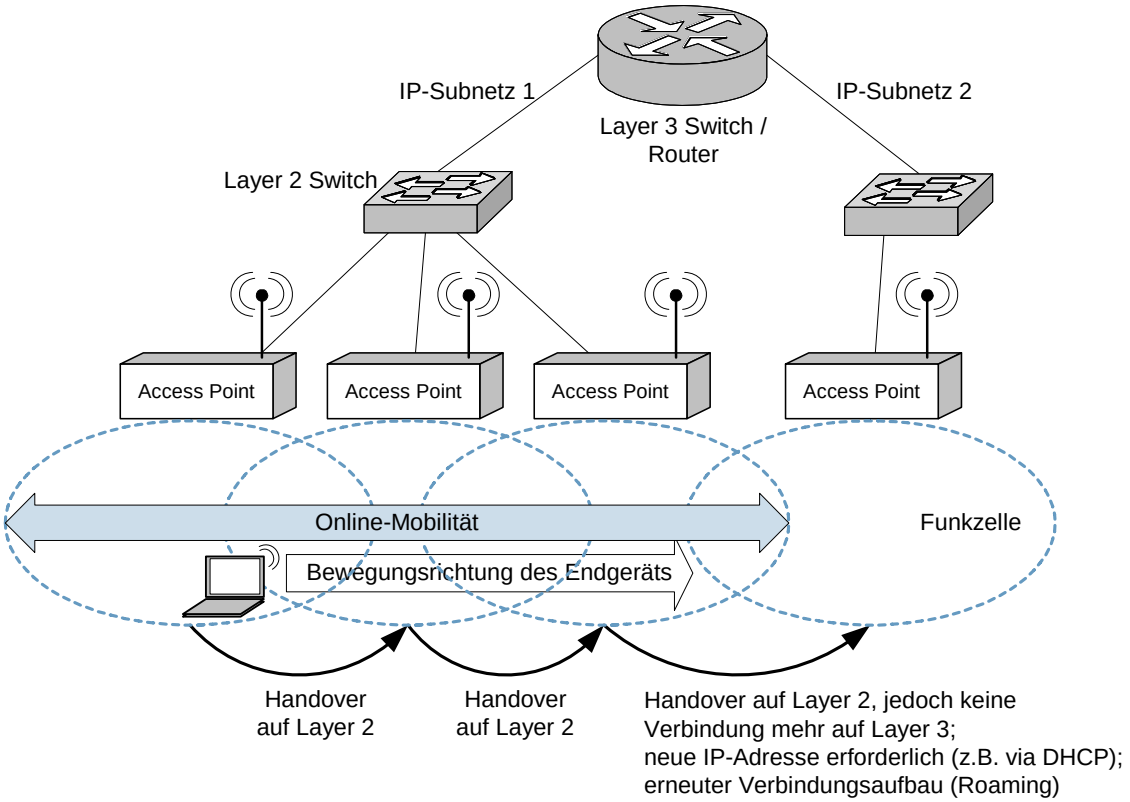



Abbildung 32: Problematik beim Handover in ein anderes IP-Subnetz

Allerdings ist nicht jede Anwendung in der Lage, automatisch eine neue TCP-Verbindung unter einer neuen IP-Adresse aufzubauen. Außerdem sind in diversen WLAN im Bereich der Produktion und der Logistik oft Clients im Einsatz, die per statischem DHCP stets eine feste IP-Adresse erhalten bzw. nicht DHCP-fähig sind.

Solange der Client beim Handover in einer Broadcast-Domäne bleibt, kommt es auch nicht zu den skizzierten Problemen. Dies ist der Hauptgrund, warum das Distribution System oft als flaches Layer-2-Netz aufgebaut wird.

### 9.1.2 Mobile IP

Mobile IP erhält automatisch die Erreichbarkeit des Clients unter einer einzigen IP-Adresse auch bei einem IP-Subnetzwechsel aufrecht. Die IP-Pakete zu einem mobilen Client werden dabei zunächst zum Heimatnetz des mobilen Clients geroutet und von dort zum aktuellen Aufenthaltsort getunnelt (siehe Abbildung 33). Das Prinzip ist also ähnlich zu einer Rufumleitung, wie man sie von ISDN her kennt. Damit wird theoretisch eine Online-Mobilität auf Layer 3 erreicht. So einfach sich diese Funktion auch anhört, Mobile IP für IPv4 ist ein aufwändiger Mechanismus, verbunden mit komplexen Protokollen und vielen Sonderfällen (siehe [MIP02]. Außerdem kann die Anwendung eines IP-VPN über Mobile IP zu technischen Problemen führen. Dies gilt auch für die Verwendung von DHCP. In vielen Fällen fehlt auch der Support von Mobile IP auf der Client-Seite[30].

[30] Mobile IP wird beispielsweise **nicht** von Microsoft Windows 2000 und Windows XP unterstützt.

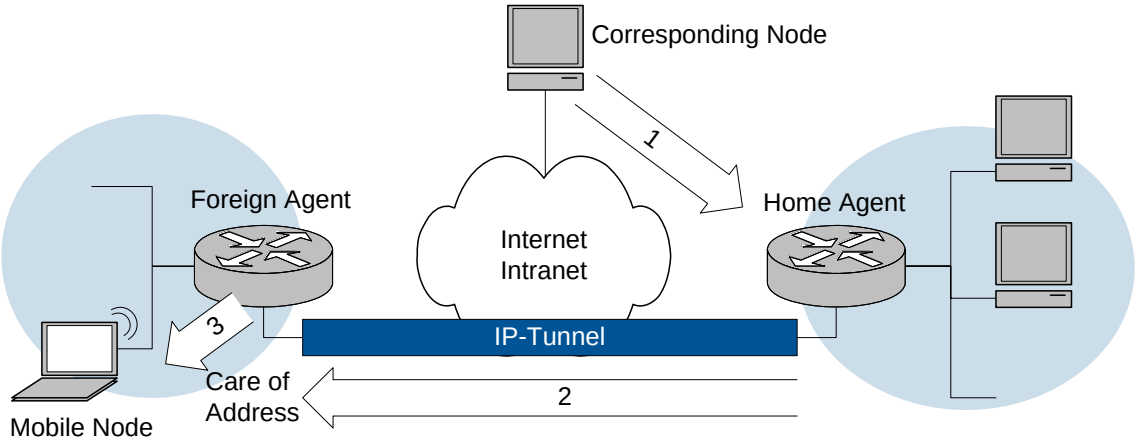



Abbildung 33: Routing zu mobilen Endgeräten mit Mobile IP

Manche Access Points unterstützen Proxy Mobile IP. Hiermit ist die Client-seitige Verfügbarkeit einer Mobile-IP-Implementierung nicht mehr erforderlich, da der Access Point stellvertretend für den Client diese Aufgabe erledigt.

Die Konfiguration von (Proxy) Mobile IP ist sehr aufwändig und gerade bei sehr großen WLAN-Installationen mit einer entsprechenden Anzahl von Clients, die sich außerhalb ihres Heimat-Netzes befinden, besteht die Gefahr, dass die eingesetzten Mechanismen (z. B. Tabellen zur Verwaltung des Aufenthaltsorts sowie der Auf-, Abbau und Verwaltung der Tunnel) einen nicht unerheblichen Einfluss auf die Leistung haben.

In der Praxis sind WLAN-Installationen mit einem Distribution System basierend auf Mobile IP sehr selten anzutreffen. Trotzdem kann das generelle Konzept von Mobile IP als wesentlicher Ideenlieferant für die im Folgenden beschriebenen Wireless Switches angesehen werden.

### 9.1.3 Spezifische Tunnelmechanismen und Wireless Switches

Wireless Switches sind ein Sammelbegriff, unter dem Netzelemente verstanden werden, die zusätzliche Mobilitäts- und WLAN-spezifische Funktionen enthalten.

Wireless Switches sind proprietär und noch nicht in der WLAN-Standardisierung des IEEE berücksichtigt.

Insbesondere lässt sich die weitere Entwicklung in diesem Segment noch nicht abschätzen.

Grundsätzlich sind zwei Architekturvarianten zu unterscheiden:

- **Gateway-Perspektive**: Die Wireless Switches bilden den Abschluss des Distribution Systems (Abbildung 34). Das Distribution System wird konventionell aus Layer 2 Switches aufgebaut, kann jedoch – je nach Hersteller – durchaus in mehrere IP-Subnetze strukturiert werden, die an den Wireless Switches zusammengeführt werden. Typischerweise realisiert ein Wireless Switch, der als Gateway ausgelegt ist, (rudimentäre) Firewall-Funktionen und kann als VPN-Gateway für verschiedene VPN-Techniken (Tunnelmechanismen, Verschlüsselungs- und Authentifizierungsmethoden) konfiguriert werden. Eine Verwaltung der verschiedenen Nutzergruppen wird hier typischerweise mit angeboten. Im Folgenden wird dieser Typ eines Wireless Switches auch als Mobility Gateway bezeichnet.

  Die Mobilität zwischen den IP-Subnetzen wird innerhalb eines Mobility Gateways abgehandelt (falls mehrere Distribution Systems an einem Gateway angeschlossen werden können) bzw. zwischen den Mobility Gateways durch Tunneltechniken realisiert. Diese Tunnel sind transparent für Clients, Access Points und das Distribution System. Es gibt auch Systeme am Markt, die einen Tunnel zwischen Mobility Gateway und Access Points etablieren.

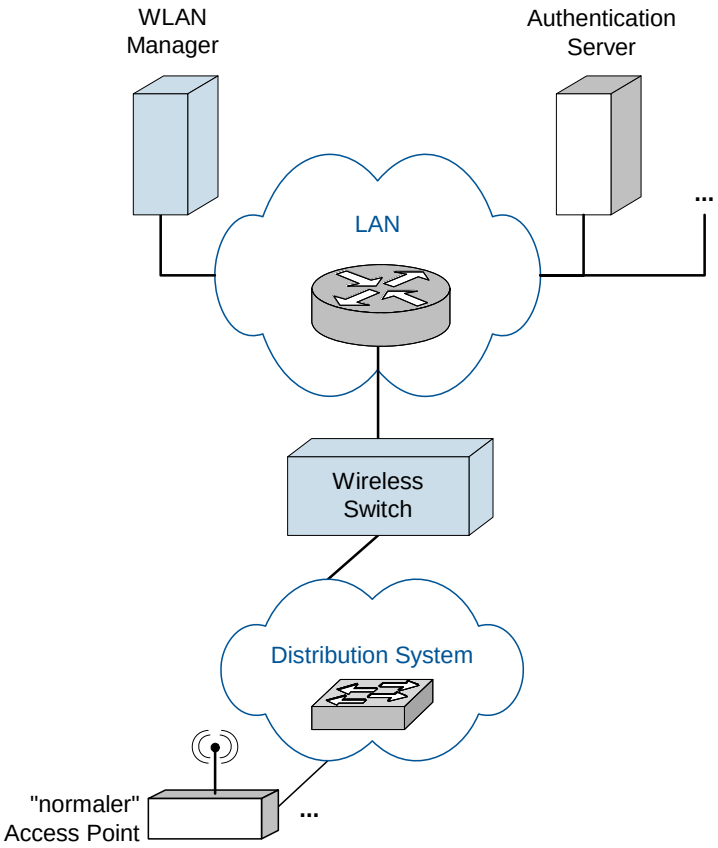



Abbildung 34: Wireless Switch aus der Gateway-Perpektive

- **Access-Switch-Perspektive**: Hier wird typischerweise ein konventioneller Access Switch um Mobilitäts- und WLAN-spezifische Funktionen erweitert. Access Points werden direkt an den Wireless Switch angeschlossen. Die WLAN-Switches bilden dabei das Distribution System (Abbildung 35). Einem WLAN-Switch kann (herstellerspezifisch) meist ein VLAN für Access Points zugeordnet werden. Jedem Wireless Switch entspricht so ein eigenes VLAN.

  Die Mobilität zwischen den VLAN wird durch Tunneltechniken realisiert, die transparent für den Client ablaufen. Wireless Switches gemäß der Access-Switch-Perspektive bieten üblicherweise Funktionen zum Management der angeschlossenen Access Points sowie Funktionen zur Überwachung der Luftschnittstelle hinsichtlich der Qualität der Übertragung und hinsichtlich Verletzungen einer WLAN Security Policy. Stichworte sind in diesem Zusammenhang die Erkennung fremder WLAN-Stationen und die Erkennung von Angriffen auf die Infrastruktur (Wireless IDS). Dieser Typ von Wireless Switches erfordert meist den Einsatz von Access Points, die speziell auf den Wireless Switch zugeschnitten sind. Access Points (oft mit einer neuen Bezeichnung versehen, wie „Mobility Point“ oder „Access Port“) und Wireless Switches kommen daher dann aus einer Hand. Da die Access Points Funktionen an den Wireless Switch abgeben, sind sie nicht mehr alleine lauffähig und werden daher oft auch als „Thin Access Point“ bezeichnet.

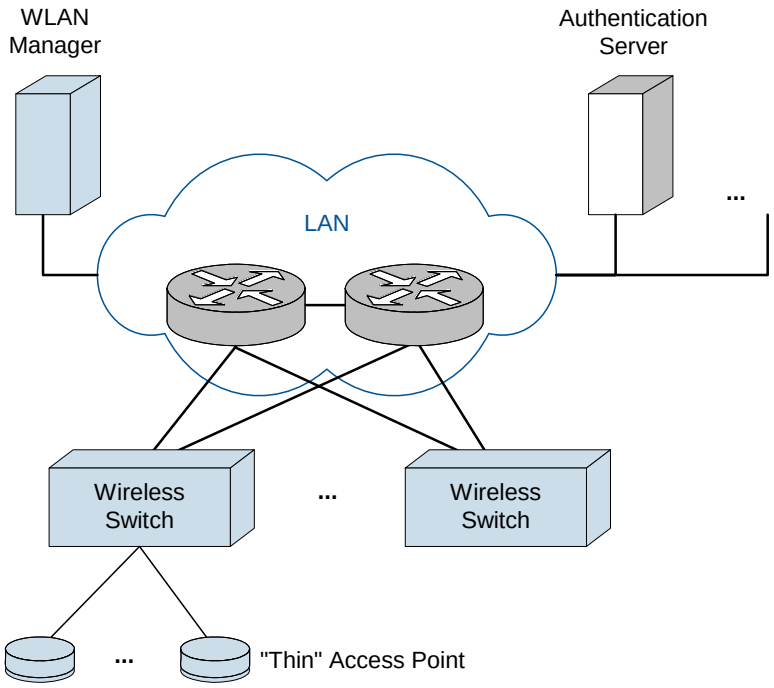



Abbildung 35: Wireless Switch aus der Access-Switch-Perspektive

## 9.2 Roaming zwischen WLAN-Installationen

Die Forderung der Unterstützung eines Roaming zwischen WLAN-Installationen hat im Vergleich die weitest reichenden Auswirkungen auf den Aufbau der WLAN-Sicherheitsinfrastruktur.

Folgendes Beispiel illustriert die typische Anwendung: Ein Gast von einem anderen Standort einer Behörde oder eines Unternehmens besucht die lokale Niederlassung. Der Gast erwartet, dass er über das WLAN in der lokalen Niederlassung zumindest auf seine heimatlichen Ressourcen zugreifen kann. Je nach verwendeten Sicherheitsmechanismen müssen nun spezifische Dinge bedacht werden, damit diesem Wunsch des Gasts ohne Probleme entsprochen werden kann. Kapitel 9.2.2 betrachtet hierzu die Aspekte, die bei einer MAC-Adressen-Authentifizierung zu beachten sind. Die Möglichkeiten bei Verwendung eines VPN werden in Kapitel 9.2.3 beschrieben. Abschließend wird die Palette der Probleme und Lösungsalternativen zur Unterstützung eines standortübergreifenden Roaming für IEEE 802.11i bzw. WPA analysiert.

### 9.2.1 Roaming und WEP

Sofern das symmetrische Verfahren WEP eingesetzt wird, ist es natürlich erforderlich, dass ein Client, der ein anderes WLAN besucht, den WEP-Schlüssel dieses besuchten WLAN kennt und der WEP-Schlüssel des besuchten WLAN auf dem Client-Adapter konfiguriert ist. Hierzu können auf den Clients typischerweise Profile angelegt werden, über die neben unterschiedlichen SSIDs auch unterschiedliche Schlüssel hinterlegt werden können. Das Roaming basiert dann je nach verwendetem Client-Adapter auf einer manuellen oder automatischen Auswahl eines passenden Profils.

### 9.2.2 Roaming und Authentifizierung über die MAC-Adresse

Ein Roaming eines Clients erfordert bei Verwendung einer RADIUS-basierten Authentifizerung von MAC-Adressen, dass der RADIUS-Server, der am entsprechenden Access Point eingetragen ist, die MAC-Adresse des Clients kennt. Hierzu müssen die MAC-Adressen der Besucher-Clients im zustän-

digen RADIUS-Server eingetragen werden. Je nach Implementierung der verwendeten RADIUS-Server kann der Verwaltungsaufwand durch Replikationsmechanismen reduziert werden. Alternativ kann man über die Schaffung eines zentralen standortübergreifenden RADIUS-Servers nachdenken. Unabhängig davon, welche Lösung gewählt wird, der Aufwand ist insbesondere dann erheblich, wenn standortübergreifend MAC-Adressen verwaltet werden müssen.

### 9.2.3 Roaming mit VPN

Bei der Verwendung eines VPN kann das standortübergreifende Roaming von Clients meist mit einem geringfügigen Aufwand realisiert werden.

Es ist im besuchten WLAN lediglich notwendig, dass sich der Client assoziieren darf und das im Client konfigurierte VPN-Gateway im Heimatnetz erreichen kann. Der Client baut dann im besuchten WLAN einfach einen VPN-Tunnel zum heimatlichen VPN-Gateway auf (Abbildung 36). Dem Client stehen so im besuchten WLAN genau die Kommunikationsmittel zur Verfügung, die er auch im Heimat-WLAN nutzen kann.

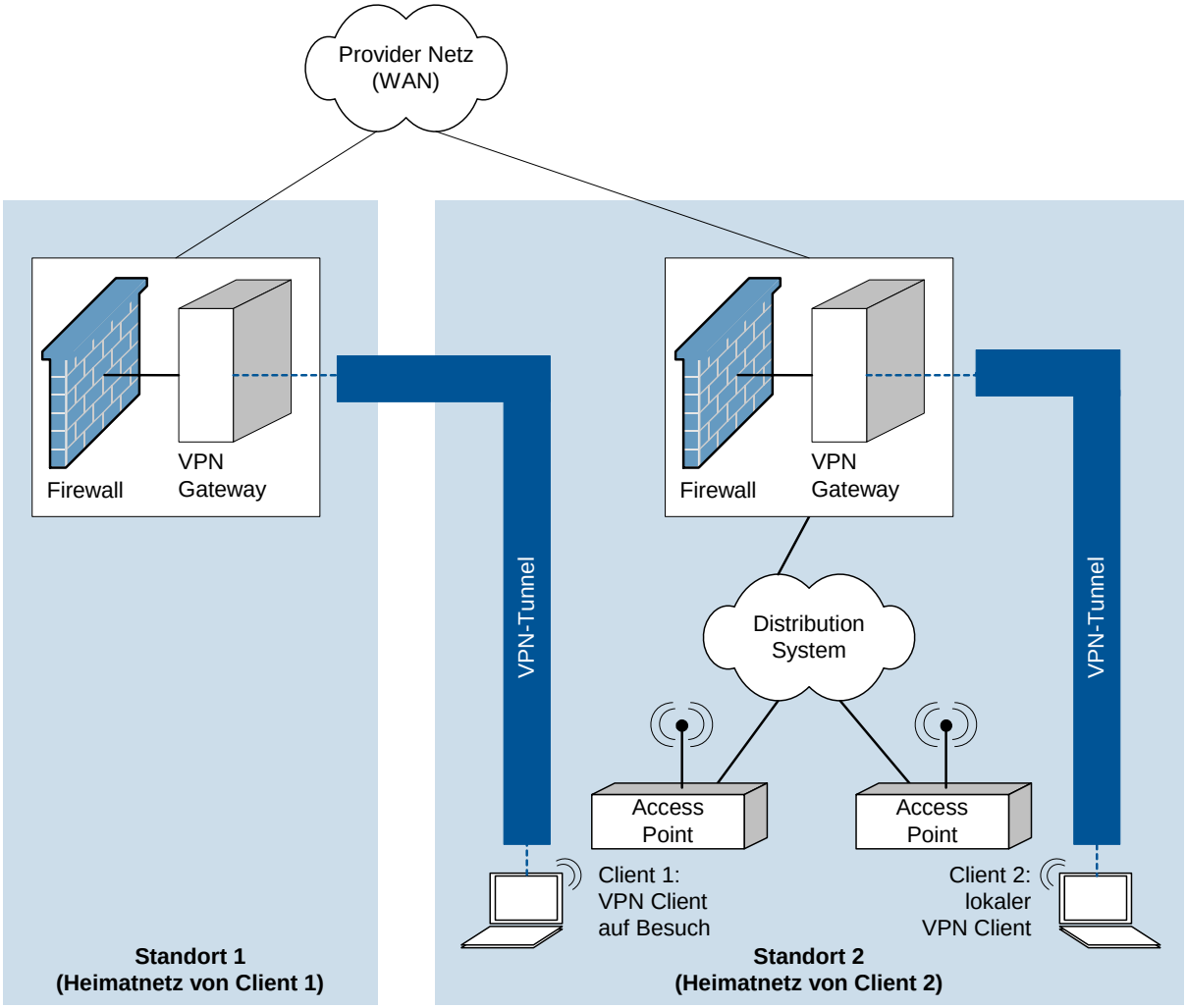



Abbildung 36: Roaming mit VPN

Die Authentifizierung des Clients erfolgt nach wie vor im Heimatnetz und das besuchte Netz erhält noch nicht einmal die Information, ob ein Authentifizierungsvorgang erfolgreich war. Im besuchten WLAN muss daher sichergestellt werden, dass Besucher-Clients lediglich ihr VPN-Gateway erreichen

können und nur VPN-Verkehr fließt. Hierzu kann ein Paketfilter eingesetzt werden, der wie in Kapitel 4.2 vorgestellt, das Distribution System terminiert. In diesem Paketfilter werden nun Regeln für die VPN-Gateways, zu denen Besucher einen Tunnel aufbauen können, eingepflegt. Vereinfacht kann eine solche Regel wie folgt aussehen:

> „Wenn (Destination IP-Adresse = VPN-Gateway im Heimat-WLAN) und (Service = IKE oder Service = IPSec), dann darf das Paket das Distribution System verlassen."

Je nach verwendeter VPN-Technik (z. B. bei IPSec) muss beachtet werden, dass auf der gesamten Strecke des VPN-Tunnels keine Network Address Translation (NAT) stattfindet, sofern nicht alle VPN Clients NAT Traversal unterstützen. Dies betrifft die Client-IP-Adressen außerhalb des Tunnels (d. h. im gesamten Transportnetz für das VPN).

Mit dieser Methode kann zwar auf die Ressourcen im Heimatnetz zugegriffen werden, ein Besucher kann aber nicht ohne weiteres auf die lokalen Ressourcen im besuchten Netz zugreifen. Dieser Effekt ist allerdings oft durchaus gewünscht.

### 9.2.4 Roaming mit IEEE 802.11i und WPA

Hier muss zunächst unterschieden werden, ob mit WPA-PSK oder mit IEEE 802.1X gearbeitet wird.

Bei der Verwendung von PSK erfordert ein Roaming natürlich, dass der Client-Adapter mit dem Schlüssel des besuchten Netzes konfiguriert wird. Je nach Supplicant können hierbei mehrere Profile unterstützt werden, die manuell von dem Nutzer ausgewählt werden.

Bei IEEE 802.1X stellt sich die Situation deutlich flexibler dar, allerdings müssen die Eigenheiten der verschiedenen EAP-Methoden beachtet werden. Aus dem Blickwinkel eines Roaming ist dabei zunächst wichtig, ob die Nutzerverwaltung auf dem Authentication Server geschieht oder ob zur Authentifizierung auch ein Directory Service genutzt wird.

Im ersteren Fall liegt eine ähnliche Situation wie bei der MAC-Adressen-Authentifizierung über RADIUS vor: Unabhängig vom Nutzer wird am Authenticator (d. h. am Access Point) die Adresse bzw. der Name des Authentication Servers konfiguriert. Die Authentifizierungsanfrage für einen Besucher im WLAN wird also zu einem Server geleitet, der zunächst den Besucher nicht kennt, denn die Authentifizierungsdaten für den Benutzer sind natürlich im heimatlichen Authentication Server zu finden. Auch hier gilt wieder, dass entweder der Gast manuell zusätzlich im Authentication Server des besuchten WLAN eingetragen wird oder eine Synchronisation bzw. Replikation zwischen den beteiligten Systemen diesen Prozess automatisiert. Alternativ kann natürlich auch der Aufbau eines zentralen Authentication Servers in Betracht gezogen werden, was allerdings mit gewissen Nachteilen verbunden ist. Eine zentrale Lösung muss die gesamte Authentifizierungsverkehrslast von allen beteiligten Standorten verkraften. Kommt es hier zu Engpässen, kann beispielsweise ein Handover signifikant verzögert werden. Weiterhin muss das Problem der Verfügbarkeit bedacht werden.

Wird ein Directory Service durch den Authentication Server in Anspruch genommen, um die notwendigen Informationen zu einem Nutzer zu erfragen, genügt es, wenn die beteiligten Standorte eine zusammenhängende Directory-Struktur aufgebaut haben. Über diesen Weg lässt sich beispielsweise auch eine standortübergreifende PKI realisieren, wie sie zur Unterstützung eines Roaming bei Verwendung von EAP-TLS erforderlich wäre.

In dem skizzierten Szenario dürfte der Besucher nach einer erfolgreichen Authentifizierung im besuchten WLAN dieselben Kommunikationsdienste nutzen, wie ein lokaler Nutzer. Es sind daher gegebenenfalls zusätzliche Mechanismen nötig, um die Rechte eines Besuchers wieder einzuschränken. Dies kann beispielsweise dadurch geschehen, dass der Besucher in ein spezifisches VLAN kommt, über das nur bestimmte Ziele erreichbar sind.

# 10 Management von WLAN aus der Sicherheitsperspektive

Wie im kabelgebundenen LAN ist ein zentrales Management der WLAN-Infrastruktur – insbesondere bei großen WLAN-Installationen – von entscheidender betrieblicher Bedeutung. Was die prinzipiellen betriebsorganisatorischen und architektonischen Rahmenbedingungen angeht, unterscheidet sich das Management im WLAN nicht von kabelgebundenen Systemen. So stellt sich auch im WLAN die wesentliche Aufgabe als ein Lifecycle Management mit den folgenden Disziplinen:

- Configuration Management und Change Management
- Fault Management
- Performance Management
- Security Management
- Accounting Management

Diese Disziplinen erstrecken sich nicht nur auf den Betrieb und das Management der Access Points, sondern es ist beim Management die gesamte Infrastruktur einer WLAN-Installation zu berücksichtigen. Hierzu zählen zunächst die Komponenten des Distribution-Systems, aber auch die zusätzliche WLAN-Sicherheitsinfrastruktur wie z. B. Authentication Server, Firewall-Systeme und VPN-Gateways. Für den Bereich der Luftschnittstelle ist speziell zu beachten, dass eine Überwachung sowohl aus der Perspektive der Access Points als auch aus der Client-Perspektive möglich ist. Schließlich darf die Verwaltung der Client-Systeme in einem geschlossenen Managementkonzept nicht vernachlässigt werden.

In den weiteren Betrachtungen in diesem Kapitel werden nur die WLAN-spezifischen Managementaufgaben betrachtet und zwar aus folgenden Gründen:

- Für das Distribution System besteht von einem Sicherheitsstandpunkt aus betrachtet kein Unterschied zum Management einer klassischen LAN-Infrastruktur.
- Zum Management von Sicherheitskomponenten (z. B. RADIUS-Server) sind entsprechende Betriebs- und Managementkonzepte vorhanden, die in der Regel auf die WLAN-Sicherheitsinfrastruktur übertragen werden können.
- Schließlich stellt die Verwaltung der (mobilen) Client-Systeme eine eigenständige Disziplin dar, die ebenfalls für die Clientsysteme des LAN prinzipiell gelöst sein sollte und im Hinblick auf die Systeme im WLAN zu erweitern ist. Details hierzu sind in Kapitel 12 enthalten.

Aus dem Blickwinkel der IT-Sicherheit sind zwei Fragestellungen von Interesse: Welche Managementaspekte tragen unmittelbar zur Sicherheit bei (Kapitel 10.1) und wie kann das Management als solches sicher durchgeführt werden (Kapitel 10.2).

## 10.1 Management-Systeme für WLAN

Die Besonderheiten des Übertragungsmediums Funk führen auch unter Sicherheitsaspekten zu einer Erweiterung der Managementaufgaben. Diese Erweiterungen spiegeln sich nicht oder nur bedingt in den Objekten der Management Information Base (MIB) für WLAN nach IEEE 802.11 wieder und haben zur Entwicklung von eigenständigen WLAN-Management-Systemen und -Werkzeugen geführt.

Im Folgenden werden nun anhand der verschiedenen Management-Disziplinen die sicherheitsspezifischen Aspekte des WLAN-Managements erörtert.

### 10.1.1 Configuration Management und Change Management

Configuration Management und Change Management sind Schlüsseldisziplinen für alle IT-Infrastrukturen, und WLAN sind hier keine Ausnahme. Für die IT-Sicherheit gilt allgemein: Die Fähigkeit, zu jedem Zeitpunkt die Konfiguration eines jeden Netzelements prüfen zu können und so je-

derzeit die Vollständigkeit und Aktualität einer Dokumentation nachweisen zu können, ist eine fundamentale Grundlage für die Vorbeugung und Behandlung von Sicherheitsvorfällen.

Für den WLAN-Bereich sind nun folgende Aspekte zu berücksichtigen:

- **Ortspezifische Konfigurationen:** Es kann nicht ausgeschlossen werden, dass sich die Konfigurationen von einem Ort des WLAN-Versorgungsgebiets zu einem anderen Ort unterscheiden. Typischerweise betrifft dies die Parameter zur physikalischen Ebene und zum Kanalzugriff. Es kann beispielsweise sein, dass verschiedene Antennen mit unterschiedlichem Antennengewinn verwendet werden und daher die Sendeleistung angepasst werden muss.
- **Hohe Patch- und Update-Frequenz:** Der WLAN-Bereich ist ausgesprochen dynamisch. Neben einer kontinuierlichen Flut an neuen WLAN-Produkten ist innerhalb eines Produkts oft eine vergleichsweise hohe Frequenz an Software-Updates und Patches festzustellen. Das Testen aller Updates und Patches unter Laborbedingungen ist dann häufig mit einem akzeptablen Aufwand nicht mehr möglich, mit der Konsequenz, dass man es beim Test von wichtigen Updates oder Patches belässt. Damit ist naturgemäß auch ein Sicherheitsrisiko verbunden. Ab einer gewissen Größe des WLAN ist das manuelle Ausrollen eines Updates oder Patches nicht mehr möglich und es muss eine geeignete Unterstützung vom Netzmanagementsystem gegeben sein. Insbesondere muss seitens des Netzmanagements die zentrale Überprüfung der aktuellen Software-Stände möglich sein.
- **Koexistenz unterschiedlicher (Sicherheits-)Konfigurationen:** In heterogenen Client-Umgebungen werden oft Clients eingesetzt, die lediglich ältere bzw. sehr eingeschränkte Sicherheitsmechanismen unterstützen. Als Konsequenz müssen dann oft unterschiedliche Sicherheitskonfigurationen parallel über eine WLAN-Infrastruktur betrieben werden. Dies muss mit der gebührenden Sorgfalt konfiguriert und gepflegt werden, da gerade der Parallelbetrieb unterschiedlicher Sicherheitstechnologien auch größere Risiken für die Sicherheit des WLAN birgt. Das Configuration Management muss hier Mittel bereitstellen, die unterschiedliche Benutzergruppen mit ihren spezifischen Sicherheitskonfigurationen verwalten können. Die Situation des Parallelbetriebs unterschiedlicher Sicherheitskonfigurationen ergibt sich speziell bei der Migration von einer Sicherheitstechnik zu einer anderen (beispielsweise von WEP nach WPA).
- **Erweiterte Dokumentation:** Für das Configuration Management und das Change Management ist auch die lückenlose Dokumentation aller Konfigurationsänderungen ausgehend von der Erstkonfiguration wesentlich. Auch hier müssen spezielle Eigenschaften von WLAN berücksichtigt werden: Die (bauliche) Umgebung eines WLAN bestimmt entscheidend die Ausbreitungseigenschaften und damit die Leistung. Neben den Positionen von Access Points und externen Antennen sowie der Führung von Hochfrequenz-Kabeln ist die Dokumentation der für die WLAN-Ausbreitung wesentlichen baulichen Gegebenheiten ein Schlüsselelement. Dabei ist eine einmal erfolgte Dokumentation nur dann wirklich brauchbar, wenn sie im Weiteren gepflegt wird. Umbaumaßnahmen können zu einer unmittelbaren Beeinflussung der WLAN-Leistung führen. Das Configuration Management muss daher im Rahmen der Dokumentation sicherstellen, dass stets der aktuelle Gebäude- oder Geländezustand reflektiert werden kann. Die Dokumentation sollte bei allen Umbaumaßnahmen im Abdeckungsbereich des WLAN geprüft und angepasst werden. Für die Sicherheit ist diese Dokumentation eine wichtige Hilfe bei der Lokalisierung von Angriffen.

Es existieren WLAN-Management-Systeme, die sich im Bereich Configuration Management dadurch auszeichnen, dass über sie nicht nur die Objekte der Standard-MIB konfiguriert werden können, sondern darüber hinaus auch verschiedene herstellerspezifischen MIBs genutzt werden können. Neben der Parametrierung der teilweise herstellerspezifischen Funkparameter ist hier vor allem die Konfiguration der erweiterten Sicherheitsfunktionen wie WPA möglich. Des Weiteren kann eine Verwaltung der Software-Stände für die Access Points durchgeführt werden.

### 10.1.2 Fault Management

Die empfindlichste Ressource im WLAN ist die Luftschnittstelle. Störungen auf der Luftschnittstelle beeinträchtigen das allgemeine Sicherheitsziel der Verfügbarkeit. Dabei ist zu beachten, dass zwei Sichten im Fault Management unterstützt werden müssen, denn aus der Access-Point-Perspektive mag

das Netz fehlerfrei sein, ein Client mag jedoch feststellen, dass er sich in einem Funkloch befindet (Abbildung 37).

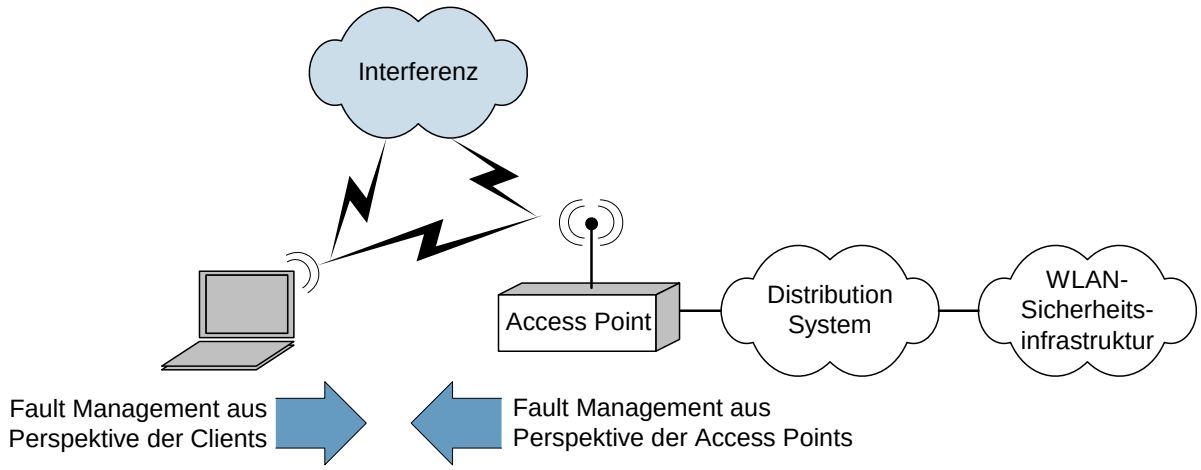



Abbildung 37: Sichtweisen im WLAN Fault Management

Die MAC-Statistiken, die gemäß der MIB für IEEE 802.11 für die Luftschnittstelle an Access Points geführt werden, sind ein möglicher Indikator für Fehlerfälle. Die Festlegung von Schwellwerten für diese Zähler (sogenanntes Baselining) ist jedoch schwierig, da ein Shared Medium vorliegt und zusätzlich die Eigenschaften der Funkübertragung generell zu einer gewissen natürlichen Fehlerhäufigkeit führen. Zudem sind Störungen oft temporärer Natur und abhängig von der aktuellen Position eines Clients.

Neben den traditionell überwachten Zählern und Tabellen, die auf Fehler bei der Übertragung hindeuten (wie zum Beispiel die Erreichbarkeit von Netzelementen oder die Anzahl der Neuübertragungen) und dem Sicherheitsziel der Verfügbarkeit zuzuordnen sind, ist aus dem Blickwinkel der Sicherheit die Überwachung weiterer Werte und Ereignisse über ein WLAN-Management-System erforderlich:

- **Authentifizierungsversuche**: Die Anzahl fehlgeschlagenen Authentifizierungen im Verhältnis der Gesamtzahl der Authentifizierungsversuche an einem Access Point kann auf einen Eindringungsversuch hindeuten.
- **Integritätsverletzungen**: CRC-Fehler können auch auf gefälschte Pakete hinweisen. Ab einem gewissen lastabhängigen Schwellwert sollte eine Meldung generiert werden. Meldet bei Verwendung von WPA bzw. IEEE 802.11i das Verfahren Michael einen Fehler, ist sogar von einer Paketfälschung auszugehen.
- **Fremdgeräte**: Werden auf einem der Funkkanäle eines WLAN Geräte festgestellt, deren MAC-Adresse nicht bekannt ist, kann dies zwar lediglich auf ein benachbartes WLAN oder den versehentlich aktivierten WLAN-Adapter eines Besuchers hindeuten. Es kann allerdings auch einen ernsten Sicherheitsvorfall anzeigen. Dieser Aspekt wird im Kapitel 10.1.4 zum Thema Security Management diskutiert.

Inzwischen gibt es WLAN-Management-Systeme, die Störungen auf der Luftschnittstelle von zentraler Stelle sowohl aus der Access-Point-Perspektive als auch aus der Client-Perspektive detektieren können. Dies beinhaltet nicht nur Messungen auf dem Kanal, auf dem ein Access Point operiert, sondern das gesamte Spektrum muss beobachtet werden.

Manche Management-Systeme nutzen die bestehenden Access Points für diese Messungen. Die Access Points schalten dann regelmäßig zwischen dem Betriebsmodus und einem Messmodus um. Da eine Messung außerhalb des operativen Kanals bedingt, dass der Access Point in dieser Zeit keine Pakete senden und empfangen kann, sind Leistungseinbussen durch diesen Umschaltmechanismus möglich. Eine andere Vorgehensweise nutzt außerdem die authentifizierten Clients als Sensoren für

die Luftschnittstelle. Diese melden Messergebnisse und sicherheitsrelevante Vorkommnisse an die WLAN-Management-Zentrale. Es gibt allerdings auch Produkte, die eine eigene Infrastruktur an Mess-Sensoren erfordern. Diese Sensoren beobachten quasi als „WLAN-Wächter“ alle Funkkanäle hinsichtlich möglicher Fehler, Leistungsengpässe und insbesondere Sicherheitsvorfälle.

Diese Systeme können jedoch Messungen vor Ort nicht vollständig ersetzen. Sie sind als zusätzliche Informationsquelle zu sehen, die insbesondere eine schnellere Reaktion auf Fehlersituationen ermöglichen und durchaus dazu beitragen können, Vororteinsätze auf das notwendige Maß zu reduzieren.

### 10.1.3 Performance Management

Die Messung der Leistungsparameter im WLAN ist wie im LAN eng gekoppelt mit dem Fault Management. Zunächst kann man die Werte, die im Rahmen des Fault Management erfasst werden, für das Performance Management hinsichtlich ihres Langzeitverhaltens betrachten. Im Bereich des Performance Managements für WLAN ist allerdings auch die Client-Perspektive zu beachten. Erst mit der Bewertung der Kommunikationsqualität aus der Perspektive des Clients kann beispielsweise eine Aussage hinsichtlich der Güte der WLAN-Ausleuchtung getroffen werden. Dies betrifft Funktionen zum sogenannten Site Survey, d. h. der systematischen Messung im Rahmen einer Begehung des WLAN-Abdeckungsbereichs.

Es gibt spezielle Werkzeuge für ein Site Survey, sowohl aus dem Open-Source-Bereich als auch kommerzielle Werkzeuge. Ergänzt werden diese Werkzeuge durch inzwischen verfügbare Management-Systeme, die auch aus der Client-Perspektive eine Messung von Leistungsparametern gestatten, wie bereits im Kapitel 10.1.2 zum Thema Fault Management erörtert wurde.

### 10.1.4 Security Management

Im Rahmen des Security Managements sind folgende Bereiche zu berücksichtigen:

- Management der Sicherheitskonfigurationen: Siehe hierzu Kapitel 10.1.1.
- Erkennung und Lokalisierung von Sicherheitsvorfällen

Die Erkennung von Sicherheitsvorfällen beinhaltet dabei:

- **Erkennung von Verletzungen der WLAN Security Policy:** Hier geht es vor allem um die Erkennung von Verstößen gegen zentrale Security-Parameter, wie z. B. die Nutzung von nicht zulässigen Anmeldeprotokollen oder Anmeldeversuche mit einem falschen SSID.
- **Erkennung von Fremdgeräten:** Speziell die Erkennung fremder Access Points (sogenannter Rogue Access Points) auf dem Behörden- bzw. Betriebsgelände und in der unmittelbaren Nachbarschaft ist von besonderem Interesse. Oft stellt sich heraus, dass ein solcher Access Point von einem Mitarbeiter installiert wurde, ohne aus Unkenntnis der Sachlage die IT-Abteilung um Erlaubnis zu fragen. Solche Geräte stellen ein erhebliches Risiko dar, da sie meist nur oberflächlich konfiguriert sind und ohne weitere Sicherheitsmechanismen direkt an die LAN-Infrastruktur angeschlossen sind. Es kann allerdings auch sein, dass es sich bei einem fremden Access Point um die Ausrüstung für eine Attacke vom Typ „Man in the Middle“ (MitM) handelt! Die Erkennung eines Fremdgeräts erfolgt z. B. über die MAC-Adresse und die Verwendung eines fremden SSID. Die Erkennung eines fremden Access Points, der irgendwo auf dem Gelände an das LAN angeschlossen wurde, erfordert jedoch eine über das WLAN hinaus gehende Überwachung von Geräten, die an einem kabelbasierten Endgeräteanschluss angebracht werden.
- **Erkennung von Angriffsmustern:** Ein Indikator auf WLAN-Ebene ist eine Häufung von fehlgeschlagenen Anmeldeversuchen am Access Point. Hierzu können typischerweise im WLAN-Management-System entsprechende Alarme konfiguriert werden. Die nach einer erfolgreichen Authentifizierung dennoch möglichen klassischen Angriffe auf LAN-Ebene wie ARP-Poisoning können in der Regel durch die Nutzung von IEEE 802.1X unterbunden werden. Angriffe auf höherer Netzwerkebene, wie DNS-Spoofing, können über ein WLAN-Management-System nicht de-

tektiert werden. Hier ist auf die Nutzung von herkömmlichen Intrusion-Detection-Systeme zu verweisen.

Interessant ist nun die Frage der Möglichkeit der Lokalisierung eines Sicherheitsvorfalls. Zunächst kann der Access Point bzw. der Access Switch Port ermittelt werden, über den der Vorfall gemeldet wurde. Eine ordnungsgemäße Dokumentation vorausgesetzt, kann auf diese Weise eine recht grobe Genauigkeit der Positionsbestimmung erreicht werden.

Aus einer funktechnischen Perspektive stehen zwei Parameter für eine Positionsermittlung zur Verfügung: Empfangsleistung und Laufzeitdifferenz. Letzterer Parameter wird im satellitengestützten Global Positioning System (GPS) verwendet. Im WLAN sind die Differenzen in der Signallaufzeit durch die vergleichsweise extrem geringen Distanzen dagegen entsprechend gering. Außerdem tut hier die Mehrwegeausbreitung ihr Übriges. Es bleibt also die Möglichkeit der Auswertung der Empfangsleistung. Die Ungenauigkeit ist hier allerdings erheblich. Schwankungen der Empfangsleistung um plus/minus 10 dB sind nicht ungewöhnlich. Auch bei einer Messung von mehreren Access Points aus kann (im Gegensatz zu klassischen triangulären Verfahren wie GPS) kein deutlicher Mehrgewinn an Genauigkeit erwartet werden. Es ist also mit einer eher groben Lokalisierungsgenauigkeit zu rechnen.

### 10.1.5 Accounting Management

Im Rahmen des Accounting Managements sind für WLAN primär die Anmeldezeiten von Clients von Interesse, wobei in nicht öffentlichen WLAN eine Aufzeichnung und vor allem deren Auswertung immer in Rücksprache mit dem Betriebs- bzw. Personalrat erfolgen sollte. Unter Sicherheitsaspekten sind allerdings ungewöhnliche Nutzungszeiten z. B. außerhalb der Bürozeiten von Interesse, da eine Häufung von Anfragen zu ungewöhnlichen Zeiten unter einem ansonsten akzeptierten Zugang durchaus ein Anzeichen eines Angriffs sein kann.

Ein wesentlich stärkeres Gewicht gewinnt das Accounting im Rahmen der Hotspots (siehe hierzu Kapitel 11).

## 10.2 Management-Protokolle

Im Folgenden findet eine Bewertung der für das Management von WLAN eingesetzten Protokolle und Mechanismen statt, wobei sich diese allerdings nicht wesentlich von denen in kabelgebundenen Netzen unterscheiden. Das Bedrohungspotential ist aber durch eine ungesicherte Luftschnittstelle ungleich größer.

Grundsätzlich gilt in diesem Zusammenhang für Access Points, dass der Management-Zugang über die Luftschnittstelle möglichst deaktiviert werden sollte.

### 10.2.1 Einsatz von SNMP

Wie schon im IT Grundschutzhandbuch des BSI in der Maßnahme M 2.144 „Geeignete Auswahl eines Netzmanagement-Protokolls“ beschrieben, birgt der Einsatz von SNMPv1 und SNMPv2 Sicherheitsrisiken, da die Informationsübertragung im Klartext erfolgt. Dadurch können die wesentlichen Authentifizierungsinformationen wie die IP-Adresse und der SNMP Community String ausgelesen werden.

Im WLAN verschärft sich diese Problematik. Viele Access Points erlaubten den administrativen Zugriff sowohl über das kabelgebundene LAN als auch über die Luftschnittstelle. Bei unverschlüsselter oder nur schwach verschlüsselter (WEP) Kommunikation im WLAN können also die notwendigen SNMP-Informationen mitgelesen werden und zur Manipulation der Access Point Konfiguration genutzt werden.

Abhilfe schafft die Nutzung von SNMPv3, dass mittlerweile von einigen Access Point Herstellern unterstützt wird.

### 10.2.2 Einsatz von telnet, HTTP und FTP

Wie bei SNMP handelt es sich bei telnet, HTTP (Hypertext Transfer Protocol) und FTP (File Transfer Protocol) um Klartext-Protokolle. Sämtliche damit übertragenen Daten werden unverschlüsselt übertragen. Da viele Access Points die Nutzung dieser Protokolle auch für Zugriffe auf den Access Point über die Luftschnittstelle zulassen, kann ein Angreifer in einem ersten Schritt die Anmeldeinformationen (Benutzername und Passwort) mitlesen, sofern die Kommunikation auf der Luftschnittstelle nicht geeignet verschlüsselt ist.

### 10.2.3 Einsatz von TFTP

Bei vielen Access Points besteht die Möglichkeit, neue Firmware-Stände per TFTP (Trivial FTP) auf den Access Points abzulegen. Bei TFTP findet im Gegensatz zu FTP keine Benutzerauthentifizierung statt. Dadurch ist es einem Angreifer wesentlich einfacher möglich, Access Points mit manipulierter bzw. fehlerhafter Firmware zu versorgen.

### 10.2.4 Nutzung von SSH und SSL

Neben den Zugriffen per FTP, TFTP, telnet und HTTP unterstützen viele Access Points das Protokoll SSH (Secure Shell) für administrative Zugriffe..

Der entscheidende Vorteil bei der Nutzung von SSH besteht darin, dass sämtliche zwischen den beiden Kommunikationspartnern übertragenen Informationen (inklusive der Authentifizierungsinformationen) verschlüsselt übertragen werden.

In der Vergangenheit hat sich allerdings die Implementierung von SSH in der Version 1 als anfällig gegenüber MitM-Attacken herausgestellt, bei denen der verschlüsselte Kommunikationskanal zwischen den Endgeräten aufgebrochen und die übertragenen Informationen im Klartext durch den Angreifer gelesen werden konnten. Sichere Implementierungen nutzen deshalb SSH in der Version 2, welches diese Sicherheitslücke behebt.

Zur Absicherung der Web-Schnittstelle bieten einige Access Points auch SSL/HTTPS (Secure Sockets Layer bzw. HTTP Secure) an. Allerdings ist der Access Point nach wie vor auf Port 80 erreichbar, und die Sicherheit der Web-basierten Konfigurationsschnittstelle ist von der Stabilität der auf dem Access Point laufenden Web-Applikation abhängig.

## 10.3 Zusammenfassung

Beim Configuration Management ist im Hinblick auf die Sicherheit einer WLAN-Installation neben der zentralen Administration der Sicherheitseinstellungen auch die Bereitstellung abgesicherter Installations- und Managementwege von entscheidender Bedeutung. Aus Sicherheitsaspekten ist darüber hinaus dringend zu empfehlen, dass WLAN-Management-Systeme die Möglichkeit zur Überwachung der Luftschnittstelle, die Interpretation der dabei gewonnenen Messergebnisse und Funktionen wie „Rogue Access Point Detection“ oder „Wireless IDS“ unterstützen.

# 11 Sichere Hotspots

Neben der Erweiterung der LAN-Infrastuktur im betrieblichen Umfeld hat sich relativ schnell eine weitere Nutzungsform der WLAN-Technik – diesmal im kommerziellen Bereich – etabliert, die sogenannten Hotspots. Diese öffentlichen Netzzugänge werden über WLAN Access Points realisiert.

Stehen bei betrieblichen WLAN-Installationen die Aspekte Flächendeckung, Mobilität und Absicherung des WLAN gegen unautorisierten Zugang im Vordergrund, sind für einen Hotspot die Aufgabengebiete Teilnehmerverwaltung, Authentifizierung des (zahlenden) Teilnehmers dem Netz gegenüber sowie Zahlungsabwicklung und Abrechnung zu betrachten. Da Hotspot-Anbieter hier im Sinne des Telekommunikationsgesetzes (TKG) als Telekommunikationsdienstleister auftreten, sind u. a. die Auflagen bzgl. Sicherheit der Abrechnungs- und Benutzerdaten (Datenschutz, Speicherung von Verbindungsdaten) zu berücksichtigen, siehe [TKG04].

## 11.1 Hotspot-Architekturen

Bislang haben sich noch keine Standards in der Realisierung von einheitlichen Hotspot-Architekturen etabliert. Dies hängt zum großen Teil mit unterschiedlichen Betreibermodellen und der vergleichsweise jungen Technik zusammen.

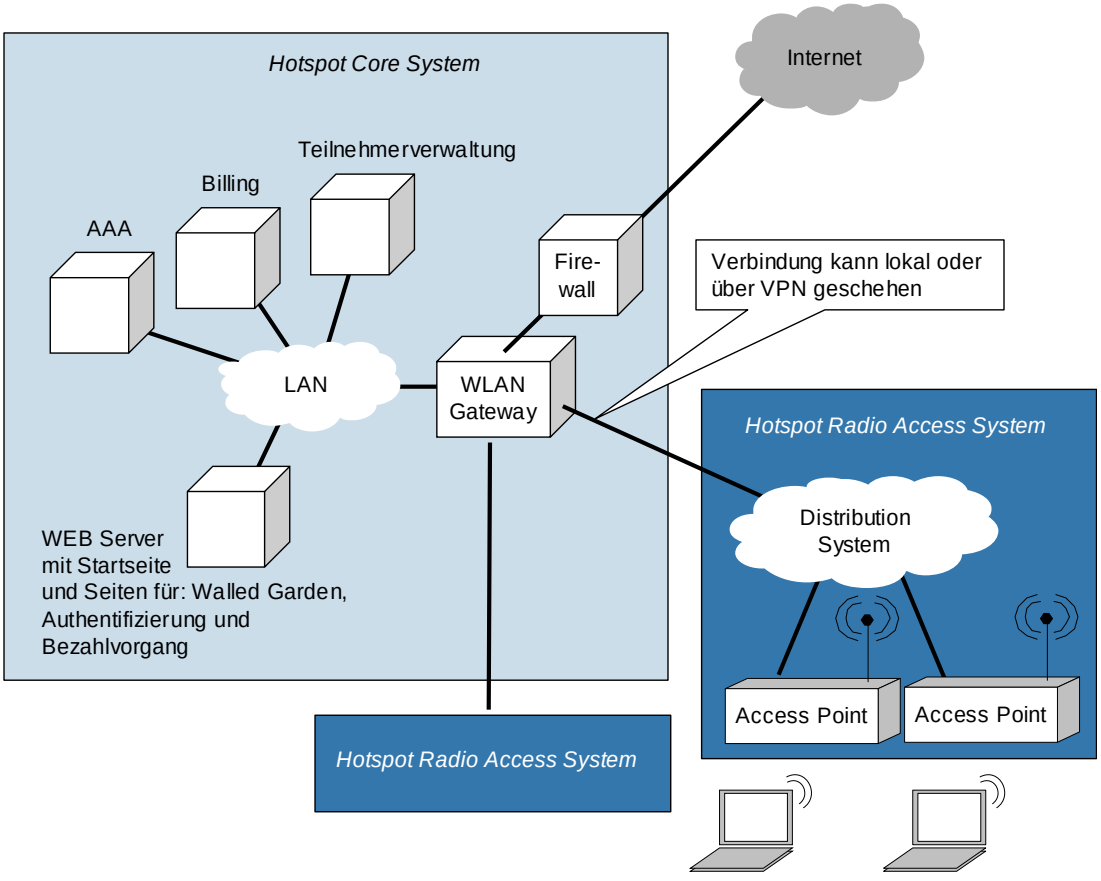



Abbildung 38: Allgemeine Komponenten eines Hotspot-Systems

Generell werden durch ein WLAN nach IEEE 802.11 lediglich der Netzzugang im Sinne der Luftschnittstelle und gewisse Aspekte zur Ermöglichung von Mobilität zwischen Funkzellen spezifiziert. Damit entspricht ein WLAN einem sogenannten Radio Access Network. Für die genannten Funktio-

nen zur Teilnehmerverwaltung, Hotspot-Teilnehmer-Authentifizierung sowie Zahlungsabwicklung und Abrechnung muss also eine zusätzliche Infrastruktur geschaffen werden, an welche die einzelnen WLAN-Inseln angekoppelt werden.

Der Aufbau dieses sogenannten Core-Systems unterscheidet sich je nach gewählter Hotspot-Architektur. Bei größeren öffentlichen Hotspots z. B. für Hotelketten ist das Core-System oft zentral aufgebaut, und die einzelnen über ein größeres Gebiet verteilten Radio-Access-Systeme werden beispielsweise über ein IP-VPN angebunden. Bei kleinen Hotspot-Installationen, wo der Betrieb eines einzelnen Hotspots in Eigenregie erfolgt, ist das Core System hingegen lokal am Ort realisiert. Für solche „Mini Hotspots“ gibt es bereits Systeme, die alle notwendigen Zusatzfunktionen in einer Box z. B. als Appliance realisieren.

Abbildung 38 zeigt die allgemeinen Komponenten eines Hotspot-Systems im Überblick.

### 11.1.1 Grundprinzip der Anmeldung an einem Hotspot

Im Prinzip verfahren alle Hotspots, mehr oder weniger ähnlich, nach folgendem Verfahren:

- **Netzverbindung:** Die Anmeldung an einem Access Point eines Hotspots erfolgt üblicherweise über die Broadcast SSID. Dies geschieht meist dadurch, dass in der Client-Konfiguration das SSID-Feld leer gelassen wird. **In der Regel erfolgt keine Verschlüsselung auf der Luftschnittstelle**, um dem Client einen möglichst unproblematischen Netzzugang zu ermöglichen, da nicht jeder Nutzer die Kenntnisse oder Rechte hat, um auf seinem Client einen WEP-Schlüssel, WPA-PSK oder eine EAP-Methode zu konfigurieren. Dies ist zur Zeit noch eine fundamentale Schwachstelle vieler Hotspots, die jedem Benutzer bewusst sein muss[31]. Aktuelle Entwicklungen in den USA zeigen allerdings, dass es grundsätzlich möglich ist, einen Hotspot unter Einsatz von IEEE 802.1X besser abzusichern[32]. Da dieser Ansatz noch sehr jung ist, unterstützen nur wenige Hotspot-Anbieter dieses Konzept. Nach der Assoziierung erhält der Client alle Parameter für die Netzwerkverbindung über DHCP. Sofern der Nutzer keine Möglichkeit hat, potentiell erforderliche Änderungen an der Konfiguration seiner Netzwerkkarte bzw. seines Systems vorzunehmen, bieten einige Hotspot-Lösungen die Funktion Dynamic Address Translation (DAT) an (siehe Kapitel 11.1.2).
- **Redirect und Walled Garden:** Im zweiten Schritt startet der Nutzer seinen Web Browser und greift auf eine von ihm gewünschte Internet-Seite zu. Der entsprechende http-get-Befehl wird von einem speziellen Gateway (in Abbildung 38 als WLAN Gateway bezeichnet) empfangen und nicht ins Internet weitergeleitet, sondern in Richtung Hotspot Core System. Hierbei erhält der Browser des Nutzers vom Hotspot Core System die Aufforderung zu einem Redirect zu einem speziellen URL. Dies erfolgt für den Nutzer transparent, also ohne dass er darüber besonders unterrichtet wird (er merkt es nur am URL). Der Browser führt dann ein erneutes http-get auf den umgeleiteten URL durch.
  Dieser URL führt auf die Hotspot-Startseite in einem dem Hotspot zugeordneten Web Server.

---

31 Als Randbemerkung sei in diesem Zusammenhang nur erwähnt, dass in öffentlichen Mobilfunknetzen auf Basis von GSM oder UMTS die Verschlüsselung einer Sprach- oder Datenübertragung selbstverständlich ist, ohne dass der Nutzer hier irgendwelche manuellen Konfigurationen vornehmen muss.

32 Der Zugang zu einem Hotspot kann prinzipiell auch durch ein IP-VPN abgesichert werden, sofern der Hotspot-Betreiber einen Weg einrichtet, der es dem Kunden erlaubt den entsprechenden VPN Client zu installieren und zu konfigurieren. Die beiden Tunnelendpunkte sind der Hotspot Client und ein VPN Gateway in der Hotspot-Infrastruktur.

IPSec kommt als Layer-3-Verfahren für diesen Zweck meist nicht in Frage, da insbesondere in Verbindung mit einer weiteren IPSec-VPN-Lösung zum Zugriff des Nutzers auf das heimatliche Netz technische Komplikationen zu erwarten sind. Manche Hotspots realisieren den Schutz der Luftschnittstelle über das Point to Point Tunneling Protocol (PPTP), also durch einen Layer-2-Mechanismus. PPTP wird von einer Vielzahl von Client-Systemen unterstützt und kann mit vergleichsweise geringem Aufwand konfiguriert werden. Über einen PPTP-Tunnel kann dann eine nutzerspezifische VPN-Lösung eingesetzt werden.

Dort hat der Nutzer die Möglichkeit kostenfreie Seiten des Hotspot-Betreibers (den sogenannten Walled Garden) oder die eigentliche Anmeldeseite des Hotspots zu besuchen. Auf dieser Anmeldeseite (bzw. den von dieser Seite zugänglichen Folgeseiten) können die systemspezifischen Bezahlmodalitäten festgelegt werden, und der Nutzer kann sich für einen Internetzugang anmelden.

- **Authentifizierung:** Die Authentifizierung und die darauf folgende Freischaltung des eigentlichen Internetzugangs erfolgt je nach eingesetztem Hotspot-System unterschiedlich. Es gibt Systeme, bei denen man eine Zugangskarte erwirbt und an dieser Karte das Passwort „frei rubbeln“ muss. Dieses Passwort wird auf der entsprechenden Anmeldeseite im Browser eingegeben. Andere Systeme erfordern die Eingabe einer Kreditkartennummer.
  Das Hotspot Core System prüft das Passwort und teilt bei einem positiven Ergebnis dem Browser ein abschließendes Redirect auf die eigentlich gewünschte ursprünglich angesprochene Web-Seite im Internet mit. Der entsprechende http-get Request wird wieder vom WLAN Gateway abgefangen. Das WLAN Gateway führt eine RADIUS-Anfrage durch und leitet den Request in Richtung Internet, sofern die Anfrage vom AAA-Server positiv beantwortet wurde.
  Als Ergebnis erhält der Nutzer die gewünschte Seite und kann „beliebig“ (je nach System können auch Content Filter installiert sein) im Internet surfen.
- **Abrechnung:** Die Abrechnung erfolgt in Abhängigkeit des Zugangssystems, d. h. Prepayment über eine „Rubbelkarte“, Postpayment über Kreditkarte oder über die GSM Subscription.

### 11.1.2 Dynamic Address Translation

Ein Hotspot-Betreiber muss mit unterschiedlichst konfigurierten Clients rechnen. Nicht selten ist seitens der Nutzer auch nicht das Wissen um die Netzwerkkonfiguration vorhanden, oder die entsprechenden administrativen Rechte sind dem Nutzer entzogen. Ein Hotspot sollte also (aus Betreibersicht) im Idealfall mit „jeder“ Client-Konfiguration zurechtkommen.

Der Hotspot stellt deshalb in seinem WLAN Gateway oft einen Proxy-Server bereit (siehe Abbildung 39).

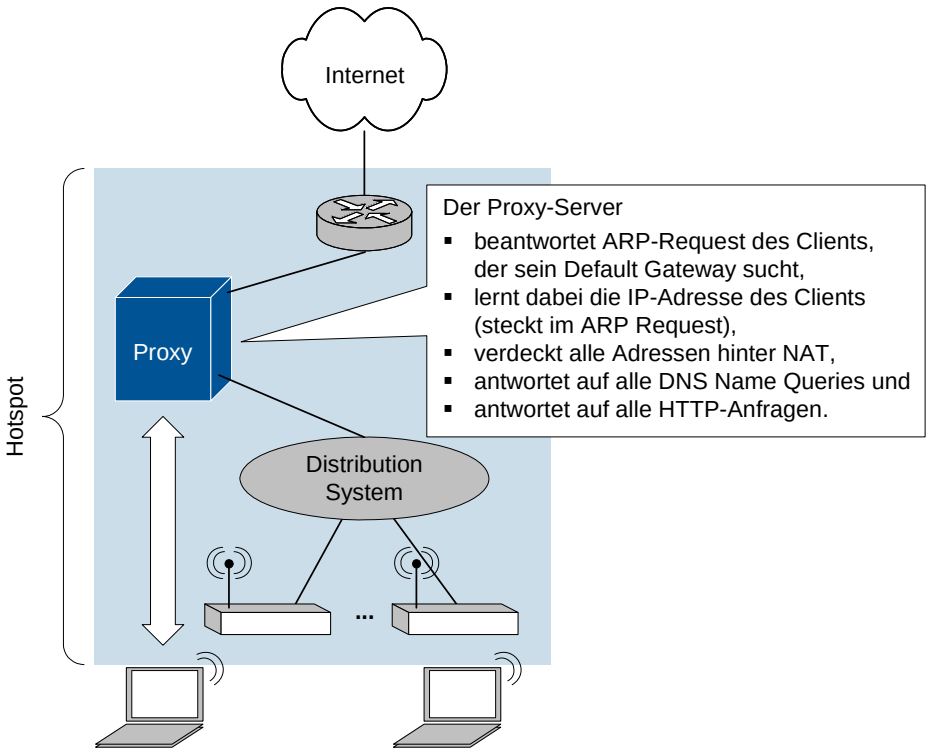



Abbildung 39: Einsatz eines Proxy-Servers im Hotspot

Für einen Client mit einer statischen IP-Konfiguration beantwortet dieser Proxy Server alle ARP-Requests, wenn dieser für die Kommunikation in Richtung Internet sein Default-Gateway sucht. Im Zuge dieses ARP-Requests lernt der Proxy-Server automatisch die IP-Adresse des WLAN-Clients. Durch die Nutzung von Network Address Translation (NAT) kann der Client dann über den Proxy-Server mit dem Netz hinter dem Proxy eine Verbindung aufbauen. Zur Nutzung des Internet antwortet der Proxy auf alle DNS Name-Queries und HTTP-Anfragen des Clients.

### 11.1.3 Authentifizierungsvariante SMS

Neben der Übermittlung des Zugangscodes per „Rubbelkarte“ kann dies auch per GSM Short Message Service (SMS) erfolgen, wie es in den Systemen einiger Mobilfunkbetreiber geschieht. Ein solches System basiert auf der Tatsache, dass eine GSM Mobile Station eigentlich ein universelles Authentifizierungsgerät darstellt, welches einheitlich und (fast) weltweit eine Authentifizierung über das Subscriber Identity Module (SIM) gestattet, das in die Mobile Station eingeschoben wird.

Grundlage ist der Authentifizierungsvorgang in GSM, der (vereinfacht) folgendermaßen funktioniert: Nach dem Einschalten des Mobiltelefons wird der Benutzer üblicherweise aufgefordert seine PIN einzugeben. Bei erfolgreicher Eingabe wird im Einbuchungsprozess der Mobile Station (d. h. des Mobiltelefons) in das GSM Netz eine Authentifizierung zwischen SIM und Home Location Register HLR (genauer gesagt: zwischen SIM und Authentication Center AuC) des Heimat-GSM-Netzes durchgeführt. Erst nach erfolgreicher Authentifizierung wird der Mobile Station der Zugang zum (besuchten) GSM-Netz gewährt.

Ein Nutzer, der ein eingebuchtes Mobiltelefon mit sich trägt, hat sich also bereits erfolgreich authentifiziert und ist eindeutig über seine Telefonnummer (Mobile Station ISDN Number, kurz: MSISDN) identifizierbar.

Der WLAN-Zugang wird dann wie folgt hergestellt:

- Zunächst wird die Umleitung auf den Web-Server des Hotspot mit der entsprechenden Anmeldeseite durchgeführt.
- Auf dieser Seite wird der Nutzer aufgefordert seine MSISDN einzugeben.
- Das Portal (d. h. der Web-Server des Hotspot-Betreibers) ist an ein Short Message Service Center (SMSC) eines GSM-Netzbetreibers angeschlossen. Das Portal schickt daraufhin eine Short Message mit dem Zugangscode an die hinterlassene Rufnummer. Abbildung 40 zeigt (vereinfacht) die Architektur dieses Systems.
- Der Zugangscode wird dem Hotspot-Nutzer als Inhalt einer SMS mitgeteilt. Der Nutzer liest den Code aus der SMS von seinem Mobiltelefon und gibt das Passwort in das entsprechende Formular auf der Anmelde-Seite der Hotspot-Applikation ein.
- Das WLAN Core System prüft den eingegebenen Code.
- Nach einer erfolgreichen Überprüfung wird die zugehörige IP-Adresse im AAA-System freigeschaltet. Beim nächste Zugriff über das WLAN Gateway erfolgt eine RADIUS-Anfrage an das AAA-System, welches diese positiv beantwortet und das WLAN Gateway dazu veranlasst, den Request ins Internet weiterzuleiten.

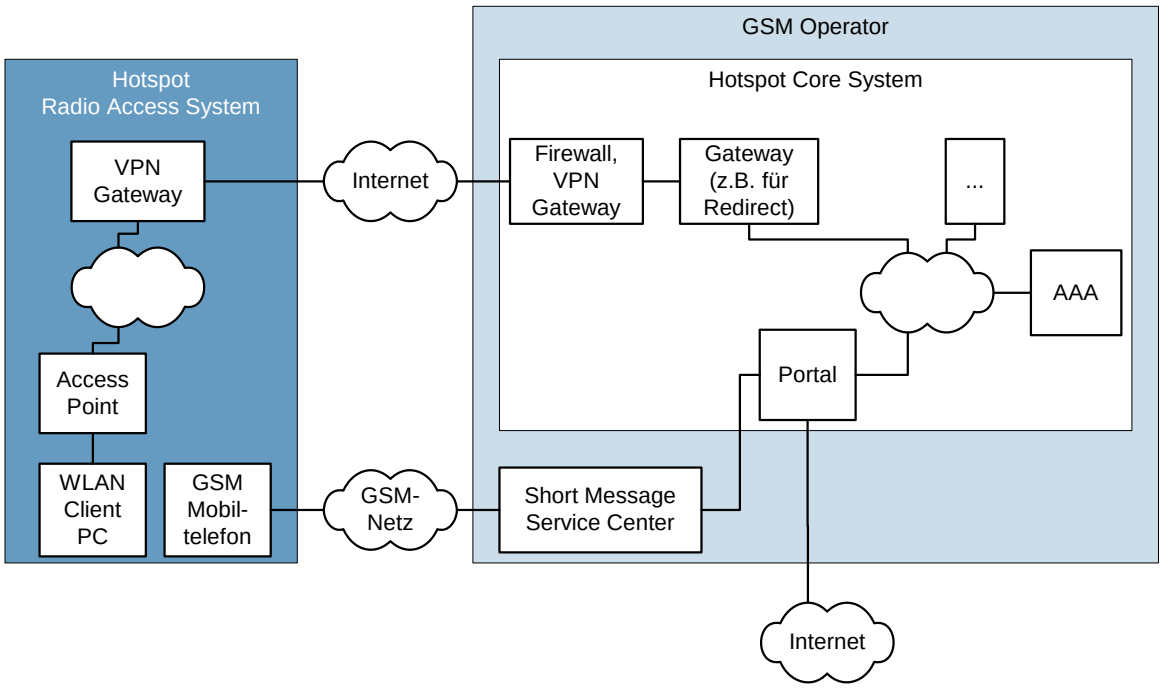



Abbildung 40: Architektur für eine Authentifizierung per SMS

### 11.1.4 Fazit zur Hotspot-Zugangstechnik

Leider ist bis heute keine einheitliche systemübergreifende Authentifizierung, Anmeldung und Abrechnung für Hotspot-Systeme realisiert.

Durch den Einsatz eines Clearing House oder durch direkte Kooperationen von Wireless ISPs (WISPs) kann dieses Problem zwar inzwischen deutlich gemildert werden, von der Umsetzung eines internationalen Standards ist man aber noch weit entfernt.

Es zeichnet sich für größere Hotspot-Systeme weiterhin der Trend ab, ein GSM- bzw. UMTS-Netz für Authentifizierung und Abrechnung zu nutzen, da diese elementaren Funktionen hier bereits implementiert sind.

Im Rahmen der Standardisierung von UMTS ist bereits eine Anbindung von WLAN vorgesehen. Bis das dort beschriebene Verfahren allerdings weltweit zur Marktreife gelangt, können durchaus noch Jahre vergehen (sofern es überhaupt umgesetzt wird). Hierbei wird im Endeffekt ein Hotspot als weiteres Radio Access Network an das UMTS Core Network angebunden und die Authentifizierung erfolgt auch im Hotspot über eine (U)SIM-Karte.

## 11.2 Sicherheitstechnische Bewertung

Bei der Bewertung der IT-Sicherheit in einer Hotspot-Umgebung sind generell folgende Perspektiven zu unterscheiden:

- Sicherheit der Hotspot-Systeme des Providers inkl. Hotspot-Applikation
- Sicherheit der Endgeräte der Hotspot-Nutzer
- Sicherheit der Kommunikation in einem Hotspot

### 11.2.1 Sicherheit der Hotspot-Systeme

Was den sicheren Betrieb der WLAN-Infrastruktur betrifft, gelten die gleichen Aussagen wie im Kapitel 10. Hinzu kommt allerdings die Absicherung des Web-Servers und der Web-Applikation zum Betrieb des Hotspots sowie der Billing- und Accounting-Systeme. Das hierbei nach dem Telekommunikationsgesetz (TKG) umzusetzende Sicherheitskonzept erfährt je nach Betreiber und gewähltem architektonischen Ansatz eine individuelle Umsetzung. Allen gemeinsam ist die Abschottung der Serversysteme gegenüber dem Internet über Firewall-Systeme und der Schutz der übertragenen Daten zwischen WLAN-Gateway des Hotspots und Netzzugang zu den Serversystemen (z. B. über ein VPN).

Kompaktsysteme für kleinere Hotspots werden häufig als Appliance mit einem gehärteten Betriebssystem angeboten.

Die Sicherheit dieser Systeme ist somit abhängig von der Güte der durchgeführten Härtungsmaßnahmen, der Programmierqualität der Web-Applikation sowie der auf den Firewall-Systemen implementierten Filterregeln.

Aktuelle Sicherheitsvorfälle im Hotspot-Bereich betreffen primär die Übernahme einer Sitzung durch einen Angreifer. Der Angreifer nutzt einfach den IP-Kontext eines echten Hotspot-Kunden weiter, nachdem dieser den Hotspot verlassen hat, und spart so die Kosten für den Internet-Zugang. Kritisch wird dies, wenn der Angreifer Informationen zu kriminellen Zwecken über diesen Zugang erhält bzw. verschickt.

### 11.2.2 Sicherheit der Endgeräte der Hotspot-Nutzer

Der Nutzung von Hotspot-Systemen widersprechen die unter Umständen in einem Unternehmen bisher geltenden strengen Sicherheitsvorgaben und Client-Konfigurationen. Damit zumindest das Web-Portal des Hotspots erreicht werden kann, müssen die Dienste DNS und HTTP für alle IP-Adressen freigeschaltet werden. Auf DHCP kann ggf. bei der Unterstützung von DAT durch das Hotspot-System verzichtet werden.
Sind diese Dienste nun freigeschaltet, hängt die Sicherheit des Endgerätes im wesentlichen vom eingesetzten Web-Browser und seiner Konfiguration ab. Auch hier muss ggf. eine Änderung der Internet-Policy des Unternehmens erfolgen, die häufig besagt, dass aus dem internen Netz auf das Internet nur über ein zwischengeschaltetes Web-Proxy-System zugegriffen werden darf. In den Browser-Einstellungen muss nun ein Profil eingerichtet werden, das den direkten Zugriff auf das Internet erlaubt.
Man sieht also schon an dieser Stelle, dass unterschiedliche Konfigurationsprofile für die WLAN-Nutzung benötigt werden, beispielsweise ein Profil für die Nutzung von WLAN auf dem Behörden- bzw. Firmengelände, ein anderes Profil für die Nutzung öffentlicher WLAN. Diese Profile müssen umfassend von der Konfiguration des WLAN-Zugangs bis zu den Browser-Einstellungen reichen.
Das Risiko der Kompromittierung des Endgerätes ist je nach eingesetzter Browser-Software gegenwärtig als unterschiedlich hoch zu bewerten. Alle Browser, insbesondere ist hier an den Internet Explorer von Microsoft gedacht, welche die Ausführung von ActiveX Controls, VBScript und JScript für aus dem Internet geladenen mobilen Programmcode zulassen, sind einer erheblich größeren Gefährdung ausgesetzt, als Browser, die lediglich Java und Java Script unterstützen und ausführen (siehe hierzu [Gri01]). Wird für den Internet-Explorer die vom BSI empfohlene Konfiguration für den Internet Explorer umgesetzt (Deaktivierung von Active Scripting, siehe etwa [BSI04]), sind gegebenenfalls die Web-Applikationen von Hotspot-Systemen nicht mehr nutzbar, so dass ein Hotspot-Zugang nicht möglich ist.
Erwähnt sei noch, dass im Hotspot-Bereich auch Clients berücksichtigt werden müssen, die nur vergleichsweise aufwändig (oder teils gar nicht) geeignet abgesichert werden können. Zu nennen sind hier PDAs, Pocket-PCs und MDAs. Nicht selten enthalten solche Geräte standardmäßig keine Sicherheits-Features. Diese sind – sofern überhaupt angeboten – durch Zusatzsoftware nachzurüsten.
Aber auch bei konventionellen Notebooks findet in vielen Fällen keine ausreichende Absicherung des Systems statt. Stichworte sind hier:

- Aktuelle Virenschutzsoftware
- Nutzung einer Personal Firewall
- Absicherung von Remote-Support-Zugängen und privilegierten Benutzerkonten
- Unterbindung von Laufwerksfreigaben

Weitere Aspekte hierzu sind im Kapitel 12 enthalten.

### 11.2.3 Sicherheit der Kommunikation in einem Hotspot

In der Regel wird die Übertragung der Informationen zur Authentifizierung des Benutzers vom WLAN-Client in Richtung Hotspot-Web-Applikation per SSL verschlüsselt. Bei der nachfolgenden Betrachtung und Diskussion denkbarer Angriffe auf diese Web-basierte und dabei SSL-geschützte Authentifizierungsprozedur werden folgende Rahmenbedingungen unterstellt:

- Auf Client-Seite werden oft **keinerlei** WLAN-Sicherheitsparameter gesetzt, d. h. es erfolgt insbesondere meist keine Verschlüsselung per WEP oder TKIP! Erste Hotspots, die eine Authentifizierung über IEEE 802.1X via WPA bzw. WPA2 gestatten, sind in den USA allerdings schon vereinzelt anzutreffen.
- Das WLAN im betrachteten Hotspot stellt somit ein Shared Medium im klassischen Sinne dar, in dem alle Teilnehmer an jeglicher Kommunikation zumindest passiv teilhaben können.
- Für die Adressvergabe an die Client-Systeme wird DHCP eingesetzt.

Diese Annahmen decken sich mit der Realität der überwiegenden Mehrheit der Hotspots. Damit ist der Nutzer eines Hotspot den folgenden Gefährdungen ausgesetzt:

- **Man-in-the-Middle-Attacke**

  Bei der Man-in-the-Middle-Attacke platziert sich der Angreifer wie ein Proxy zwischen dem sich authentifizierenden Client und dem entsprechenden Server. In dieser Situation etabliert er zwei SSL-geschützte Kommunikationsbeziehungen (bzw. lässt dieses zu):

  - eine HTTPS-Session mit dem Server
  - eine HTTPS-Session mit dem Client

  Erstere kann er wie jeder andere Client auch problemlos initiieren, da er sich dem Server gegenüber nicht authentifizieren muss. Letztere ist etwas kniffliger: Da er sich dem Client gegenüber als Server ausgibt, muss er sich auf Basis eines Zertifikats (genauer: mit Hilfe des dazu gehörenden privaten Schlüssels) authentifizieren. Da er kein gültiges Zertifikat (bzw. den privaten Schlüssel) für den echten Server besitzt und eine Fälschung von Zertifikaten nach derzeitigem Stand der Kryptologie nicht möglich ist, muss er dem Client ein ungültiges bzw. ein nicht vertrauenswürdiges Zertifikat anbieten, das er sich z. B. selbst generiert hat. An dieser Stelle lässt sich der Angriff entdecken und abwehren, indem der aufmerksame Anwender dieses Zertifikat ablehnt. Leider akzeptieren die meisten Anwender derartige obskuren Zertifikate, meist infolge von Unkenntnis und aus Gewohnheit: ungültige Zertifikate sind im Internet nichts ungewöhnliches, so dass der Angreifer darauf hoffen darf, dass der Anwender auch in diesem Fall automatisch dem neuen Zertifikat vertraut.

  Sobald die beiden HTTPS-Sessions etabliert sind, kann der eigentliche Authentifizierungsprozess ablaufen. Dazu reicht der Angreifer einfach alle Informationen, die Client und Server austauschen, an den jeweils anderen weiter. So kann er sich, auch ohne das Kennwort zu besitzen, authentifizieren.

  Um die Man-in-the-Middle-Attacke durchführen zu können, muss der Angreifer dem Client gegenüber die Identität des Servers annehmen. Dazu geeignete Techniken sind im Folgenden beschrieben.

- **ARP Poisoning**

  Beim ARP Poisoning manipuliert der Angreifer den ARP Cache des Clients. Dies geschieht über den Gratuitous-ARP-Mechanismus.

  Unter Gratuitous ARP versteht man unaufgefordert gesendete ARP Responses, die bereits vorhandene Einträge in den ARP Caches empfangender Stationen updaten. Jede standardkonforme ARP-Implementierung muss Gratuitous ARP unterstützen.

  Der Angreifer macht sich diesem Umstand zunutze, indem er Gratuitous-ARP-Pakete sendet, die zur IP-Adresse des Servers (oder eines anderen Netzelements), dessen Identität er übernehmen möchte, seine eigene MAC-Adresse enthalten. Befindet sich die IP-Adresse des auf diese Weise gespooften Servers bereits im ARP Cache des Clients (wovon bei Infrastrukturservern auszugehen sein dürfte), so wird dieser aktualisiert, d. h. mit der MAC-Adresse des Angreifers überschrieben. In der Folge werden Pakete dieses Clients an den Server zwar – da es sich um ein Shared Medium handelt – nach wie vor von diesem physikalisch empfangen, aber nicht mehr beachtet, da sie die falsche MAC-Adresse enthalten. Somit kann der Angreifer sich nun dem Client gegenüber ungehindert als der Server ausgeben.

- **DNS Spoofing**

  DNS Spoofing bezeichnet eine Angriffsmethode, bei der ein Angreifer die Antwort auf die DNS-Anfrage des Clients nach der IP-Adresse des authentifizierenden Web-Servers dahingehend manipuliert, dass diese seine eigene IP-Adresse enthält. Je nach Rahmenbedingungen kann er dazu z. B. die Anfrage abhören und dann (unter Spoofing der IP-Adresse des DNS-Servers) eine entsprechend gefälschte Antwort an den Client senden. Falls er dies schneller tut, als der eigentliche DNS Server, wird der Client dieser Fehlinformation folgen und die HTTPS-Sitzung zur IP-Adresse des Angreifers aufbauen. Alternativ kann auch mit Hilfe des Cache Poisoning der DNS-Server dazu gebracht werden, die gefälschte Information zu übermitteln; Voraussetzung hierfür ist allerdings, dass der DNS-Server nicht selbst der autorisierte Server für die DNS-Zone des Hotspot-Web-Servers und außerdem für diese Art Angriff anfällig ist. Letzteres ist bei aktuellen DNS-Implementierungen in der Regel nicht mehr der Fall.

- **DHCP Spoofing**

  Beim DHCP Spoofing liefert der Angreifer dem Client gefälschte DHCP Options, indem er die jeweiligen DHCP-Offer- bzw. DHCP-Acknowledge-Pakete schneller an den Client sendet, als der etatmäßige DHCP Server. In den DHCP Options gibt er jeweils seine eigene, ggf. manipulierte IP-Adresse an. Als Options kommen aus Sicht des Angreifers u. a. die folgenden in Frage:

  - DNS-Server

    Damit vereinfacht er ein nachfolgendes DNS-Spoofing, da er vom Client gezielt mit dem DNS-Request bedacht wird.

  - Gateway

    Indem er sich als das Default-Gateway des Clients ausgibt, erreicht er, dass alle Pakete, sofern sie das Subnetz des Clients verlassen, an ihn gesendet werden.

    Damit dieser Angriff letztlich sein Ziel erreicht, muss er außerdem dem Client eine Adresse aus einem Subnetz zuteilen, das nicht mit dem Subnetz des authentifizierenden Web-Servers übereinstimmt. Die gelieferte Gateway-Adresse muss in diesem Fall ebenfalls aus dem besagten Subnetz stammen. Um dem Client eine geeignete IP-Adresse zuzuteilen, reicht es bereits aus, wenn der Angreifer die Subnetzmaske geeignet verkleinert. Dies ist weniger auffällig als eine völlig fremde Adresse und insbesondere innerhalb der Pakete nicht sichtbar.

- **ICMP-Redirect-Attacke**

  Bei der ICMP-Redirect-Attacke nutzt der Angreifer ähnlich wie beim ARP Poisoning einen Standard-Mechanismus, in diesem Fall das Internet Control Message Protocol (ICMP). Der ICMP

Redirect teilt dem empfangenden System einen alternativen, besser geeigneten Router mit, über den dieses System fortan die betroffene Kommunikation abwickelt.

Der Angreifer sendet bei diesem Angriff seine eigene IP-Adresse als die des zuständigen Routers. Da der angegriffene Client daraufhin die Datenpakete an den Angreifer sendet, kann dieser alle Pakete an den authentifizierenden Server abfangen. Voraussetzung für diesen Angriff ist, dass sich der authentifizierende Server in einem anderen Subnetz befindet als der Client, da letzterer ansonsten den Gateway-Parameter nicht berücksichtigt.

Den genannten Gefährdungen durch ARP Poisoning, DHCP Spoofing, DNS Spoofing, ICMP Redirect und ähnliche Angriffe kann prinzipiell durch entsprechende herstellerspezifische Sicherheitsmaßnahmen an den Access Points und den Switches des Distribution System begegnet werden.

## 11.3 Zusammenfassung

Hotspots stellen in jeglicher Beziehung eine neue Herausforderung an alle Beteiligte – Betreiber wie Nutzer – dar. Sicherheit muss hier auf allen Ebenen von den Mechanismen auf MAC-Ebene bis hin zur Applikation implementiert und neu überdacht werden. Gerade durch die am Markt gängigen Systeme und Verfahren wird unter Sicherheitsaspekten zur Zeit zu wenig getan. Hier muss ein Umdenken erfolgen, was allerdings auch mit einer sicherheitsbewussteren Haltung der Benutzer einhergehen muss.

# 12 Absicherung mobiler Clients

Zur Illustration der Wichtigkeit einer sicheren Konfiguration (nicht nur) der mobilen Clients sei hier zunächst ein - nicht ganz unrealistisches - Szenario dargestellt:

„Ein Firmen-Laptop ist mit einer WLAN-Schnittstelle ausgerüstet, welche bei der Sicherheitskonfiguration von Clients nicht weiter beachtet wurde – z. B. weil die Sicherheitsrichtlinien der Unternehmung bzw. der Behörde noch nicht für diesen Fall aktualisiert wurden oder gar, weil der Benutzer über USB unerlaubt einen WLAN-Adapter angeschlossen hat. Ohne entsprechende Vorkehrungen ist damit der Benutzer in der Lage z. B. an einem öffentlichen Hotspot am Netzwerk teilzunehmen. Ein Angreifer nimmt in der Nähe des eingeschalteten Laptops einen Access Point in Betrieb, dessen SSID auf einen öffentlichen Hotspot hindeutet. Der Benutzer verbindet sich zu diesem Access Point in der Erwartung, die Dienste eines seriösen Hotspot-Betreibers nutzen zu können. Der Angreifer nutzt die nun bestehende Netzwerk-Verbindung, um gegen den mobilen Client Angriffe zu starten, indem er z. B. versucht, bekannte Sicherheitsschwächen des Systems zu finden und diese auszunutzen. Geeignete Lücken vorausgesetzt (Betriebssystem, Internetbrowser etc.), kann der Angreifer auf diese Weise z. B. einen so genannten „keystroke logger“ zur Ausführung bringen, welcher sämtliche Tastaturanschläge des Nutzers aufzeichnet und dem Angreifer zur Verfügung stellt – auch das Erstellen von „screenshots“ wäre auf diese Weise möglich.“

Es ist sicher eine sehr unangenehme Vorstellung, wenn das oben beschriebene Szenario zu einer Veröffentlichung von Daten mit hohem Schutzbedarf führen würde.

Die Nutzung insbesondere von fremden bzw. unbekannten WLAN muss man also sicherheitstechnisch im Allgemeinen mit dem Einstecken eines Netzwerkkabels in einen fremden Hub (nicht Switch) vergleichen. Dieses Einstecken von Kabeln ist zwar ebenso eine Gefahr, die oftmals nicht ausreichend bedacht wird, jedoch wird ein solcher Anschluss von Geräten an fremde Netze zumindest meist in Form von Vorschriften untersagt – und es gibt hier, so ist zu hoffen, auch für den unbedarften Anwender instinktiv eine gewisse Hemmschwelle. Bei WLANs ist dies aber meist nicht der Fall – schließlich werden entsprechende Dienste allerorts angeboten und der praktische Nutzen kann eben auch sehr groß sein. Ebenso wie das Internet bergen öffentliche (oder auch nur scheinbar vertraute) WLAN sehr vielschichtige Gefahren, die es abzuwehren gilt.

## 12.1 Sicherheitspatches

Ein wichtiger Gesichtspunkt zur Absicherung mobiler WLAN-Clients ist die Pflege des Client-Betriebssystems (Operating System, OS) und wichtiger Applikationen (insbesondere auch Internetbrowser) im Hinblick auf die Schließung von Sicherheitslücken; mittlerweile sind auch Personal Firewalls und Virenschutzprogramme selbst das Ziel von Angriffen. Vielfach können andernfalls Angreifer Schwächen ausnutzen, die bereits lange Zeit öffentlich bekannt sind und für die es unter Umständen bereits seit geraumer Zeit entsprechende Korrekturmittel (Patches) gibt – aber eben ggf. auch Angriffswerkzeuge. Eine dahingehende permanente Pflege der Systeme ist ganz allgemein anzuraten und nicht speziell nur für WLAN-Clients empfehlenswert – gerade für mobile Clients ist aber diese Empfehlung zu unterstreichen.

Es ist ratsam, durch geeignete technische Maßnahmen für eine derartige Pflege der Systeme zu sorgen. Hierzu können beispielsweise OS-spezifische Verfahren verwendet werden. Softwaremanagement-Produkte bieten vielfach solcherlei Möglichkeiten, und auch eigens für diese Zwecke geschaffene Produkte sind erhältlich. Oft unterstützen Applikationen auch eigene Mechanismen zum Update (wie z. B. Virenscanner oder Sicherheits-Tools); nicht immer sind diese allerdings sicherheitsrelevant. Manchmal ergeben sich auch erst durch scheinbare Verbesserungen neue Angriffsmöglichkeiten. Meist wird aber ein regelmäßig gepflegtes System weniger Verwundbarkeiten aufweisen als ein „ungepflegtes“. Grundsätzlich ist empfehlenswert, ein Verfahren zu wählen, bei dem der Administrator auch die Möglichkeit der Auswahl hat, welche Updates oder Patches eingespielt werden sollen und welche nicht.

Für die weit verbreiteten Windows-Clients bietet es sich an, möglichst moderne Versionen des OS nebst zugehörigen Service Packs zu wählen. Beispielsweise verwaltet MS Windows XP die privaten Schlüssel zu Zertifikaten sicherer als MS Windows 2000, siehe [MSKB03]. Besonders für den Fall, dass der Client nicht Mitglied einer Active-Directory-Domäne ist, ist dies von Bedeutung, da andernfalls bei Diebstahl des Clients unter anderem die privaten Schlüssel von Softwarezertifikaten gefährdet sind. Zu der auch in diesem Zusammenhang erneut wichtigen Wahl von sicheren Benutzerkennwörtern sei auf das Kapitel 12.4 verwiesen.

## 12.2 Personal Firewall

Je stärker ein Client-System Angriffen ausgesetzt ist, desto wichtiger ist es, geeignete Techniken zu dessen Schutz einzusetzen. Personal Firewalls (PFs) können hierzu einen wichtigen Teil beitragen.

Solche PFs können bestimmte Arten von Netzwerkverkehr erlauben bzw. verbieten, ähnlich zu den bereits wesentlich länger gebräuchlichen „normalen“ Firewalls zur Absicherung von Netzen. Grundsätzliche Idee ist, dass nur solcher Netzwerkverkehr zugelassen wird, der für die beabsichtigte Funktion des Clients erforderlich ist. Die meisten dieser Systeme bieten u. a. die Möglichkeit, nur denjenigen eingehenden Netzwerkverkehr zuzulassen, der von innen, also vom Client-System selbst, initiiert wurde. Beispielsweise dürfen nur dann Netzwerkpakete von Port 80 (HTTP) eines Web-Servers die PF passieren, wenn der Benutzer eine solche Art von Paketen von diesem Server auch angefordert hat. Diese Art von Filterung wird gelegentlich auch als SPI (Stateful Packet Inspection) bzw. SPF (Stateful Packet Filtering) bezeichnet; die PF arbeitet auf Verbindungsebene.

Diese Art von Filterung kann bereits eine ganze Reihe von Angriffen verhindern oder erschweren, sie alleine schützt allerdings prinzipbedingt z. B. nicht vor so genannten „Trojanischen Pferden“ oder kurz Trojanern. Solche Trojaner sind zumeist schadenstiftender Code (Malicious Code, Malware), welcher Informationen auf dem hiermit infizierten System sammelt und diese über ein Netzwerk dem Angreifer bereitstellen kann. Es sind bereits Werkzeuge zur Erstellung ganzer trojanischer Systeme in Umlauf, mit denen auch ein Laie solchen Code erzeugen kann; nebst Verfahren zur Infizierung und zum Sammeln von Informationen. Falls also ein System auf anderem Wege (z. B. über die WWW-Nutzung) mit einem Trojaner infiziert wurde (ein Virenscanner dies also nicht unterbinden konnte), kann eine auf Verbindungsebene arbeitende Firewall zunächst nicht verhindern, dass diese „Malware“ Informationen auch versendet; die Netzwerkpakete stammen ja von innen. Es gibt jedoch auch PF-Produkte, die nur ausgehenden Verkehr von festzulegenden Applikationen zulassen. Besonderns dann, wenn dies durch geeignete Maßnahmen sicher gestaltet werden kann, z. B. durch Vergleichen einer Prüfsumme (Hash) der Applikation, um deren schadhafte Veränderung auszuschließen, so kann dies die Sicherheit weiter erhöhen – vielfach zum Preis einer aufwändigeren Administration.

Weiterhin beinhalten gewisse Trojaner als Schadfunktion die Fähigkeit, bekannte Antivirensoftware oder PFs abzuschalten. Damit kann ggf. die gesamte Host-basierte Systemsicherheit nicht nur umgangen sondern nachhaltig verhindert werden. Dies ist insbesondere dann der Fall, wenn der angemeldete Anwender, in dessen Kontext der Trojaner gestartet wird, über zu weitgehende Rechte am System verfügt (vgl. Kapitel 12.5.1).

Zu beachten ist bei PFs außerdem, dass auch bestimmte Arten von eingehendem Verkehr in der praktischen Verwendung oft zugelassen werden müssen, z. B. um die Verwaltbarkeit des Clients im Behörden- bzw. Firmennetz sicherzustellen. Die zu einer solchen PF-Lösung gehörige Konfiguration sollte daher möglichst zentral administrierbar sein und sehr sorgfältig vorgenommen werden, um größtmögliche Sicherheit[33] zu erreichen. Auch ist zu berücksichtigen, dass die PF mindestens für die gefährdeten Interfaces eingeschaltet ist. Manchmal ist zwar eine einfache PF im Betriebssystem enthalten, je-

[33] Ein möglicher Fehler könnte z. B. sein, lokale Subnetze des Clients automatisch zur Liste vertrauenswürdiger Netze hinzuzufügen. Für feststehende Rechner im Firmennetz mag dies manchmal sogar tragbar sein. Gerade im Bereich der drahtlosen Netze ist dies aber tückisch, da sehr leicht (ggf. sogar automatisch) ein nicht vertrauenswürdiges Netz (wie das WLAN eines Hotspot) zu einem lokalen Subnetz des Clients wird.

doch oft standardmäßig nicht aktiviert[34]; insbesondere nicht für Netzwerkadapter, die durch Einstecken im laufenden Betrieb hinzukommen. Hierauf ist also besonderes Augenmerk zu legen. Ebenfalls ist die Implementierung von Werkzeugen zu erwägen, welche ein solches Hinzufügen von Geräten durch den Nutzer einschränken oder verhindern können (siehe auch Kapitel 12.5.2).

Auch Personal Firewalls sind keine WLAN-spezifische Technologie. Für die drahtlosen Netze haben sie aber wiederum besondere Relevanz, da hier die Angriffsfläche recht groß ist. Es können an dieser Stelle bei weitem nicht alle Aspekte von PFs betrachtet werden; nur einige Grundfunktionen und -überlegungen wurden angesprochen. Es empfiehlt sich ggf. weitere Literatur zu Rate zu ziehen.

Keinesfalls ist eine Personal Firewall als Ersatz für andere Sicherheitsmaßnahmen, wie Sicherheitskonfiguration, Virenschutz oder Einpflegen von Sicherheitspatches usw., anzusehen – nur die Kombination verschiedener Techniken bringt die höchste erreichbare Sicherheit.

## 12.3 Virenschutz

Wie bereits an verschiedenen Stellen angedeutet, existieren mannigfaltige Bedrohungen für Computer, sei es, dass sie direkt mit dem Internet verbunden sind oder in einem LAN oder WLAN stehen. Einigen dieser Bedrohungen kann mit Maßnahmen begegnet werden, die unter den Oberbegriff Virenschutz fallen. Hiermit ist nicht nur der Schutz vor klassischen Viren (Boot-, File-, und Makroviren sowie speicheresidente Viren) und deren Auswirkungen gemeint, sondern auch vor den bereits genannten Trojanischen Pferden und den vor allem in letzter Zeit immer stärker auftretenden sog. Würmern – letztlich bedeutet der Begriff Virenschutz in der Praxis nichts anderes als Schutz von Computern vor schadenstiftendem Code.

Im Bereich der Client Computer sollte zu diesem Zweck – wie bereits im vorigen Kapitel beschrieben – als eine von mehreren Maßnahmen eine gut konfigurierte Personal Firewall eingesetzt werden. Darüber hinaus haben sich in der Vergangenheit Viren-Suchprogramme bewährt, die das System nach bekannten Viren durchsuchen und ggf. Gegenmaßnahmen einleiten. Aktuelle Virenschutzprodukte führen diese Suche in der Regel permanent im Hintergrund durch und bieten teilweise durch Schnittstellen zu gängigen Internet-Programmen (Browser, Mail-Client u. a.) zusätzlich Schutz vor schadenstiftendem Code, der durch die entsprechenden Programme übertragen wird (z. B. in Form von bösartigen Java Applets und ActiveX-Controls). Über tatsächliche Malware hinaus – die Grenzen sind jedoch fließend – existieren noch weitere „Störenfriede“, die nicht selten in die Kategorien „Spyware“, „Adware“, „Hijacker“ und „Dialer“ einzuordnen sind und von vielen Virensuchprogrammen ebenfalls erkannt und gebannt werden können. Es existieren hierzu jedoch auch spezialisierte, teils frei verfügbare Schutzprogramme.

Allen Programmen zum Schutz vor schadenstiftendem oder unerwünschtem Code gemeinsam ist ihr Bedürfnis nach Aktualität – ein Computer kann nur dann optimal geschützt werden, wenn die installierten Schutzprogramme über aktuelle Informationen zu potentiellen Bedrohungen verfügen.

> Für die Client-Systeme ist der Einsatz einer Virenschutzsoftware, die regelmäßig aktualisiert wird, unbedingt zu empfehlen.

Im professionellen Umfeld sollten aus diesem Grund möglichst Produkte eingesetzt werden, die von zentraler Stelle aus konfiguriert und in regelmäßigen und kurzen Abständen aktualisiert werden. Hierbei ist insbesondere bei mobilen Clients darauf zu achten, dass diese ebenfalls durch eine Lösung auf praktikable Weise in die zentrale Administration und ein Verfahren zum Update mit einbezogen werden.

Gerade im Zusammenhang mit diversen Schutzmechanismen ist noch ein weiterer Hinweis angebracht: Sofern nicht unbedingt erforderlich, sollten Benutzer keinesfalls über Administratorrechte ver-

[34] Dies hat sich mit Service Pack 2 für MS Windows XP geändert: Hier ist die nun „Windows Firewall“ genannte PF mitsamt der bestehenden Regelbasis auch für neu hinzukommende Interfaces standardmäßig automatisch aktiviert.

fügen (siehe auch Kapitel 12.5.1). Einerseits kann hierdurch weitestgehend verhindert werden, dass mühsam aufgebaute Sicherheitsmechanismen durch die Benutzer einfach abgestellt oder unterlaufen werden können, andererseits sind viele der oben genannten Schädlinge ohne einen unwissentlich „helfenden“ Administrator wesentlich weniger effektiv, da sie sich nicht oder nur deutlich schwieriger dauerhaft in das System einbinden können.

Auch in Bezug auf Viren, Trojaner, Würmer etc. muss jedoch festgestellt werden, dass es niemals einen absoluten Schutz geben kann. Seit es Schädlinge dieser Art gibt, liefern sich deren Erschaffer und die Entwickler von Schutzprogrammen einen regelrechten Wettlauf, in dem allerdings letztere immer der zweite Sieger sind, da sie auf neue Schädlinge meist erst dann wirksam reagieren können, wenn diese einen gewissen Verbreitungsgrad erlangt haben. Nichtsdestotrotz vermindern die Schutzprogramme das Risiko einer Infektion beträchtlich, da die Reaktionszeiten der Hersteller mittlerweile extrem kurz sind.

## 12.4 Integritätsprüfung der Client-Konfiguration

Verschiedene Hersteller bieten Systeme an, die eine Integritätsprüfung der Client-Konfiguration durchführen und den Netzzugang abhängig von dem Ergebnis dieser Prüfung machen. Ein Client, dessen Virenschutz beispielsweise nicht mehr auf dem neuesten Stand ist (und so eine potentielle Bedrohung darstellt), kann etwa nach der Anmeldung am Netz automatisch in ein von der weiteren LAN-Infrastruktur isoliertes Quarantäne-VLAN gesetzt werden, um den Virenschutz zu aktualisieren. Hierzu ist typischerweise eine Komponente auf dem Client erforderlich, welche lokal die Integritätsprüfung vornimmt. Das Resultat der Prüfung wird durch eine spezielle EAP-Methode über IEEE 802.1X an einen RADIUS Proxy übertragen. Der RADIUS Proxy ist die zweite (herstellerspezifische) Komponente bei der Integritätsprüfung. Dieser Server wertet das Prüfergebnis aus und dient als Bindeglied zum eigentlichen Authentication Server, der die Authentifizierung bearbeitet. Für den Authentifizierungsprozess ist die Prüfung der Client-Konfiguration unsichtbar (siehe Abbildung 41). Wenn sowohl die Authentifizierung als auch die Integritätsprüfung erfolgreich waren, erhält der Client einen Zugang zum Netz. Andernfalls kann der Client abgewiesen werden oder nur einen eingeschränkten Zugang erhalten.

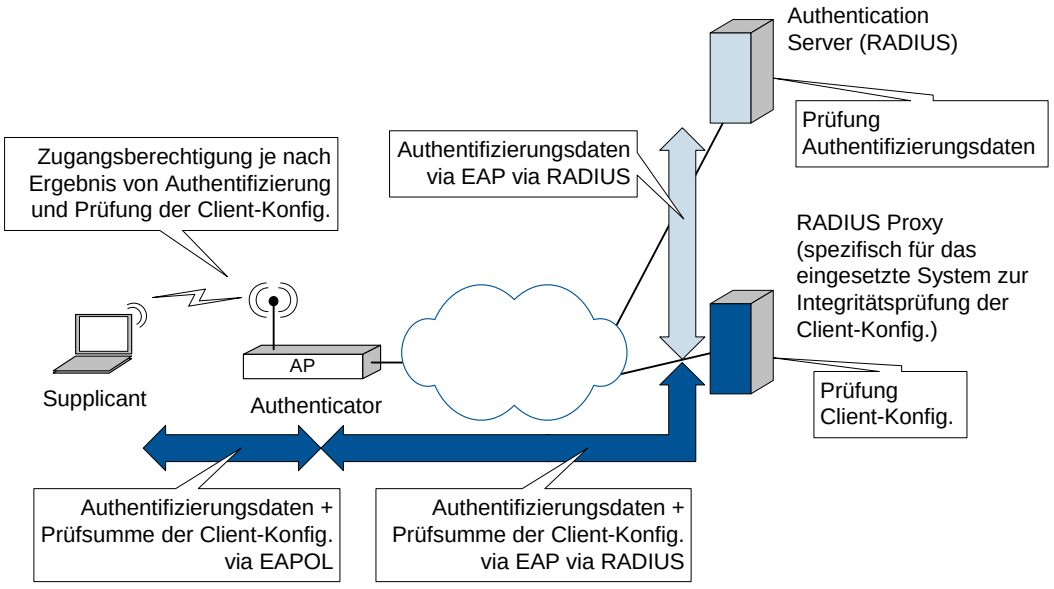



Abbildung 41: Integritätsprüfung der Client-Konfiguration über EAP

## 12.5 Sicherheitskonfiguration des Client-Betriebssystems

Nachfolgend sollen einige wichtige Themengebiete genannt werden, die bei der sicheren Konfiguration des Betriebsystems auf den Client-Rechnern (wie z. B. auch mobile Notebooks), beachtet werden sollten. Die genannten Hinweise können aber bei weitem nicht alle Felder der Sicherheit von Clientbetriebssystemen berücksichtigen. Hauptaugenmerk liegt bei der Betrachtung auf solchen Clients, die von Firmen- oder Behördenmitarbeitern beruflich genutzt werden und welche zentral durch eine IT-Abteilung verwaltet werden (Managed Clients).

### 12.5.1 Vermeidung von Administrations-Konten

Um sich vor den vielfältigen möglichen Bedrohungen und Angriffen zu schützen, ist es zumeist wichtig, dass die von den Verantwortlichen vorgesehenen Maßnahmen und Konfigurationen eines Systems nicht vom Anwender (ob absichtlich oder unbeabsichtigt) geändert werden können.

Es ist unter anderem auch daher dringend zu empfehlen, dass der normale Anwender eines Client-PCs, kein Benutzer mit weitgehenden Rechten oder Berechtigungen (Administrator oder Superuser) ist.

Dies bedeutet z. B. bei MS Windows-Systemen unter anderem, dass der Anwender kein Administrator-Benutzerkonto benutzen sollte, also nicht Mitglied der Gruppe der Administratoren oder gar der Domänen-Administratoren ist. Unter Linux sollte der Anwender beispielsweise keinesfalls root-Rechte und nur eingeschränkten Zugriff auf System-relevante Dateien haben.

Falls ein Anwender nämlich über solcherlei Rechte und Berechtigungen verfügt, kann er letztendlich sämtliche Konfigurationen ändern und auch wichtige Tools wie z. B. eine Personal Firewall oder den Virenscanner außer Funktion setzen. Des Weiteren ist ein Administrator-Konto auch bei der Internetnutzung unbedingt zu vermeiden, da schadenstiftender Code (siehe auch Kapitel 12.3), der unter diesem Benutzerkontext ausgeführt wird, besonders gefährlich ist – ein Administrator kann diesen Code mit viel weitergehenden Möglichkeiten ausführen[35], als ein gewöhnlicher Benutzer. Unter anderem kann die dauerhafte Installation von Trojanischen Pferden so leichter erreicht werden.

Eine wichtige Voraussetzung für den Schutz, der bei Nutzung weniger privilegierter Benutzerkonten erreicht werden kann, ist jedoch unter MS Windows-Systemen die Nutzung des Dateisystems NTFS bzw. im Falle von UNIX-Systemen die sachgerechte Verwendung von Dateizugriffsberechtigungen.

### 12.5.2 Härtung des Client-Systems

Unbedingt empfehlenswert sind auch betriebsystemspezifische Härtungsmaßnahmen. Hierzu können die für das jeweilige System verfügbaren Literatur-Quellen zur Sicherheit sowie auch Internet-Angebote zu diesem Thema genutzt werden, um für die beabsichtigte Funktion des Systems eine sicherheitsoptimierte Konfiguration zu erreichen.

Das Härten sollte sich nicht nur auf das Einspielen von Sicherheits-Patches (siehe auch Kapitel 12.1) und anderen Updates wie Service Packs beschränken, sondern u. a. auch das gezielte Deaktivieren von nicht benötigten Funktionalitäten des Systems und dessen Software einschließen.

Wenngleich diese Aufgabe weder leicht noch pauschalisierbar ist, sollte jeder, der die Sicherheit von Clients – insbesondere solcher, die auch an WLANs teilnehmen sollen – zu verantworten hat, mit den spezifischen Methoden zur Härtung des OS vertraut sein. Beispiele hierfür können unter MS Windows das Deaktivieren des Nachrichtendienstes, das Einschalten einer (ggf. integrierten) Personal Firewall

[35] Derzeit benötigen beispielsweise die meisten in Umlauf befindlichen „E-Mail-Würmer“ Zugriffsberechtigungen, welche im Normalfall nur ein Administrator-Konto hat, um ihre volle Wirkung zu entfalten.

auf dem WLAN-Interface oder die Konfiguration eines Kennwortes zum Systemstart (Syskey) sein. Unter Unix sind das Nutzen einer shadow-Datei oder die sachgerechte Verwendung von Gruppenmechanismen ebenso Beispiele wie auch das Ergreifen von Abwehrmaßnahmen gegen so genannte „Root Kits“ oder das Anpassen der Datei /etc/inetd.conf.

Unter den Bereich der Client-Härtung im weitesten Sinne fällt auch die sichere Konfiguration von wichtigen Applikationen. Hierzu zählen insbesondere auch die Web-Browser.

Ob Internet Explorer, Netscape, Opera oder Mozilla, alle Browser sollten grundsätzlich derart konfiguriert werden, dass die nicht unbedingt notwendigen Funktionalitäten abgeschaltet sind.

Dies trägt dem Umstand Rechnung, dass eine Vielzahl von Schwachstellen in diesen Programmen existieren, welche einem Angreifer den vollständigen oder teilweisen Zugriff auf das Client-System erlauben. Jedoch wird auf vielen Internetseiten auf potentiell gefährliche Funktionen zurückgegriffen, so dass hier ein schwieriger Kompromiss zwischen Anwenderfreundlichkeit bzw. Nutzbarkeit auf der einen Seite und Sicherheit auf der anderen Seite gefunden werden muss. Auch wenn oftmals in der Praxis der Kompromiss zu Ungunsten der Sicherheit ausfällt: Die Unsicherheit von Web-Zugriffen darf nicht unterschätzt werden. Informationsbasis für eine sichere Konfiguration z. B. des Internet Explorers von Microsoft kann das Internetangebot des BSI unter www.bsi.bund.de sein. Es sei nochmals darauf hingewiesen, dass besonders für den Bereich WLAN die sicherste Konfiguration des Web-Browsers zu teils massiven Einschränkungen bei der Benutzung führt, denn bei vielen WLAN Hotspots kann unter Umständen das Angebot gar nicht genutzt werden.

Da bei modernen Systemen meist auch die Möglichkeit besteht, Hardware im laufenden Betrieb anzuschließen, ist eine weitere potentielle Sicherheitslücke entstanden. Wenn auch organisatorisch das unerlaubte Anschließen von nicht genehmigter Hardware zu untersagen ist, ist es nicht immer ganz leicht, dieses Verbot auch technisch durchzusetzen. Es gibt jedoch auch für diesen Zweck mittlerweile Produkte bzw. Möglichkeiten, so dass Nutzer ohne Administrationsrechte nur eingeschränkt neue Geräte in Betrieb nehmen können, z. B. nur vorher benannte USB-Geräte. Auch hier ist wieder ein Kompromiss zwischen Flexibilität und Sicherheit zu finden, jedoch sollte auch dieses Thema bei der Planung von Client-Sicherheit berücksichtigt werden. Dies gilt im Übrigen nicht nur für mobile Clients, sondern auch für feststehende Geräte. Man denke nur an die Möglichkeit, auch Datenträger anschließen zu können. Unter Umständen kann es sogar sinnvoll sein, Schnittstellen, welche ein „Hot Plugging“ unterstützen, ganz abzustellen, auch wenn dies unter praktischen Gesichtspunkten immer schwieriger umzusetzen ist.

In diesem Zusammenhang sollte auch der Kennwortschutz des Rechner-BIOS nicht unerwähnt bleiben: Wenn der Anwender nicht ohne weiteres „in das BIOS“ gelangt, um Änderungen vorzunehmen (z. B. das Ändern der Boot-Reihenfolge, um von einem USB-Stick zu booten), dann ist hierdurch ein wichtiger Sicherheitsgewinn erzielt worden – auch wenn meist durch entsprechenden Hardware-Eingriff dieser Kennwortschutz umgangen werden kann.

Es ist auf Client-PCs ein Kennwortschutz für den Zugang zu den BIOS-Einstellungen zu empfehlen.

### 12.5.3 Verwendung komplexer Kennwörter

In nahezu allen Fällen, in denen vom Benutzer einzugebende Kennworte verwendet werden, sind diese ein möglicher Angriffspunkt zur Kompromittierung der Sicherheit. Daher ist es dringend zu empfehlen, alle Arten von Kennwörtern (auch die Benutzerkennwörter) möglichst komplex zu gestalten – insbesondere kurze Kennwörter sollten tabu sein. Meist lassen sich solche Vorgaben mittels Richtlinien durchsetzen, z. B. unter gängigen Linux-Distributionen für lokale Accounts bereits bei der Installation (mit grafischer Unterstützung auch für weniger versierte Anwender) oder unter MS Windows im Active Directory über die Kennwortrichtlinien. Die Benutzer sollten darauf hingewiesen werden, keinesfalls leicht zu erratende Kennwörter zu wählen oder solche, die in einem Wörterbuch stehen könnten; auch Eigennamen von Personen, Musikgruppen, Fernsehserien etc. sind ungeeignet. Dies

betrifft insbesondere auch die Kennworte von Administratorkonten, wie adm, sys, root oder unter MS Windows z. B. das des lokalen Administrators.

Es sollten unbedingt komplexe Kennwörter verwendet werden, um ein Mindestmaß an Sicherheit zu erreichen. Einfache Kennwörter, womöglich sogar solche, die über Wörterbuchangriffe ermittelt werden können, sind keinesfalls ausreichend.

Die Wahl von komplexen Kennwörtern kann aber nicht nur für eine sichere Authentifizierung erforderlich sein, sondern auch Auswirkungen auf die Angreifbarkeit z. B. von mit EFS (Encrypting File System) verschlüsselten Dateien haben. Bei schwachen Kennwörtern sind auch die verschlüsselten Dateien dann letztlich weniger stark geschützt – ebenso wie weiteres Schlüsselmaterial.

Grundsätzlich empfehlenswert, aber ggf. nicht überall anwendbar, ist der Einsatz von Hardwarebasiererter Kryptografie, beispielsweise durch Einsatz von Smartcards oder Token (welche kryptografische Verfahren im Gerät selbst durchführen). Hierdurch lassen sich in vielen Bereichen die Schwächen von Kennwörtern u. a. bei der Benutzerauthentifizierung umgehen oder reduzieren.

### 12.5.4 Verschlüsselung von Dateien

Sofern auf der Festplatte eines Clientsystems auch schützenswerte Daten gespeichert werden (dies ist in sehr vielen Fällen der Fall, wenn auch oft erst auf den zweiten Blick zu erkennen), ist eine geeignete Verschlüsselung solcher Dateien bzw. Verzeichnisse oder der gesamten Festplatte anzuraten.

Die Verschlüsselung von Daten auf der Festplatte ist insbesondere bei personenbezogenen Daten eine wichtige Sicherheitsmaßnahme, die auch juristisch in Hinblick auf das Bundesdatenschutzgesetz relevant ist.

Dies ist insbesondere bei mobilen Clients wichtig, da das Diebstahlrisiko hier größer ist. Da sich ein Angreifer, der physisch vollständigen Zugriff auf ein Gerät hat, über nahezu alle Arten von Zugriffsschutz hinwegsetzen kann, ist meist nur auf solche Weise ein Schutz auf Dateiebene erreichbar. In diesem Bereich ist eine Vielzahl von Produkten unterschiedlichster Preis- und Leistungsklassen verfügbar; auch vom Anspruch und vom Administrationsaufwand sowie von der Skalierbarkeit unterscheiden sich die Produkte stark.

Unter MS Windows sollte u. a. beachtet werden, dass bei Einsatz von EFS (Encrypting File System) auch temporäre Dateien und die so genannten Offline-Dateien“ verschlüsselt werden sollten, damit nicht auch unverschlüsselte Versionen von schützenswerten Dateien auf dem Datenträger abgelegt werden. Sowohl EFS als auch ganz allgemein alle Verfahren zur Verschlüsselung von Dateien und Verzeichnissen oder auch Festplatten bedürfen einer sorgfältigen Planung des Einsatzes – hier sollte sehr gewissenhaft vorgegangen werden. Als nur ein Beispiel für die Themengebiete, die hierbei Beachtung finden sollten, sei die Frage der Wiederherstellbarkeit für den Fall des Schlüsselverlustes genannt.

## 12.6 WLAN Client-Konfiguration

Es lässt sich leider nur schlecht verallgemeinern, welche Maßnahmen auf Client PCs für die WLAN-Konfiguration zur Erhöhung der Sicherheit geeignet sind, da die Anforderungen sehr unterschiedlich sein können: Der „Hotspot-Nomade“, welcher über verschiedenste öffentliche Hotspots das Internet nutzen möchte (und soll), bringt ganz andere Randbedingungen mit als das Notebook eines Personalchefs, der vertrauliche Daten ausschließlich über ein stark gesichertes, firmeneigenes WLAN bearbeiten soll. Besonders letzterer Fall wird im Folgenden betrachtet.

### 12.6.1 Assoziierung zu fremden WLAN

Bei der Konfiguration von möglichst sicheren WLAN Clients ist auch die Auswahl der Client-Software wichtig. Das gewählte Produkt sollte es erlauben, dass ein Administrator die sicheren Einstellungen vornehmen und der spätere Benutzer diese nicht mehr beeinflussen kann. Der WLAN Client sollte sich ferner auch nicht zu beliebigen Netzen in Funkreichweite assoziieren dürfen oder dies gar automatisch tun.

Die automatische Assoziation zu verfügbaren Funknetzwerken sollte deaktiviert werden.

Für Rechner mit mehr als nur geringem Schutzbedarf sollte der Benutzer keine Möglichkeit haben, sich zu anderen als den vorkonfigurierten drahtlosen Netzen zu verbinden.

Dies ist besonders wichtig, da ein unerfahrener Benutzer ansonsten ggf. auch neue drahtlose Netze hinzufügt („weitere SSID"), bei welchen er dann u. U. auch schwache Authentifizierungsverfahren wählen, auf gegenseitige Authentifizierung verzichten oder gar ohne Verschlüsselung arbeiten kann.

Für den Hotspot-Nomanden ist das (empfehlenswerterweise nach entsprechender Schulung) durchaus denkbar, für den Personalchef jedoch keinesfalls. Ein Angreifer könnte andernfalls zum Beispiel einen Access Point vor dem Büro des Personalchefs in Betrieb nehmen, zu dem sich der vielleicht unvorsichtige Chef assoziiert, anschließend kann der Angreifer „testen", ob der PC des Personalchefs über eine Personal Firewall verfügt, und falls nicht, einen „Test" der Qualität des Administrator-Kennwortes durchführen (einige durchaus häufig zutreffende Randbedingungen vorausgesetzt).

Sollte der Personalchef nun aber auch gleichzeitig Hotspot-Nomade sein dürfen, so ist es ungleich schwieriger, den Client vor ungebetenen Gästen zu schützen. Ohne geeignete Schutzmaßnahmen (unter anderem auch eine sicher konfigurierte Personal Firewall) sollte dies nicht in Erwägung gezogen werden.

Grundsätzlich ist zu empfehlen, Rechner mit mehr als nur geringem Schutzbedarf nicht als Reise-Rechner für Hotspot-Benutzer zu verwenden.

### 12.6.2 Problembereich Ad-hoc-Modus

Nur in wenigen Fällen werden im Ad-hoc-Modus wichtige Sicherheitsfunktionen unterstützt (da auch WPA diese Unterstützung nicht erfordert) und auch durch die Verfügbarkeit von preisgünstigen Access Points spielen die Computer-zu-Computer-Netze im Bereich WLAN zur Zeit keine wesentliche Rolle.

Da heute überwiegend WLANs im Infrastrukturmodus relevant sind, empfiehlt es sich aus Sicherheitssicht im Allgemeinen, in der Client-Konfiguration den Ad-hoc-Modus zu deaktivieren.

### 12.6.3 Geräte- und Nutzerauthentifizierung

Vorsicht ist auch geboten, wenn zwar durch die Software ein starkes Authentifizierungsverfahren vorgegeben wird, der Benutzer aber frei entscheiden kann, ob er z. B. dem Serverzertifikat vertraut. Da die wenigsten Benutzer sich über die Konsequenzen eines Vertrauens in ein Zertifikat im Klaren sind, sollte diese Entscheidung möglichst nicht dem Nutzer überlassen werden – oder nur nach sorgfältiger Schulung, möglichst nur im Ausnahmefall.

Es sollten nur sichere Authentifizierungsverfahren im WLAN vorgeschrieben werden, bei hohem Schutzbedarf möglichst solche, die gegenseitige Benutzer- und gegenseitige Computerauthentifizierung unterstützen.

Besonders die Computerauthentifizierung ist dann beachtenswert, wenn man verhindern möchte, dass ein Nutzer sich von einem unsicheren Rechner aus zu einem Firmennetzwerk verbindet. Leider ist in der Praxis eine kombinierte Geräte- und Nutzerauthentifizierung nicht so einfach umzusetzen, da nur wenige Verfahren alle notwendigen Möglichkeiten bieten (z. B. EAP-FAST unter Verwendung von EAP-TLS) und sowohl Supplicant als auch Authentication Server diese Art der Nutzung von EAP-Methoden unterstützen müssen..

### 12.6.4 Verteilung von Konfigurationen

Vorgaben für die Konfiguration von WLAN-Clients sollten von zentraler Stelle automatisch auf die Clients verteilt werden[36]. Dies verringert das Risiko von Fehlkonfigurationen erheblich. Eine solche Konfiguration würde beispielsweise die Liste der SSIDs, in die sich der Client einbuchen darf, enthalten und die zugehörigen Einstellungen für Verschlüsselung und Authentifizierung festlegen. Bei MS Windows-Clients können beispielsweise Vorgaben an die WLAN-Konfiguration als Gruppenrichtlinienobjekte (GPOs, Group Policy Objects) verteilt werden, sofern Windows die Einstellungen des WLAN-Adapters kontrolliert.

## 12.7 Zusammenfassung

Die Absicherung des Clients hat für die Gesamtsicherheit des Netzes eine nicht zu unterschätzende Bedeutung. WLAN-Infrastruktur und WLAN Client sind gleichermaßen zu schützen. Zunächst gelten für den Schutz des Clients im WLAN im Wesentlichen die selben Prinzipien, wie sie für den Schutz eines Clients beim Internet-Zugang zu beachten sind. Dies beinhaltet primär die folgenden Punkte:

- Verwaltung aus Sicherheitsperspektive der Softwarestände von Betriebssystem und Anwendungen, inklusive System- und Anwendungsparameter
- Deaktivierung nicht benötigter Dienste und Komponenten
- Einsatz einer Personal Firewall
- Implementierung eines Virenschutzes für den Client

Aufgrund des erhöhten Diebstahlrisikos eines mobilen Clients sind an dieser Stelle auch eine Benutzerauthentifizierung und eine Festplattenverschlüsselung als durchzuführende Maßnahmen zu nennen.

Die WLAN-spezifischen Aspekte der Client-Absicherung, die zu berücksichtigen sind, betreffen die Unterbindung einer automatischen Netzwahl, die Deaktivierung des Ad-hoc-Modus und die Problematik der Hotspot-Nutzung. Im letzteren Fall ist im Vergleich zur nicht-öffentlichen WLAN-Nutzung eine deutlich unsicherere Konfiguration von WLAN-Client-Adapter und Web Browser erforderlich.

[36] Dies ist bei einer größeren Zahl von WLAN Clients sinnvoll. Dagegen wird man bei WLAN im SOHO-Bereich diese Funktion selten antreffen.

# 13 Absicherung einer LAN-Kopplung

Eine wirtschaftliche Alternative zur kabelbasierten Verbindung zwischen Gebäuden und Grundstücken kann durch den Einsatz von WLAN-Technik gegeben sein. Die betreffenden LAN werden durch sogenannte Wireless Bridges gebäude- und grundstücksübergreifend über ein WLAN miteinander verbunden. Dies erfordert eine Sichtverbindung und meist den Einsatz spezieller Richtantennen. Bei der LAN-Kopplung steht also im Gegensatz zu den bisher betrachteten Techniken nicht die Mobilität der Nutzer im Vordergrund, sondern die Überbrückung einer gewissen Distanz, oft über öffentlichem Grund.

Gerade die „statische“ Nutzung der Punkt-zu-Punkt-WLAN und ihr Einsatz über öffentlichem Grund macht sie anfällig gegen Angriffe, da ein Angreifer sehr viel Zeit aufwenden kann und dabei unbemerkt bleibt. Eine wesentliche Anforderung an solche LAN-Kopplungen ist neben einer hohen Verfügbarkeit die Sicherstellung der Vertraulichkeit und Integrität der Daten bei ihrem Transport über Gelände, das sich meist jeglicher Kontrolle durch den Netzbetreiber entzieht.

Wesentliches Merkmal von WLAN zur LAN-Kopplung ist das Fehlen eines Client. Vielmehr handelt es sich um ein WLAN auf Basis zweier gleichberechtigter Endpunkte, eben der Wireless Bridges. Die Funktion einer LAN-Kopplung wird aber auch in einigen Access Points angeboten.

Es ist nun zu untersuchen, wie die in den vorangegangenen Kapiteln angesprochenen Mechanismen, die im Allgemeinen auf einer Client-Server-Struktur aufbauen, in der geschilderten symmetrischen Umgebung zu implementieren sind. In der Folge werden drei Lösungen dargestellt:

- Absicherung mittels VPN
- Absicherung mittels WPA-Personal bzw. WPA2-Personal
- Absicherung mittels WPA-Enterprise bzw. WPA2-Enterprise

Diese Lösungen adressieren zunächst nur das Problem des Schutzes der Vertraulichkeit und der Integrität. Der Schutz der Verfügbarkeit ist der auf Luftschnittstelle nicht mit einer hohen Sicherheit möglich, da unvorhersagbare Störungen auftreten können. Hier können lediglich redundante Übertragungswege geschaffen werden.

## 13.1 Absicherung mittels IP-VPN

Die grundsätzliche Idee besteht in einer Verbindung der Lokalen Netze über ein Paar VPN-Gateways. Das WLAN mit beiden Access Points bildet das unsichere Transportnetz, über das durch einen entsprechend verschlüsselten Tunnel den VPN-Gateways ein gesicherter Kommunikationskanal etabliert werden kann. Der Aufbau des Tunnels muss an eine geeignet starke Authentifizierung der Kommunikationspartner geknüpft sein.

Abbildung 42 zeigt die entsprechende Konfiguration. Es handelt sich also um ein „Site-to-Site VPN“, wie es auch zur Kopplung Lokaler Netze über das Internet allgemein eingesetzt wird. Auf die Diskussion der Parametrierung solcher VPN wird im Rahmen dieses Dokuments daher nicht weiter eingegangen.

Verschiedene Hersteller bieten Wireless Bridges an, die bereits ein VPN-Gateway enthalten. Mit Hilfe solcher Produkte lassen sich LAN-Kopplungen besonders preiswert realisieren. Zu bedenken ist hierbei jedoch, dass in diesem Fall das Ethernet-Anschlusskabel der Wireless Bridge keine verschlüsselten Daten transportiert, sondern unmittelbar mit dem LAN in Verbindung steht (vgl. Abbildung 43).

Bei Verwendung eines in eine Wireless Bridge integrierten VPN-Gateways muss der Betreiber dafür Sorge tragen, dass die LAN-Schnittstelle der Access Points gegen unbefugten Zugriff geschützt ist.

Im Einzelfall kann sich der Schutz der Ethernet-Anbindung der Wireless Bridge als schwierig gestalten, wenn die Wireless Bridge an einem Punkt zu installieren ist, der keine besonderen physischen Schutzmaßnahmen aufweist. Eigenständige VPN-Gateways lassen sich dagegen in Verteilerräumen bzw. Rechenzentren installieren, die mit entsprechenden Zugangskontrollsystemen ausgestattet sind.

Eine sichere LAN-Kopplung über VPN lässt sich erzielen, indem die VPN-Gateways von den Wireless Bridges getrennt und in geschützten Räumen (z. B. Rechenzentren) aufgestellt werden.

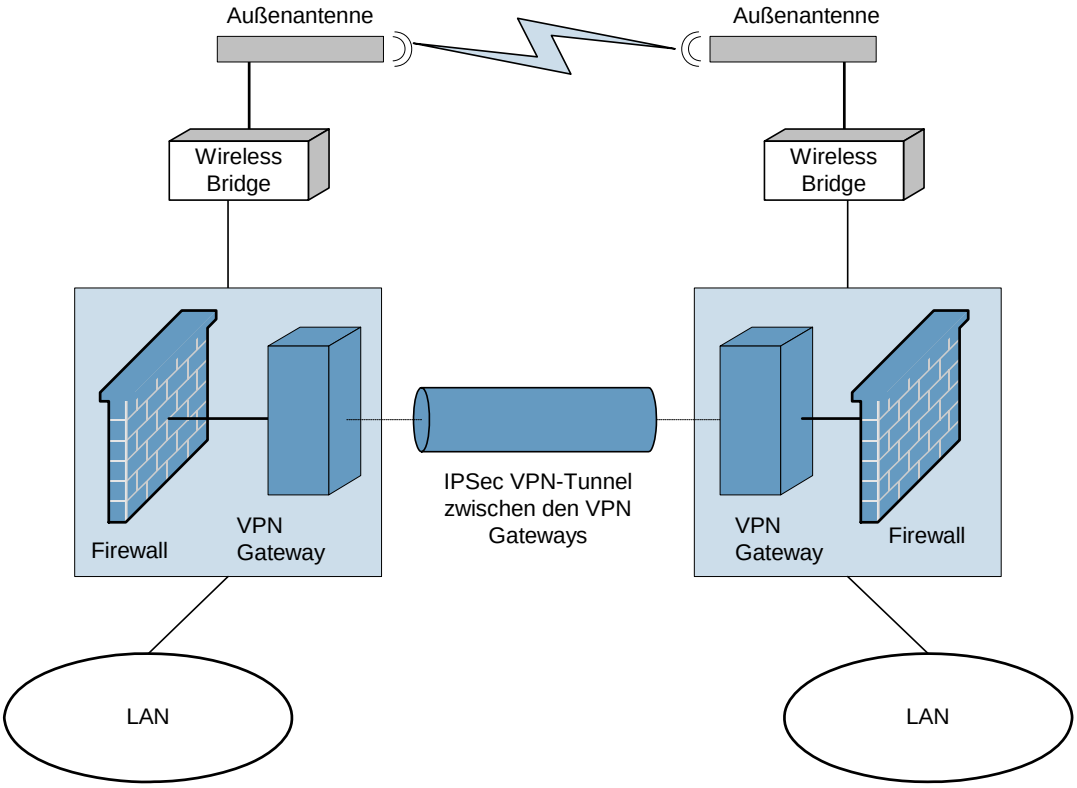



Abbildung 42: Absicherung einer LAN-Kopplung mittels eigenständigen VPN-Gateways

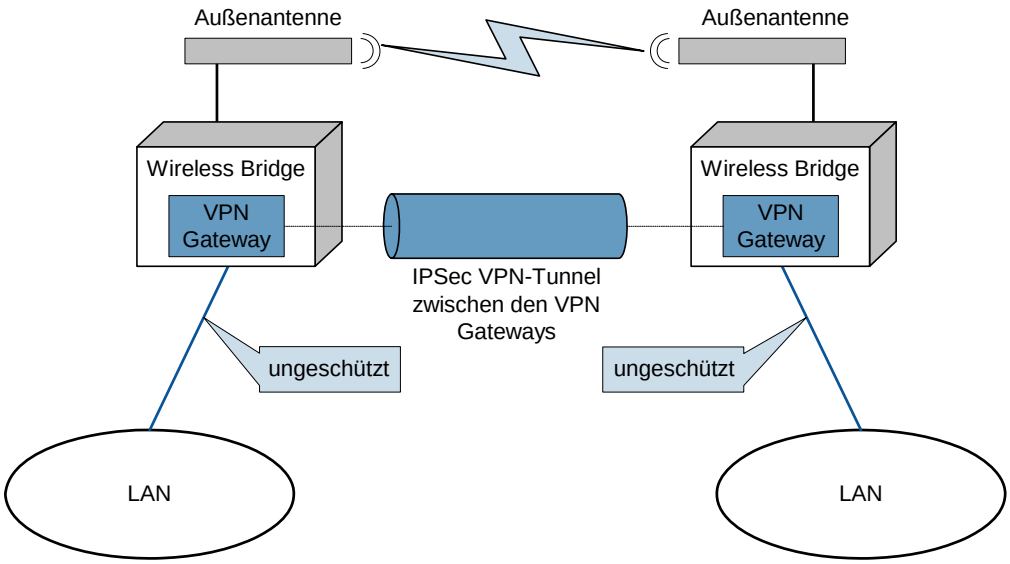



Abbildung 43: Wireless Bridge mit eingebautem VPN-Gateway

## 13.2 Absicherung mittels WPA-Personal bzw. WPA2-Personal

Die Nutzung von Sicherheitssystemen, wie IEEE 802.11i und WPA bzw. WPA2, welche in die Access Points für ein Infrastruktur-WLAN integriert sind, legt den Gedanken nahe, diese Funktionen auch in einer Wireless Bridge zu nutzen. Statt eines VPN-Gateways würde die Verschlüsselung nach WPA bzw. WPA2 genutzt, wie in Abbildung 44 für die Verwendung von PSK gezeigt. Auch hier gilt:

> Der Betreiber hat dafür Sorge zu tragen, dass die LAN-Schnittstelle der Access Points gegen unbefugten Zugriff geschützt ist.

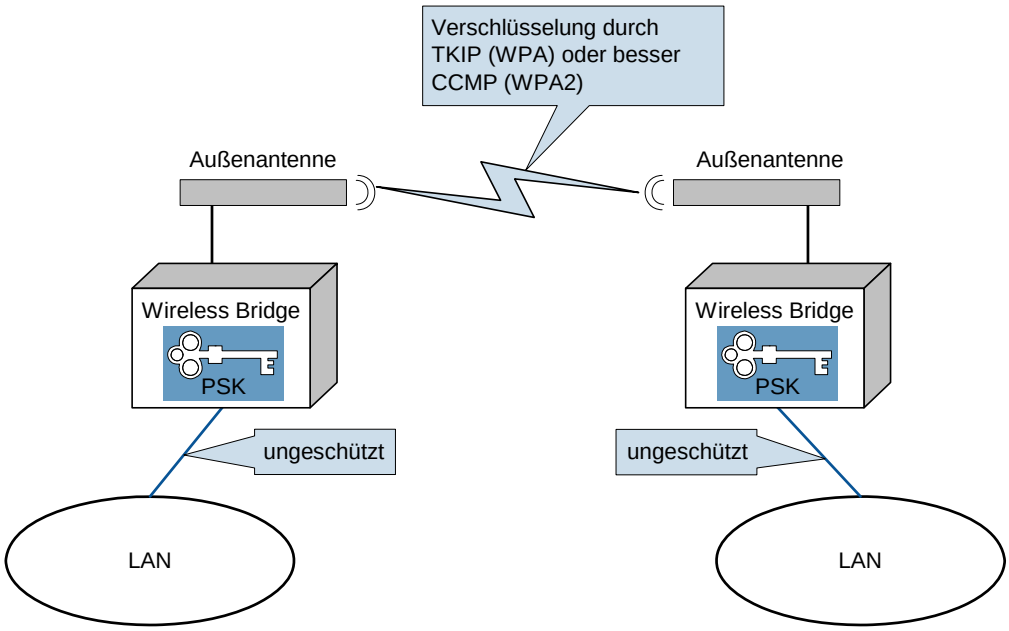



Abbildung 44: Absicherung der LAN-Kopplung mittels WPA-Personal bzw. WPA2-Personal

Die Verschlüsselung erfolgt mit Hilfe der Verfahren TKIP oder CCMP, wie in Kapitel 6.1.1 beschrieben. Im einfachsten Fall werden statische Schlüssel (Pre-Shared Keys, PSKs) verwendet, die in beiden Access Points einzutragen sind. Das Verfahren ist in Kapitel 6.1.3 beschrieben und wird von Wireless Bridges unterstützt, die gemäß WPA-Personal oder WPA2-Personal zertifiziert sind.

Die Verwaltung von PSKs gestaltet sich bei paarweisen Wireless Bridges in LAN-Kopplungen besonders einfach. Es ist jedoch zu bedenken, dass PSKs bei WPA-Personal bzw. WPA2-Personal der Angreifbarkeit durch Wörterbuch-Attacken unterliegen. Es ist also in jedem Fall auf entsprechend sichere Wahl der Schlüssel zu achten (vgl. Kapitel 6.1.2). Die im Allgemeinen statische Konfiguration von LAN-Kopplungen birgt darüber hinaus prinzipiell die Gefahr, Schlüssel auch mit Hilfe von Brute-Force-Attacken zu ermitteln. Dem Angreifer steht dafür eine lange Zeit zur Verfügung, während der er „offline“, also unbemerkt, hohe Rechenleistungen für einen derartigen Angriff einsetzen kann.

## 13.3 Absicherung mittels WPA-Enterprise bzw. WPA2-Enterprise

Der Nachteil statischen Schlüsselmaterials lässt sich unter Rückgriff auf eine Authentifizierung mittels IEEE 802.1X vermeiden. Mit diesem Verfahren lassen sich regelmäßig neue Schlüssel zwischen den beteiligten Komponenten austauschen. Eine Basis dafür stellen Benutzername-Passwort-Kombinationen (z. B. bei EAP-PEAP mit MS-CHAPv2, siehe Kapitel 7.2.5) oder X.509-Zertifikate dar (z. B. EAP-TLS, siehe Kapitel 7.2.3).

Jedoch gilt auch hier:

Der Betreiber hat dafür Sorge zu tragen, dass die LAN-Schnittstelle der Access Points gegen unbefugten Zugriff geschützt ist.

Voraussetzung für eine regelmäßige Erneuerung eines Schlüssels (d. h. eines PMK) ist eine periodische Reauthentication. Dies muss auf den Wireless Bridges entsprechend konfiguriert werden.

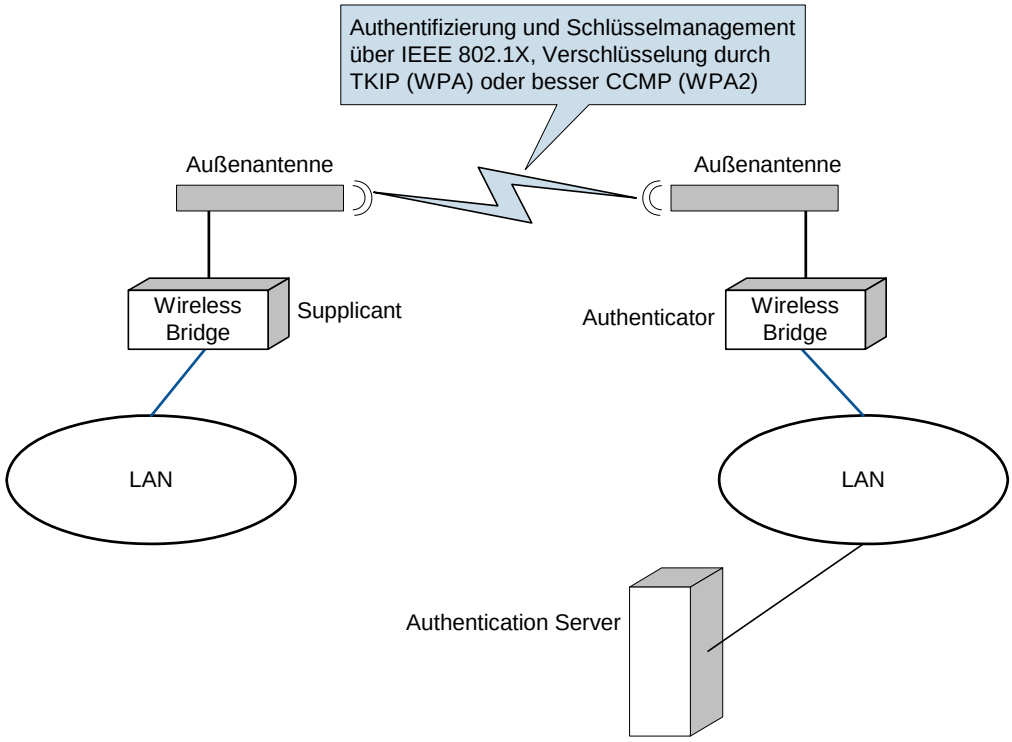



Abbildung 45: Absicherung der LAN-Kopplung mittels WPA-Enterprise bzw. WPA2-Enterprise

Der Aufbau der LAN-Kopplung kann unter Verwendung der Elemente aus Abbildung 23, wie in Abbildung 45 gezeigt, durchgeführt werden. Voraussetzung ist, dass die Wireless Bridge einen Supplicant enthält, eine Rolle, die sonst der mobile Client übernimmt.

Der gezeigte Aufbau ist prinzipiell nicht unangreifbar: Zum einen besteht unter der Voraussetzung, dass WPA mit TKIP eingesetzt wird, die Gefahr eines Angriffs vom Typ Denial of Service (DoS). Wie in Kapitel 6.1.1 bereits erwähnt wurde, werden alle Übertragungsversuche einer MAC-Adresse – hier der gegenüberliegenden Wireless Bridge – für eine Minute abgewiesen, nachdem der Message Integrity Check (MIC) eine Verletzung der Integrität festgestellt hat. Ein Angreifer könnte gezielt Datenpakete mit ungültigem MIC aussenden und so den Datenverkehr dauerhaft unterbrechen.

Daraus ergibt sich das Fazit, das auch für die Variante mit WPA-Personal bzw. WPA2-Personal, wie in Kapitel 13.2 beschrieben, gilt:

Die Absicherung einer LAN-Kopplung sollte nicht über WPA mit TKIP erfolgen. Stattdessen wird empfohlen CCMP, entsprechend WPA2, einzusetzen.

Zum anderen besitzt der Authenticator gemäß IEEE 802.1X die Rolle, den Zugriff zu einem dahinter liegenden Netz zu steuern (vgl. Abbildung 23). Der Supplicant möchte auf Dienste zugreifen, die über den Authenticator zu erreichen sind. Der Supplicant besitzt seinerseits keine Funktion, die den Zugriff auf Dienste eines hinter dem Supplicant angeordneten Netzes steuern kann. Diesem Misstand begegnet die IEEE in ihrer Ausgabe 2004 des Standards IEEE 802.1X (siehe [IEEE04b]). Sie ermöglicht die

Kombination von Supplicant und Authenticator auf dem selben System. Jedes System kann sich zur Nutzung bestimmter Dienste auf anderen Systemen mittels EAP authentifizieren, kann aber gleichzeitig auch anderen Supplicants seine Dienste anbieten, nachdem diese sich authentifiziert haben.

Die vollständige Absicherung einer LAN-Kopplung mittels WPA2-Enterprise besitzt dem entsprechend einen Authentication-Server in jedem der beiden angeschlossenen Lokalen Netze. Jede Wireless Bridge ist sowohl Supplicant als auch Authenticator. Jeder Supplicant besitzt entweder Benutzername-Passwort-Kombinationen oder X.509 Zertifikate zur Authentifizierung am gegenüberliegenden Authentication Server (Abbildung 46). Jede Wireless Bridge wird sich an seinem Gegenüber mittels EAPOL authentifizieren. Es findet jeweils eine Kommunikation gemäß Abbildung 24 statt. Zusammenfassend lässt sich sagen:

Eine vollständige Absicherung mittels WPA2-Enterprise gelingt nur unter gegenseitiger Authentifizierung der Wireless Bridges über je eine EAPOL-Kommunikation. Es sollte eine periodische Reauthentication stattfinden.

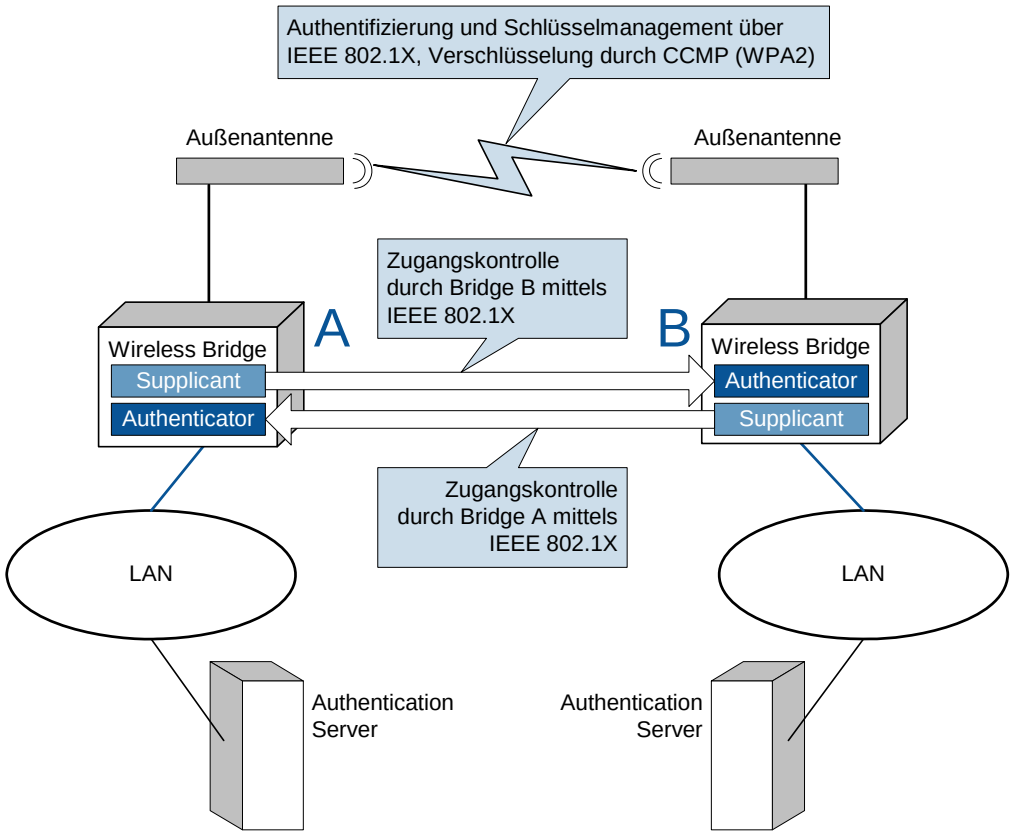



Abbildung 46: Symmetrische Absicherung der LAN-Kopplung mittels WPA2-Enterprise unter Nutzung der Neuauflage des Standards IEEE 802.1X von 2004

# 14 Zusammenfassung

Das Medium Funk, über das in WLAN kommuniziert wird, ist stets ein Shared Medium. Eine Nachricht wird also prinzipiell von allen Stationen innerhalb eines gewissen Gebiets empfangen. Die geografischen Grenzen dieses Gebiets sind zwar beschränkt, jedoch durch die Eigenschaften der Ausbreitung von Funkwellen nicht exakt beschreibbar. Eine Datenübertragung über Funk muss daher stets geeignet durch eine entsprechende Kombination von Mechanismen zur Authentifizierung, Verschlüsselung und Integritätsprüfung abgesichert werden.

Der in IEEE 802.11 ursprünglich festgelegte Mechanismus WEP ist hierzu nur mangelhaft geeignet. In dieser Situation ist es naheliegend, den Zugang zur Infrastruktur über ein WLAN mit einem VPN abzusichern. Tatsächlich ist dies in der Vergangenheit der einzige Weg gewesen, ein WLAN angemessen abzusichern. Meist wird hier IPSec (typischerweise verbunden mit Gerätezertifikaten auf Client-Seite) verwendet. SSL-VPN sind ebenfalls im WLAN-Bereich einsetzbar und insbesondere dadurch attraktiv, dass nur geringe Anforderungen an die Fähigkeiten des Clients bzw. des Client-Betriebssystems gestellt werden. Im Prinzip ist lediglich ein Web-Browser mit HTTPS-Unterstützung erforderlich. VPN basieren allgemein auf einer zentralistischen Architektur. Dabei fließt der Gesamtverkehr des WLAN durch ein (bzw. einige wenige) VPN-Gateways, die daher entsprechend performant und verfügbar dimensioniert sein müssen. Kritisch wird dies insbesondere bei großen WLAN-Installationen und beim Einsatz von Übertragungstechniken mit höheren Datenraten, wie IEEE 802.11g und IEEE 802.11a.

In manchen Fällen müssen im WLAN jedoch Geräte unterstützt werden, für die kein VPN-Client erhältlich ist. Dies sind typischerweise einfache Geräte z. B. im Produktions- und Logistikumfeld, wie beispielsweise Barcode Scanner. Trotz der Schwächen muss dann doch noch auf WEP zurückgegriffen werden. Zur Verringerung der Angriffsfläche werden dabei oft Firewall-Techniken inklusive einer Zugangskontrolle auf MAC Layer eingesetzt. Damit das WLAN für einen Angreifer nicht unmittelbar sichtbar ist, kann als schwache Sicherheitsmaßnahme die Übertragung des SSID im Beacon Frame unterbunden werden, und die Option der Assoziation am Access Point mit der Broadcast SSID wird deaktiviert.

Mit IEEE 802.11i bzw. WPA stehen inzwischen Bausteine zur Verfügung, die auf der Luftschnittstelle eine adäquate Absicherung eines WLAN gestatten. Es sind grundsätzlich dabei zwei Alternativen möglich: Verwendung von Pre-Shared Keys oder Authentifizierung und Schlüsselmanagement über IEEE 802.1X. Für größere WLAN und generell für WLAN mit höheren Sicherheitsanforderungen ist der Einsatz von IEEE 802.1X in Kombination mit einer angemessen hochwertigen EAP-Methode zur Authentifizierung dringend zu empfehlen. Zur Verschlüsselung werden in IEEE 802.11i eine abwärtskompatible auf WEP basierende Methode (TKIP) und eine Methode, die neue Hardware erfordert und AES einsetzt, spezifiziert. WPA ist eine aufwärtskompatible Auswahl der Spezifikationen in IEEE 802.11i, die von der Wi-Fi Alliance spezifiziert ist. Auf der Basis von WPA werden von der Wi-Fi Alliance WLAN-Produkte zertifiziert. WPA2 ist eine Erweiterung um die in IEEE 802.11i festgelegte Verwendungsmethode von AES. IEEE 802.11i bzw. WPA und WPA2 beseitigen die bisher bekannten Schwächen von WEP. Allerdings werden längst noch nicht alle verfügbaren Client-Systeme unterstützt. Selbst im Jahr 2005 sind noch diverse Geräte auf dem Markt verfügbar, die IEEE 802.11i bzw. WPA noch nicht anbieten. Zu nennen sind hier insbesondere auch VoIP Handsets. Für eine Migration zu IEEE 802.11i bzw. WPA sind Konzepte für die (befristete) Koexistenz speziell mit WEP notwendig.

Tabelle 4 zeigt die verschiedenen Sicherheitsmechanismen im Vergleich.

Das Netzmanagement für die IT-Infrastruktur muss generell WLAN-spezifische Eigenheiten berücksichtigen. Dabei hat die Überwachung der Luftschnittstelle eines WLAN eine besondere Bedeutung, da eine Funkübertragung vergleichsweise empfindlich gegenüber Störungen ist und eine große Angriffsfläche bietet. Dies beinhaltet speziell auch die Erkennung von Fremdstationen (Access Points und Endgeräte) und deren geografische Lokalisierung im WLAN über ein Wireless IDS. Aus einer Sicherheitsperspektive ist weiterhin zu beachten, dass die Möglichkeit des administrativen Zugangs zu

Access Points und nachgelagerten Netzelementen über die Luftschnittstelle erhebliche Risiken mit sich bringt und daher besonders abzusichern bzw. einzuschränken ist.

Die Sicherheitsanforderungen für den öffentlichen Zugang zum Internet über WLAN-Hotspots unterscheiden sich von denen privater WLAN-Installationen. Zunächst stehen für den Betreiber eines Hotspots die Möglichkeiten für eine sichere (verlässliche und nicht kompromittierbare) Abrechnung und die Sicherung der Teilnehmerdaten im Vordergrund.

Aus der Perspektive des Clients ist dessen Angreifbarkeit in einem Hotspot besonders zu berücksichtigen, da die WLAN-Übertragung auf Layer 2 meist unverschlüsselt geschieht, um den Nutzern einen möglichst einfachen Zugang zu gewähren. Die hier zu empfehlenden Maßnahmen beinhalten unter anderem zumindest den Einsatz einer Personal Firewall, eines aktuellen Virenschutzes, die Härtung des Client-Systems durch Deaktivierung nicht benötigter Dienste, die geeignete Parametrierung von Systemdiensten und Anwendungen sowie Installation der jeweils aktuellen Sicherheits-Patches für das Betriebssystem. Die Ähnlichkeit dieser Maßnahmen zu denen, die für mobile Clients für den Internet-Zugang gelten, ist offensichtlich. Grundsätzlich gilt dies auch in privaten WLAN, und insbesondere dort, wo noch WEP eingesetzt wird. Nicht selten ist die WLAN-Infrastruktur besser als der Client geschützt. Für die Auswahl der Maßnahmen und Konfiguration der Komponenten sind gewisse Systemkenntnisse notwendig; die oft anzutreffende Plug&Play-Vorgehensweise vieler Nutzer führt unwillkürlich zu Sicherheitslücken.

Dieses Dokument dient als Grundlage für die Entwicklung von Sicherheitskonzepten für WLAN und illustriert insbesondere Bandbreite und Komplexität von WLAN und der zugehörigen Sicherheitstechnik.

| Mechanismus | Produktverfügbarkeit | Unterstützung unterschiedlicher Client-Systeme | Kosten | Aufwand von Planung und Implementierung | Aufwand im Betrieb | Beitrag zum Schutz des WLAN |
|---|---|---|---|---|---|---|
| WEP | ++ | ++ | niedrig | niedrig | niedrig | niedrig |
| IEEE 802.11i mit TKIP und PSK bzw. WPA mit PSK | + | 0 | niedrig | niedrig | niedrig | mittel |
| IEEE 802.11i mit TKIP und IEEE 802.1X bzw. WPA mit IEEE 802.1X | + | 0 | mittel | mittel bis hoch | mittel | hoch (*) |
| IEEE 802.11i mit CCMP und PSK bzw. WPA2 mit PSK | 0 | - | niedrig | niedrig | niedrig | mittel |
| IEEE 802.11i mit CCMP und IEEE 802.1X bzw. WPA2 mit IEEE 802.1X | 0 | - | mittel | mittel bis hoch | mittel | hoch (*) |
| ACL auf MAC Layer | + | ++ | mittel | mittel | hoch | niedrig |
| Firewall | ++ | ++ | hoch | mittel | mittel | niedrig |
| WLAN IDS | 0 | ++ | mittel bis hoch | mittel bis hoch | mittel bis hoch | mittel |
| VPN | ++ | 0 | hoch | mittel bis hoch | mittel | hoch |

"++" = sehr gut, "+" = gut, "0" = akzeptabel, "-" = mangelhaft, "--" = ungenügend

(*) Die Einstufung "hoch" gilt nur unter der Voraussetzung der Verwendung einer angemessenen Authentifizierungsmethode

Tabelle 4: Sicherheitsmechanismen im Vergleich

# 15 Anhang

Im Anhang werden solche Themen vertieft, die zwar nicht Bestandteil der WLAN-Technik sind, aber im Rahmen der Absicherung eines WLAN eine Rolle spielen. Zunächst werden in Kapitel 15.1 einige Grundlagen der Sicherheitstechnik kurz vorgestellt. Dieses Dokument ersetzt nicht die einschlägige Fachliteratur. Kapitel 15.2 beschreibt die für VPN und IEEE 802.1X bzw. EAP wesentlichen Aspekte der Authentifizierung. Kapitel 15.3 stellt anschließend die Elemente und Mechanismen eines IP-VPN vor, und Kapitel 15.4 ergänzt diese Betrachtungen um SSL-VPN. In diesem Zusammenhang betrachtet Kapitel 15.5 Smartcards und Sicherheitstoken. Die Basis für eine Authentifizierung des (WLAN-) Clients über Zertifikate, wie sie z. B. bei IPSec und bei IEEE 802.1X eingesetzt werden kann, ist eine PKI, deren Aufbau in Kapitel 15.6 vorgestellt wird. Abschließend beschreibt Kapitel 15.7 das Protokoll RADIUS, welches ein Schlüsselelement unter anderem für IEEE 802.1X ist.

## 15.1 Grundlagen der Absicherung von Netzwerken

### 15.1.1 Verschlüsselung

Die Verschlüsselung von im Netzwerk übertragenen Daten schützt diese vor allem gegen den Verlust der Vertraulichkeit. Manche Verschlüsselungsmethoden bieten gleichzeitig aber auch Schutz gegen Manipulationen, d. h. den Verlust der Integrität der Daten.

Es existieren diverse Verschlüsselungsverfahren, die sich insgesamt in zwei Klassen einteilen lassen:

- Symmetrische Verfahren

  Diese arbeiten hochgradig effizient, da sie auf simplen Bit-Operationen beruhen, die insbesondere in Hardware sehr schnell ausgeführt werden können. Sie verwenden allerdings einen symmetrischen, d. h. auf beiden Seiten der Kommunikationsbeziehung identischen, Schlüssel, der zuvor auf einem sicheren Kanal ausgetauscht werden muss.

  Marktgängige Vertreter dieser Gattung sind z. B. DES, 3-DES, RC4, AES, IDEA.

- Asymmetrische Verfahren

  Diese benötigen keinen vertraulichen Schlüsselaustausch, da der zum Verschlüsseln notwendige (öffentliche) Schlüssel nicht geheim ist. Somit kann im Prinzip jedermann eine Nachricht für einen bestimmten Empfänger verschlüsseln. Der Sender muss sich lediglich aus einer zuverlässigen Quelle den korrekten öffentlichen Schlüssel besorgen. Der Schlüssel zum Dechiffrieren ist geheim (privater Schlüssel). Der private Schlüssel muss allerdings auch nicht ausgetauscht werden. Der große Nachteil dieser Verfahren ist ihre mangelnde Effizienz. Je nach Messmethode und Testumgebung kann ein asymmetrisches Verfahren bei gleicher Verschlüsselungsstärke um Größenordnungen (z. B. 1000mal) langsamer sein als ein symmetrisches Verfahren.

  Marktgängige Vertreter dieser Gattung sind RSA und ElGamal.

Aktuelle Verschlüsselungsprodukte kombinieren die beiden Prinzipien: Sie nutzen zum Austausch der Schlüsselinformationen, die nur ein geringes Datenvolumen aufweisen, ein asymmetrisches Verfahren und verschlüsseln die eigentlichen Nutzdaten mit einem symmetrischen Verfahren unter Verwendung des zuvor ausgetauschten symmetrischen Schlüssels.

Alternativ zu einem asymmetrischen Verschlüsselungsverfahren kann auch ein spezielles Schlüsselaustauschverfahren zum Einsatz kommen; in der Regel wird hier das Verfahren von Diffie und Hellman (DH) eingesetzt.

Neben der Eigenschaft, ein „starker“, d. h. mit analytischen Methoden nicht in vertretbarer Zeit zu brechender Algorithmus zu sein, wird die Stärke eines Verschlüsselungssystems maßgeblich durch die Länge der verwendeten Schlüssel bestimmt: Ist der Schlüssel kurz, d. h. die Menge der theoretisch

verwendbaren Schlüssel klein, so kann man einfach alle Schlüssel ausprobieren, bis man den richtigen gefunden hat. Aktuell geht man davon aus, dass mittelfristig symmetrische Schlüssellängen ab 100 Bit ausreichen; Schlüssel, die kürzer sind als ca. 75 Bit, bieten bereits heute keinen nennenswerten Schutz mehr gegen ernsthafte Angriffe. Bei den Verfahren RSA, ElGamal und DH liegen akzeptable Schlüssellängen bei 1024 Bit oder mehr[37].

### 15.1.2 Authentifizierung

Authentifizierung bezeichnet die Verifikation der Identität des Kommunikationspartners. Dies geschieht in der Regel über Kennwörter, die zwischen den Beteiligten ausgehandelt und im Bedarfsfall überprüft werden.

Während dies beim Aufbau von Site-to-Site-VPN-Tunneln durchaus ausreicht, sofern diese Kennwörter gut gewählt wurden, stellt dieser Ansatz bei der Authentifizierung von Personen ein Risiko dar: Passwörter werden oft schlecht gewählt, d. h. sie sind leicht zu erraten, und/oder werden vom Anwender leichtfertig publik gemacht (etwa durch Notieren, Mitlesenlassen bei der Eingabe oder bewusste Weitergabe). Daher sollte im Falle eines hohen Sicherheitsbedarfs ein sogenannter „starker" Mechanismus zum Einsatz kommen.

Starke Authentifizierungsverfahren kombinieren eine Kennwortabfrage mit dem Besitz eines bestimmten Gegenstands, eines sogenannten (Security) Tokens, das ein nur für einen einmaligen Authentifizierungsvorgang gültiges Passwort (One Time Password) erzeugt. Nur eine Person, die sowohl das Token als auch das zugehörige Kennwort (meist eine mehrstellige Personal Identification Number; kurz: PIN) besitzt, kann sich erfolgreich authentifizieren[38]. Solche Token sind meist als transportable Hardware (Schlüsselanhänger, Scheckkarte, ...) realisiert. Alternativ können Smartcards eingesetzt werden. Sie verkörpern das gleiche Prinzip. Ihre Vorteile liegen in der Möglichkeit der Abwicklung von kryptografischen Operationen auf der Smartcard und damit verbunden in einer höheren Sicherheit durch besseren Schutz der Schlüssel. Allerdings haben Smartcards den Nachteil, eine passende Schnittstelle zum Client zu benötigen, über welche die notwendigen Informationen zur Authentifizierung übertragen werden können. Auf die Besonderheiten von Smartcards und Sicherheitstoken wird in Kapitel 15.5 genauer eingegangen.

### 15.1.3 Integritätsprüfung

Die Integrität übertragener Daten wird durch fälschungssichere Prüfsummen sichergestellt. Hier können verschiedene Verfahren zum Einsatz kommen. Die bekanntesten Ansätze sind derzeit die Verwendung digitaler Signaturen, die meist auf der Anwendungsebene eingesetzt wird, sowie die Verwendung von Einweg-Hashfunktionen.

Digitale Signaturen basieren auf dem umgekehrten Prinzip asymmetrischer Verschlüsselungsverfahren: Nur der Besitzer des privaten Schlüssels kann ein Dokument signieren, aber jeder, der den öffentlichen Schlüssel kennt, kann die Unterschrift verifizieren.

Einweg-Hashfunktionen werden in Verbindung mit einer symmetrischen Schlüsselinformation eingesetzt: Daten und Schlüssel werden gemeinsam der Hashfunktion unterworfen und der Hashwert zusammen mit den Daten übertragen; zur Prüfung der Integrität der Daten wird diese Operation vom Empfänger wiederholt und der ermittelte Hashwert mit dem übertragenen verglichen.

Beispiele sind RSA (für digitale Signaturen) bzw. HMAC (Hashed Message Authentication Code); letzteres wird u. a. bei IPSec und TLS verwendet.

---

37 Es gibt inzwischen Verfahren, die auf elliptischen Kurven (Elliptic Curves, kurz: EC) basieren und mit einer deutlich geringeren Schlüssellänge auskommen.

38 Erwähnenswert ist in diesem Zusammenhang auch die Verwendung biometrischer Methoden, insbesondere die Erkennung des Fingerabdrucks, die als Alternative zur PIN-Eingabe beispielsweise für verschiedene Smartcard-Systeme verfügbar ist.

## 15.2 Authentifizierungsprotokolle

### 15.2.1 PAP

Das Protokoll PAP (Password Authentication Protocol, RFC 1334, siehe [PAP92]) wurde ursprünglich für die Verwendung innerhalb von PPP entworfen; es ist jedoch nicht als EAP-Methode implementiert worden, d. h. es gibt sozusagen kein „EAP-PAP“. PAP überträgt Benutzernamen und Kennwort im Klartext über das Netzwerk, sollte daher also niemals in unsicheren Netzen eingesetzt werden. Da aber PAP als mögliches Verfahren innerhalb von TTLS Anwendung finden darf, kann es unter Umständen dennoch auch für die Verwendung z. B. in WLANs interessant sein. PAP kann für Netzwerk-Logon-Systeme verwendet werden, bei denen die Überprüfung des Kennwortes durch die Methode zum Zugriff auf die Benutzerdatenbank (z. B. LDAP) bedingt, dass dem Authentication Server (i.A. der RADIUS-Server) das Kennwort im Klartext vorliegt.

### 15.2.2 CHAP

Ebenso wie PAP oder auch das EAP-Gerüst selbst, wurde CHAP (Challenge Handshake Authentication Protocol, RFC 1994, siehe [CHAP96]) für die PPP-Authentifizierung vorgesehen. Wie bei EAP-MD5 wird dem Client eine Challenge übermittelt, die der Client verwendet, um zu beweisen, dass er das Kennwort kennt.

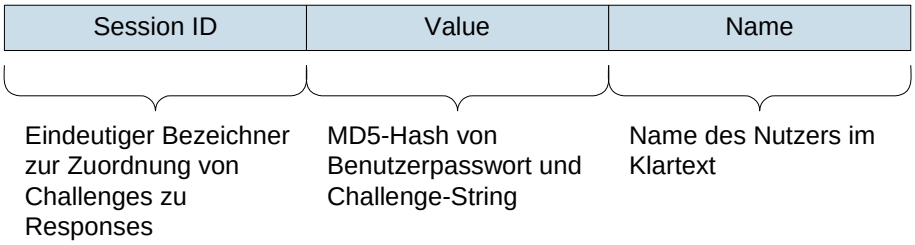



Abbildung 47: Inhalt einer CHAP-Response (vereinfacht)

CHAP und damit auch EAP-MD5 setzen voraus, dass das Kennwort dem AS (oder ggf. dem System, das die Benutzerdatenbank beherbergt) unverschlüsselt oder umkehrbar verschlüsselt vorliegt. Für eine WLAN-Authentifizierung ist dieses Verfahren kaum relevant, da eine Verwendung nur innerhalb von sicheren Tunneln in Frage kommt (EAP-FAST oder EAP-TTLS), dann jedoch meist PAP oder MS-CHAP-Varianten sinnvoller sind. Einige Hersteller unterstützen innerhalb von TTLS trotzdem dieses Verfahren.

### 15.2.3 MS-CHAPv1

MS-CHAP (in der Version 1) wurde von Microsoft geschaffen, um ähnliche Funktion wie CHAP bereitzustellen. Hierbei wird jedoch nicht das Kennwort direkt überprüft, sondern dessen „One-Way Hash“ wird als Schlüssel für eine symmetrische Verschlüsselung des Challenge-Strings verwendet (Abbildung 48). Dieser Hash wird auch in den Benutzerverwaltungen von Microsoft gespeichert (und eben im Normalfall nicht das Kennwort selbst). Daher passt das Verfahren gut zu Microsoft-Umgebungen.

Des Weiteren kann ein entsprechender RADIUS-Server über herstellerspezifische Methoden gegenüber einer MS-Benutzerdatenbank die Prüfung vornehmen lassen, ob die gesendete Response zu der

verschickten Challenge passt. Damit kann das Verfahren leicht ohne eine Anpassung der Benutzerdatenbank implementiert werden.

MS-CHAP unterstützt im Gegensatz zu CHAP oder EAP-MD5 das Ändern des Kennwortes während der PPP-Authentifizierung – ein wichtiges Merkmal, denn einfach gesagt gilt: Ein Kennwort, das nicht geändert wird, ist ein schlechtes. Allerdings kann über MS-CHAP nur der Benutzer bzw. der Client authentifiziert werden, nicht der Server. Auch sind weitere Schwächen des Verfahrens bekannt, die eine Verwendung in wenig vertrauenswürdigen Netzwerken nicht empfehlenswert erscheinen lassen. Für eine Verwendung innerhalb von Wireless LANs kommt üblicherweise das Verfahren auch nicht direkt, sondern allenfalls getunnelt zum Einsatz. Ohne Tunnel ist es von Microsoft nicht für 802.1X vorgesehen und auf Windows-Clients auch nicht als Verfahren innerhalb eines Tunnels hierfür auswählbar. Von Drittherstellern werden jedoch Supplicants nebst Servern angeboten, welche MS-CHAP in EAP-TTLS getunnelt verwenden können. Der Nachfolger MS-CHAPv2 bzw. dessen Implementierung als EAP-Methode (siehe Kapitel 7.2.8), kann unmittelbar von Windows jedoch sehr wohl – getunnelt in EAP-PEAP – für die IEEE 802.1X-Authentifizierung verwendet werden.

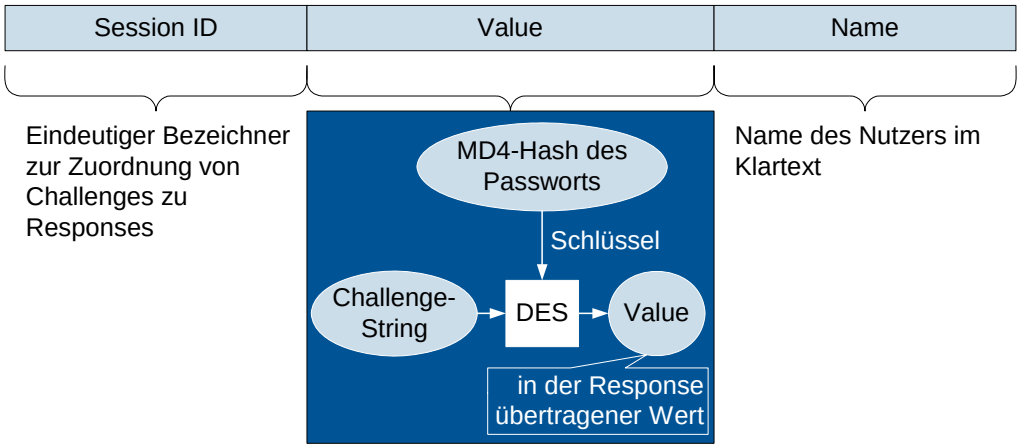



Abbildung 48: Inhalt einer MS-CHAPv1-Response, vereinfacht

### 15.2.4 MS-CHAPv2

Um einige Schwächen von MS-CHAPv1 zu beseitigen, entwickelte Microsoft MS-CHAPv2 (RFC 2759, siehe [MSCH00]) als PPP-Verfahren, bei dem unter anderem auch eine gegenseitige Authentifizierung von Client und Server erfolgt. Es konnten jedoch erneut Schwächen des Verfahrens aufgedeckt und veröffentlicht werden, die zwar weniger gravierend sind, als jene von MS-CHAPv1, trotzdem ist die Technik alleine für unsichere Netze aus heutiger Sicht nicht uneingeschränkt zu empfehlen.

Was die Integrierbarkeit in Microsoft-Umgebungen angeht, gilt das schon unter Kapitel 15.2.3 gesagte. Insbesondere für die Verwendung innerhalb von verschlüsselten Tunneln spielt aber MS-CHAPv2 und vor allem die EAP-Implementierung EAP-MSCHAPv2 eine wichtige Rolle, da EAP-PEAP und EAP-MSCHAPv2 in MS Windows XP integriert sind.

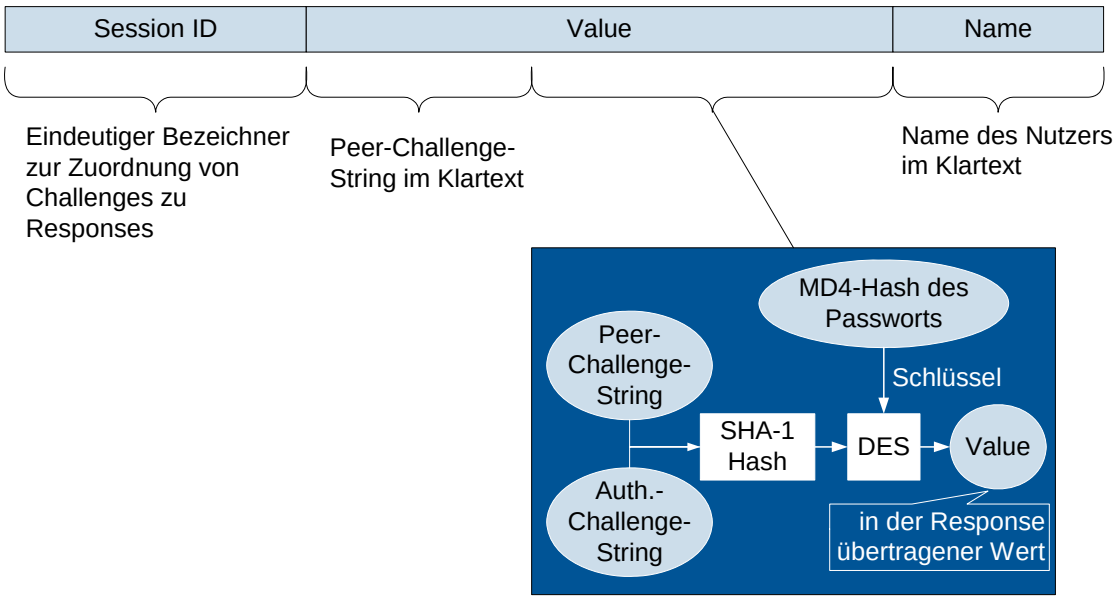



Abbildung 49: Inhalt einer MS-CHAPv2-Response, vereinfacht

## 15.3 IP-VPN

### 15.3.1 Begriffsklärung

Der Begriff des VPN (Virtual Private Network) beinhaltet zwei wesentliche Komponenten, die das Wesen eines solchen VPN charakterisieren: VPNs sind privat und virtuell.

„Privat“ bedeutet in diesem Zusammenhang, dass ein solches Netz gegen andere Netze durch geeignete technische Maßnahmen abgeschottet ist. Somit können Kommunikationsverbindungen auf der Basis solcher Techniken in der gleichen Weise genutzt werden wie eigene, exklusiv genutzte physikalische Leitungen – bei solchen exklusiven Leitungen kann es sich sowohl um Fest- als auch um Wählverbindungen handeln. In derartigen Netzen kann eine völlig unabhängige Administration des Netzes erfolgen; so kann z. B. die Netzadresse selbst gewählt und deren Struktur ohne weitere Rücksprache mit den Betreibern anderer Netze festgelegt werden.

Gleichzeitig ist dieses private Netz jedoch nur „virtuell“ vorhanden, da die zugrunde liegende physikalische Netzinfrastruktur in Wirklichkeit nicht exklusiv, sondern von mehreren solchen Netzen gemeinsam genutzt wird.

IP-basierte VPN (kurz: IP-VPN) setzen das Vorhandensein einer zugrunde liegenden Netzinfrastruktur auf Basis des Internet Protocol (IP) voraus. Diese reale Netzinfrastruktur dient als Trägernetz für alle darauf abgebildeten virtuellen Netze. Die bereits erwähnte Abschottung verschiedener solcher VPNs gegeneinander erfolgt dabei durch Verwendung von Tunnel-Verfahren.

Wesentliche Vorteile von VPNs sind Synergien bei der Nutzung des Trägernetzes und insbesondere die Möglichkeit, durch Verwendung entsprechend ausgestalteter Tunnelverfahren ansonsten im Trägernetz nicht vorhandene Sicherheitsmechanismen bereitzustellen.

### 15.3.2 Tunnel-Prinzip

Der Begriff des Tunneling wird im Folgenden auf der Basis folgender Definition verwendet:

Tunneling beschreibt eine Methode, Daten eines Netzprotokolls A über ein anderes Netzprotokoll B zu transportieren. Dabei bildet das Datenpaket des Protokolls A die Nutzlast (Payload) des Proto-

kolls B, d. h. der Datenteil des Protokolls B enthält das Paket des Protokolls A. Aus Sicht von an diesem Vorgang unbeteiligten Komponenten, die auf Basis des Netzprotokolls B arbeiten, ist der Tunnelanfang der Absender und das Tunnelende der Empfänger dieses Pakets.

Das Grundprinzip ist in Abbildung 50 illustriert. Das Datenpaket des Protokolls A (Payload) wird innerhalb des Tunnels in ein Paket des Protokolls B „eingepackt“ (gekapselt).

Der Ablauf ist dabei der folgende:

Die Netzsysteme TA (Tunnelanfang) und TE (Tunnelende) unterstützen sowohl Protokoll A als auch Protokoll B. TA ist so konfiguriert, dass Datenpakete des Protokolls A für bestimmte Ziele durch einen Protokoll-B-Tunnel zu TE transportiert werden. Empfängt TA ein zu tunnelndes Paket, so erzeugt es ein Paket des Protokolls B mit TA als Absender, TE als Empfänger und dem ursprünglichen Paket als Datenteil (gegebenenfalls ergänzt um weitere Protokoll-Header); dieses Paket wird auf Basis des Protokolls B zu TE transportiert. TE entfernt alle hinzugefügten Header – mindestens den des Protokolls B – und sendet das wiederhergestellte Paket des Protokolls A an das ursprüngliche Ziel.

Dieses Prinzip des Einpackens (engl. encapsulation) wird auch bei der Schichtung von Kommunikationsprotokollen nach dem OSI-Modell angewandt: Hier werden Pakete höherer Protokoll-Schichten (Layer) in Pakete darunter liegender Protokoll-Schichten eingepackt.

Dieser Mechanismus funktioniert auch mehrmals hintereinander, d. h. es sind auch ineinander geschachtelte Tunnel möglich.

Für VPNs in reinen IP-basierten Umgebungen stellt sich das Verfahren also in der Regel wie folgt dar: Die Datenpakete des lokalen Netzprotokolls (IP) werden am Tunnelanfang (z. B. dezentrales VPN-Gateway) in IP-Pakete, die im Trägernetz geroutet werden können, eingepackt. Am Tunnelende (z. B. zentrales VPN-Gateway) werden die Protokoll-Header des Trägernetzes entfernt, und das originale Datenpaket kann jenseits des Tunnels weitergeleitet werden.

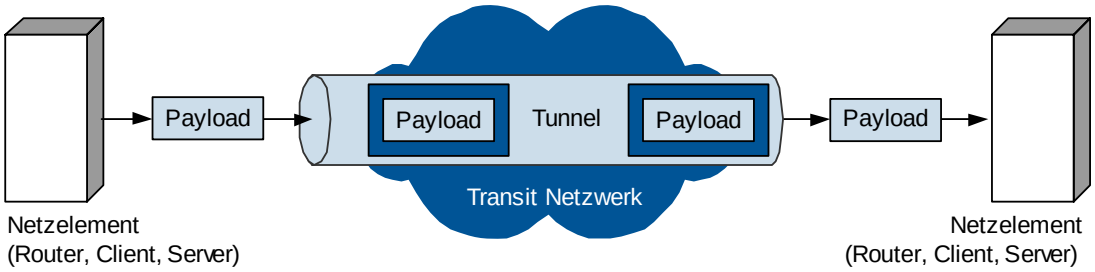



Abbildung 50: Prinzip des Tunneling

### 15.3.3 Tunnel-Protokolle

Grundsätzlich kommen verschiedene Tunnelprotokolle in Frage. Zur Auswahl stehen unter anderem:

- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)
- PPTP (Point to Point Tunneling Protocol)
- IPSec-Tunnel-Modus (Internet Protocol Security, kurz: IPSec)

Alle diese Protokolle sind weit verbreitet bzw. sogar standardisiert, sodass von einer hohen Produkt-Kompatibilität ausgegangen werden kann. Sie unterscheiden sich allerdings insbesondere hinsichtlich der unterstützten Sicherheits-Features. In Umgebungen, in denen starke Verschlüsselung gefordert ist, kommen GRE und L2TP nicht in Frage. PPTP bietet zwar auch einen Schutz der Kommunikation durch Verschlüsselung, allerdings sind in der Vergangenheit immer wieder Schwächen innerhalb der

Implementierungen aufgedeckt worden, so dass auch die Variante mit 128 Bit RC4 nur unter Vorbehalt als sicher einzustufen ist (siehe [SMW99]).

Daher bietet derzeit und auch auf absehbare Zeit IPSec die besten Voraussetzungen für sichere Kommunikation mit höchstem Kompatibilitätsgrad.

Das Verfahren L2TP over IPSec (kurz: L2TP/IPSec), das in RFC 3193 spezifiziert wird, verwendet einen speziellen Ansatz. Hier wird ein L2TP-Tunnel verwendet, der zusätzlich durch IPSec (im Transportmodus) abgesichert wird (siehe [L2TP01] und Kapitel 15.3.7).

### 15.3.4 Authentifizierung

Bei IP-VPNs ist die Authentifizierung während der beim Aufbau der IPSec-Verbindung ablaufenden IKE-Aushandlungen üblich. Hierzu wird die ursprünglich ausschließlich zur Authentifizierung von Computern vorgesehene IKE-Authentifizierung in Client-to-Gateway Szenarien in den meisten Fällen mehr oder weniger zweckentfremdet, um stattdessen Benutzer zu authentifizieren. Grundsätzlich können bei IKE Pre Shared Keys und X.509-Zertifikate verwendet werden. Andere, für die Verwendung bei IKE nicht standardisierte Authentifizierungsmerkmale wie z. B. OTPs unter Nutzung von geeigneten Kombinationen von RADIUS- und OTP-Servern, erfreuen sich jedoch weiterhin großer Beliebtheit. Während manuell konfigurierte Pre-Shared Keys bei VPN-Verbindungen zwischen zwei Gateways durchaus noch ihre Berechtigung haben, stellen sie bei der Client-Anbindung bereits bei einer geringen Anzahl von Clients ein nicht unerhebliches Sicherheitsrisiko dar. Die Situation ist hier durchaus analog zur Auswahlproblematik zwischen PSK und einer Authentifizierung mit IEEE 802.1X in WLAN mit WPA, WPA2 bzw. IEEE 802.11i zu bewerten.

Bei Layer 2-Protokollen wie PPTP und L2TP kommen PPP-Authentifizierungsprotokolle (PAP, MS-CHAP, EAP, …) für die Benutzerauthentifizierung zum Einsatz. Kombinierte Verfahren wie Microsofts L2TP-over-IPSec nutzen für die Computerauthentifizierung bei IPSec/IKE üblicherweise X.509-Zertifikate und beim anschließenden L2TP-Tunnelaufbau Benutzername/Kennwort-Kombinationen mit MS-CHAP v2 oder X.509-Zertifikate mit EAP-TLS.

Nach der erfolgreichen Einwahl kommen je nach Client-Applikation und Art der angefragten Ressource andere Authentifizierungsprotokolle zum Einsatz, beispielsweise NTLM oder Kerberos beim Zugriff auf SMB/CIFS-Shares oder NDAP beim Zugriff auf Novell eDirectory.

### 15.3.5 Funktionsweise von IPSec

IPSec bietet zwei Mechanismen zur Behebung der wesentlichen Sicherheitsprobleme der Ende-zu-Ende-Kommunikation in IP-Netzen:

- Eine Integritätsprüfung für IP-Pakete verhindert die Manipulation oder Fälschung von IP-Paketen durch Unberechtigte.
- Die Verschlüsselung des Paketinhalts verhindert das Ausspähen von Daten.

Die Sicherheitsmechanismen werden durch zwei spezielle Paket-Header realisiert bzw. kontrolliert:

- Der AH (Authentication Header) sichert durch eine kryptografische Prüfsumme die Integrität des Pakets.
- Der ESP (Encapsulating Security Payload) steuert über darin enthaltene Informationen die korrekte Entschlüsselung der kryptografisch geschützten Payload.

Beide Header können entweder einzeln oder auch kombiniert angewandt werden, wobei man zwei Modi unterscheidet: den Tunnelmodus, der nach dem Tunneling-Prinzip arbeitet, und den Transportmodus. Im Transportmodus erfolgt keine Encapsulation, sondern der IPSec-Header wird hinter den IP-Header in das Original-Datagramm eingefügt. Dieser Modus ist für die Absicherung von Peer-to-Peer-Kommunikationsverbindungen konzipiert und eignet sich wegen der Notwendigkeit, trägernetzkonforme Adressen zu verwenden, nur dann zum Aufbau von VPNs, wenn er mit einem Tunnel-Protokoll (z. B. L2TP) kombiniert wird.

Abbildung 51 illustriert den Aufbau eines IPSec-Pakets im Tunnelmodus. Entsprechend stellt Abbildung 52 den Paketaufbau im Transportmodus dar.

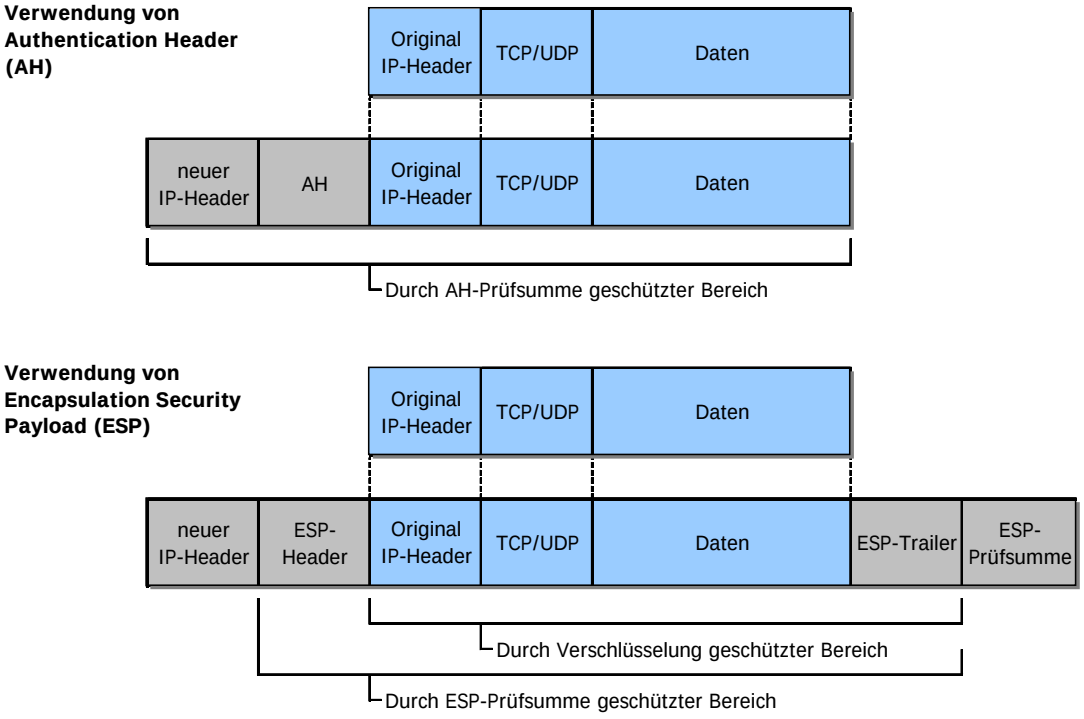



Abbildung 51: IPSec im Tunnelmodus

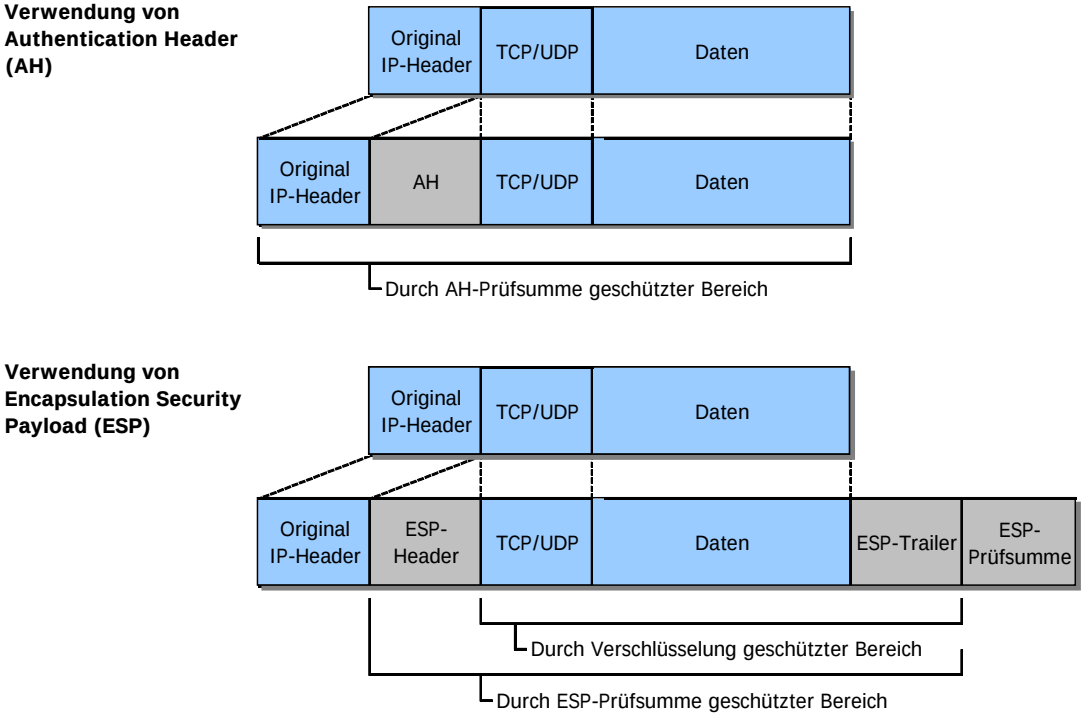



Abbildung 52: IPSec im Transportmodus

Die zum Einsatz der kryptografischen Verfahren, auf denen die Schutzwirkung der IPSec-Mechanismen beruht, notwendigen Parameter (welcher Algorithmus, welche Schlüssel, ...) werden entweder bei der Konfiguration der beteiligten Kommunikationssysteme festgelegt oder aber zwischen den Beteiligten über ein geeignetes Protokoll ausgehandelt. Hier kommt in aller Regel IKE (Internet Key Exchange) – eine pragmatische Teilmenge vom ISAKMP (Internet Security Association and Key Management Protocol) – zum Einsatz.

### 15.3.6 Grenzen und Probleme bei IPSec

IPSec hat sich heute weitestgehend durchgesetzt. Dennoch existieren derzeit noch Einschränkungen. Zwei wesentliche Aspekte, die im Zusammenhang mit dem Einsatz von IPSec bzw. IPSec-basierten VPN-Lösungen zu beachten sind, werden im Folgenden kurz diskutiert.

- **Benutzer-Authentifizierung**

  IPSec unterstützt per se keine benutzerbezogene Identitätsüberprüfung. Dies liegt daran, dass der Zweck, zu dem IPSec entwickelt wurde, lediglich der Schutz einer Kommunikationsbeziehung zweier Partner gegen Angriffe dritter war und ist. Ein gegenseitiger Schutz der beiden Kommunikationspartner vor dem jeweils anderen liegt jenseits der Spezifikation von IPSec und muss im Bedarfsfalle durch separate Mechanismen implementiert werden.

  Im Fall einer transparenten LAN-to-LAN-Kopplung über zwei VPN-Gateways wird eine Benutzer-Authentifizierung in aller Regel nicht benötigt; eine solche Kopplung entspricht letztlich einer herkömmlichen WAN-Verbindung, die im Normalfall auch transparent Übertragungsdienste zur Verfügung stellt. Eine eventuell gewünschte zusätzliche Steuerung im Sinne einer benutzerbezogenen Autorisierung kann in solchen Fällen z. B. durch Einsatz von Firewall-Technik erreicht werden.

  Wird ein VPN hingegen zur Realisierung einer RAS-Lösung eingesetzt oder ist (z. B. zur Absicherung von WLANs) generell auch bei transparentem Netzzugriff eine Prüfung der Nutzeridentität vorgesehen, so sind für VPN-Szenarien die gleichen Anforderungen an die Stärke der Benutzerauthentifizierung zu stellen wie beim klassischen Dial-In. IPSec bietet jedoch keine unmittelbare Benutzerauthentifizierung. Daher muss eine solche auf Umwegen oder über zusätzliche Maßnahmen erreicht werden. Im Einzelnen bestehen unter anderem folgende Möglichkeiten, eine Identifizierung des jenseitigen Benutzers zu gewährleisten:

  - Verwendung von Zertifikaten zur Systemidentifizierung und Bindung dieser Zertifikate an einen Benutzer (z. B. mittels Smartcard, auf der das Zertifikat abgelegt ist)
  - Durchführung einer (in der Regel proprietären) Authentifizierung im Rahmen des Tunnelaufbaus, d. h. während der IKE-Phase (z. B. kann im Schutze des IKE-Tunnels eine Username/Password-Abfrage durch den VPN-Gateway durchgeführt werden)
  - Einsatz von geschachtelten Tunneln, bei denen ein Tunnelmechanismus Benutzerauthentifizierung unterstützt (z. B. L2TP over IPSec; hier kann im Schutz des IPSec-Tunnels sogar auf besondere Maßnahmen zum Schutz der Anmeldeinformationen während der Übertragung verzichtet werden)
  - Nachgelagerte Authentifizierung an einer Firewall (d. h. der Tunnel wird auf der Basis der Systemidentifikation etabliert, aber eine nachgelagerte Firewall verlangt im Rahmen der Autorisierung eine Authentifizierung auf Benutzerebene)

- **Einsatz von NAT**

  Network Address Translation (NAT) stellt ein großes Problem beim Einsatz von VPN-Mechanismen auf IPSec-Basis dar.

  Der Hauptgrund liegt darin, dass Authentication Header, der ja die Integrität der übertragenen Pakete sicherstellen soll, die IP-Adressen des Pakets in die Prüfsummenberechnung mit einbezieht.

Eine nachträgliche Manipulation einer der originalen Adressen führt somit beim Empfänger des IPSec-Pakets zu einer negativen Prüfsummenverifikation und damit zum Verwerfen des empfangenen Pakets.

Weitere Probleme im Zusammenhang mit NAT sind:

- IKE arbeitet unter anderem bei Verwendung von Shared Secrets zur Authentifizierung nicht korrekt mit NAT.
- Bei Einsatz von ESP können im Transportmodus die TCP-Prüfsummen nicht korrekt bearbeitet werden; diese beziehen die IP-Adressen mit ein, die aber durch NAT verändert wurden.
- NAPT (Network Address and Port Translation) und ESP schließen sich grundsätzlich aus, da die TCP/UDP-Ports im verschlüsselten Teil des Datenpakets liegen.

Eine Arbeitsgruppe der Internet Engineering Task Force (IETF) hat sich dieses Problems angenommen und mit NAT Traversal (NAT-T) ein Verfahren entwickelt, das die wesentlichen praxisrelevanten Probleme löst. NAT-T ist seit Anfang 2005 in RFC 3947 und RFC 3948 als Proposed Standard spezifiziert.

NAT-T hat gegenüber am Markt verfügbaren proprietären Mechanismen (s.u.) vor allem folgende Vorteile:

- Durch die Standardisierung ist die Chance auf korrekte Funktion auch in heterogenen Szenarien deutlich größer.
- NAT-T arbeitet vollautomatisch, d. h. eine spezielle Konfiguration der beteiligten Systeme ist nicht erforderlich.
- NAT-T arbeitet auf Transportebene unter Nutzung von UDP und generiert dadurch einen deutlich geringeren Overhead als Verfahren, die einen Tunnel auf Netzwerkebene verwenden (s.u.).

Bis zur flächendeckenden Verfügbarkeit entsprechender Implementierungen am Markt verursacht NAT weiterhin Probleme. Aktuell funktioniert NAT regelmäßig in zwei Fällen:

- NAT wird durch das oder die IPSec-System(e) selbst angewendet; in diesem Fall kann das System, z. B. ein VPN-Gateway, die Auswirkungen von NAT beim Tunnelaufbau in geeigneter Weise berücksichtigen.
- Das eingesetzte VPN-Produkt unterstützt explizit den Einsatz von NAT. Ein solches Feature wird z. B. als NAT Transparent bezeichnet; gemeint ist unabhängig von der jeweiligen Bezeichnung stets, dass innerhalb der durch IPSec geschützten Kommunikationsstrecke NAT angewendet werden kann, ohne dass dies Auswirkungen auf die korrekte Arbeitsweise von IPSec hat. Solche Verfahren werden mittlerweile von den meisten namhaften Anbietern angeboten, sind aber in vielen Fällen noch proprietär[39]. Dementsprechend ist mit Kompatibilitätsproblemen in heterogenen VPN-Szenarien zu rechnen – aufgrund der bisherigen Erfahrungen bei der Standardisierung von IPSec können derartige Probleme zumindest nicht ausgeschlossen werden.

Das Funktionsprinzip der proprietären Lösungsansätze ist simpel: Es wird ein zusätzlicher äußerer IP-Header zum Paket hinzugefügt, d. h. ein Tunnel um das IPSec-Paket herum aufgebaut. Da dieser äußere IP-Header weder von den Sicherheitsmechanismen von IPSec erfasst wird, noch in irgendeiner Form am IKE-Verfahren beteiligt ist, und auch nicht Bestandteil von Prüfmechanismen der IPSec-Payload-Protokolle, können die dort verwendeten Adressen beliebig manipuliert

[39] Auch Verfahren, die vom Hersteller mit „NAT Traversal“ bezeichnet werden, müssen nicht zwangsläufig auf dem IETF-Verfahren basieren, da dieser Begriff nicht geschützt ist.

werden. Die derzeitigen Lösungen unterscheiden sich in der Art der Kapselung; die Bandbreite reicht von UDP über TCP bis zu HTTPS (Hypertext Transfer Protocol Secure).

### 15.3.7 Funktionsweise von L2TP over IPSec

Das Layer 2 Tunneling Protocol (L2TP) stellt eine Weiterentwicklung des Point to Point Tunneling Protocol (PPTP) dar. Ursprünglich zur Realisierung einer Verteilung der Aufgaben physikalischer Verbindungsaufbau und logischer Verbindungsaufbau bei großen Dial-In-Lösungen konzipiert, lässt sich der dazu definierte Tunnel, der die PPP-Verbindungen gleichsam über die Zugangskomponente hinaus „verlängert", auch zum Aufbau von VPNs verwenden. Dazu wird er in Richtung Client verlängert, d. h. der Client etabliert den L2TP-Tunnel anstelle eines Network Access Servers (NAS).

L2TP kapselt die Payload in PPP-Frames, die wiederum auf UDP-Basis in IP-Pakete verpackt werden. Da PPP die Basis des Protokolls darstellt, bietet L2TP – anders als IPSec – insbesondere eingebaute Verfahren zur Benutzerauthentifizierung sowie zur Datenkompression. Eine Verschlüsselung ist optional definiert, wird jedoch in der Praxis kaum verwendet. Stattdessen wendet u. a. die in Windows 2000 und Windows XP eingebaute VPN-Lösung zur Client-Anbindung das L2TP/IPSec-Verfahren an (siehe [L2TP01).

Bei L2TP/IPSec wird zunächst eine IPSec-geschützte Kommunikationsbeziehung zwischen Client und VPN-Server etabliert. Diese verwendet ESP im Transportmodus. Im Schutze dieser Verschlüsselung erfolgt dann der Aufbau des L2TP-Tunnels, über den sowohl die Netzkonfiguration (IP-Adresszuweisung) als auch der Datentransport erfolgt. Hierdurch wird eine zweistufige Authentifizierung erreicht: Im ersten Schritt authentifizieren sich die Computer beim Aufbau der IPSec-Verbindung, im zweiten Schritt die Benutzer beim Aufbau des L2TP-Tunnels. Für die Computerauthentifizierung kommen üblicherweise X.509-Zertifikate und für die Benutzerauthentifizierung beliebige PPP-Authentifizierungsprotokolle zum Einsatz. Die Tatsache, dass bei entsprechender Konfiguration zur Computerauthentifizierung zwingend Zertifikate notwendig sind, führt aus Sicherheitssicht zu einem zusätzlichen Steuerungsmechanismus, da durch die Entscheidung, welche Computer ein entsprechendes Zertifikat erhalten, festgelegt wird, welche Computer am VPN teilnehmen dürfen. Anders als beispielsweise im Falle von PPTP kann so verhindert werden, dass Benutzer mit beliebigen und womöglich unsicheren Windows PCs VPN-Verbindungen ins Unternehmensnetz aufbauen. Vorraussetzung hierfür ist natürlich, dass die entsprechenden Zertifikate von Benutzern nicht auf andere Computer übertragen werden können, was bei Windows grundsätzlich gewährleistet ist.

## 15.4 SSL-VPN

SSL-VPN sollen – so der Tenor aller Hersteller – neben einer möglichst geringen Komplexität der Lösung vor allem den Vorzug haben, in weiten Einsatzbereichen ohne spezielle Client-Software auszukommen. Dies vereinfacht den Ausrollvorgang erheblich, reduziert die notwendige Schulung von Benutzern auf ein Minimum und erhöht die Flexibilität hinsichtlich der Client-Auswahl. Die marktverfügbaren SSL-VPN gehen dazu von einem Terminalserver-Ansatz aus, bei dem als Client ein Standard-Web-Browser zum Zugriff auf bestimmte Applikationen zum Einsatz kommt. Dieser Ansatz musste allerdings mit steigenden Ansprüchen an die Flexibilität der Nutzung erweitert werden, um z. B. File Sharing zu ermöglichen.

Neben diesem – kommerziell forcierten – Ansatz existieren auch Open Source-Projekte, die einen transparenten Netzzugriff, ähnlich wie bei IPSec-basierten VPN, unter Verwendung von Tunneln realisieren.

### 15.4.1 Kommerzielle Ansätze für SSL-VPN auf Browser-Basis

Produktspezifische Mechanismen existieren hier in großer Vielfalt. Die nachfolgende kurze Beschreibung der gängigsten technischen Ansätze für Browser-basierte SSL-VPN kann daher nur einen groben Überblick bieten.

#### Grundprinzip

Anders als IPSec-VPN verwenden SSL-VPN der hier beschriebenen Ausprägung keinen speziellen Client – zumindest in ihrer Grundform – sondern den bereits auf praktisch allen in Frage kommenden Endgeräten vorhandenen Web-Browser. Damit der User mit Hilfe eines Standard-Browsers über ein SSL-VPN zentrale Ressourcen nutzen kann, benötigen diese Ressourcen ein Web-Front-End. Anders gesagt: die jeweilige Anwendung muss „Web-enabled" sein.

Ein Beispiel für eine solche Anwendung ist der OWA-Dienst (Outlook Web Access). OWA ist eine Anwendung, die unter Zuhilfenahme eines Web-Servers dem Browser als Web-Client einen Zugriff auf Exchange-Server ermöglicht. Dabei greift allerdings der Browser nicht direkt auf den Exchange-Server zu, sondern er übermittelt die Benutzer-Aktion (etwa Klicken des Send-Button) per HTTP/HTTPS an den OWA-Server, der dann entsprechend auf den Exchange-Server zugreift.

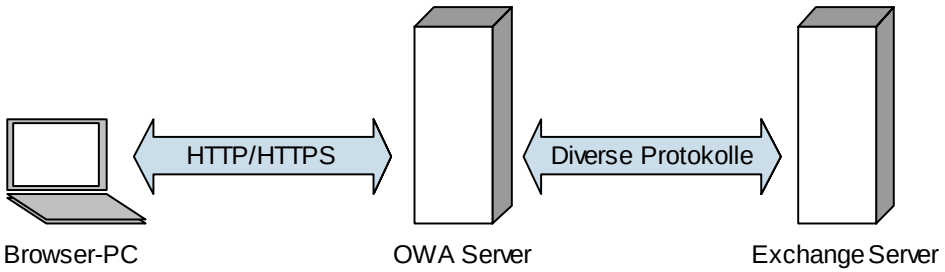



Abbildung 53: SSL-VPN für E-Mail mit Outlook Web Access

Bei diesem Beispiel dient der Browser also nur zur Visualisierung der Vorgänge[40], die eigentlich auf dem OWA-Server ablaufen. Es gibt grundsätzlich verschiedene Möglichkeiten, ein solches Web-Front-End bereitzustellen:

- Erweiterung des Anwendungs-Servers um eine solche Funktion
- Vorschaltung eines anwendungsspezifischen Gateways (wie beim OWA-Beispiel) auf Basis eines Web-Servers
- Vorschaltung eines Web-basierten Terminalservers – dieser muss dann für die gewünschten Applikationen entsprechende Front-Ends beinhalten

Um den eigentlichen Applikationsserver nicht über Gebühr zu belasten – vor allem die Verschlüsselung bei SSL-basierter Kommunikation geht zu Lasten der Leistungsfähigkeit – empfehlen sich die beiden letztgenannten Ansätze. Ein weiterer Vorteil der Verwendung vorgelagerter Systeme ist die Möglichkeit, den Web-Access auch für solche Anwendungen bereitzustellen, bei denen der Server sich dafür prinzipbedingt eher schlecht oder auch gar nicht eignet.

Über die beschriebenen Ansätze hinaus bietet der Markt auch spezielle VPN-Gateways (oft in Appliance-Form), die zum einen die Absicherung von ansonsten nicht hinreichend „VPN-tauglichen" Web-Applikationen[41] übernehmen können, zum anderen aber auch (s.u.) erweiterte Zugriffsmöglich-

---

40 Überhaupt ähneln SSL-VPN-Lösungen sehr stark Terminalserver-Ansätzen (nicht zuletzt deshalb funktionieren andersherum Terminalserver ausgezeichnet auf der Basis von Browser-Clients).

41 Dazu zählen z. B. auch beliebige Intranet-Anwendungen.

keiten für Applikationen bereitstellen, für die kein Web-basierter Zugriff verfügbar bzw. möglich ist. Die übliche technische Realisierung solcher VPN-Gateways basiert auf dem Reverse Proxy-Mechanismus.

### Reverse Proxy

Ein Reverse Proxy sendet im Auftrag bzw. anstelle eines Back-end HTTP-Servers – nicht eines Clients – (deswegen der Begriff Reverse – aus Sicht des Clients) und fungiert somit als Gateway eines Web-Servers oder einer Web-Server-Farm, indem er als die finale IP-Adresse fungiert, die von außen angefragt wird. Aus Sicht eines Clients ist der Reverse Proxy der tatsächliche Web-Server.

Damit dies funktioniert, muss der Reverse Proxy die übertragenen Inhalte manipulieren; beispielsweise werden die verwendeten URLs sowie in den übermittelten Seiten enthaltene Hyperlinks dahingehend modifiziert, dass sie auf den Reverse Proxy verweisen. Für diese Operationen ist neben einer gewissen Intelligenz vor allem auch eine nicht unbeträchtliche Rechenleistung erforderlich.

Reverse Proxies in ihrer Originalform unterstützen nur Web-Applikationen; sollen weitere Anwendungen angeboten werden, müssen zusätzliche Mechanismen implementiert werden.

### Erweiterungen

Nicht immer reichen die Standardmechanismen des Browsers aus, denn je nach Applikation benötigt der Browser eine Erweiterung seiner Möglichkeiten, die ihm allerdings zur Laufzeit mittels entsprechender Plug-Ins (etwa in Form von Java-Applets oder ActiveX-Controls) verabreicht werden können.

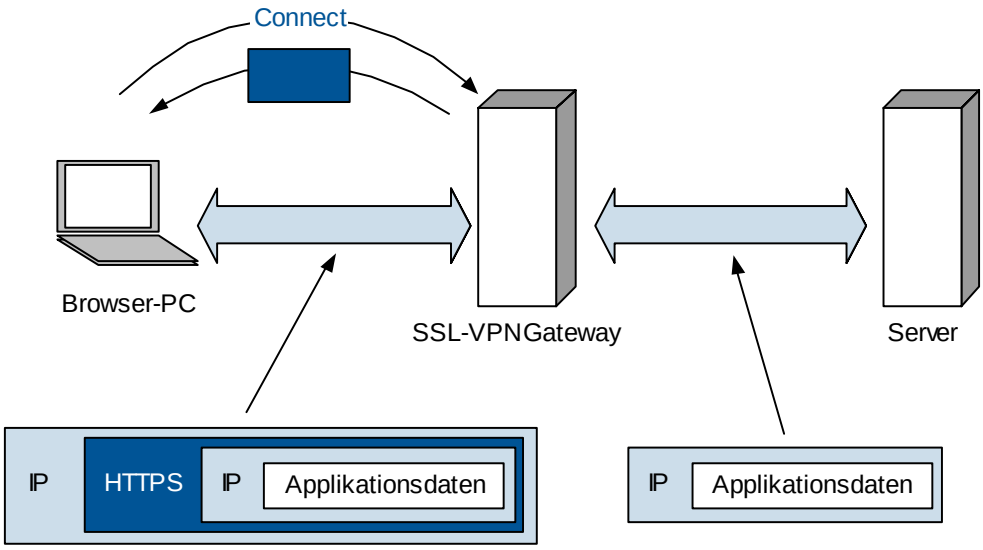



Abbildung 54: Erweiterter VPN-Zugriff mittels Plug-In

### Funktionsweise derartiger Plug-Ins

Üblicherweise verbindet sich der User mit seinem Browser zunächst mit einem auf dem Gateway laufenden Webportal, wobei im ersten Schritt der Server über ein entsprechendes Zertifikat authentifiziert und eine SSL-verschlüsselte HTTP-Verbindung aufgebaut wird. Durch diese Verbindung geschützt, wird im zweiten Schritt der Benutzer vom Portal aufgefordert, sich zu authentifizieren – hier steht je nach Produkt eine Vielzahl verschiedener Authentifizierungsmechanismen zur Verfügung. Nachdem die Authentifizierung erfolgreich abgeschlossen ist, erhält der User Zugriff auf eine auf ihn zugeschnittene Seite, auf der alle Applikationen anwählbar sind, die für den User freigegeben wurden.

Nun wird ein Java-Applet oder ActiveX-Control heruntergeladen, das je nach Produkt verschiedene Funktionen bietet, letztlich jedoch immer ein Ziel verfolgt: Den von einer bestimmten (für den User

freigegebenen) Applikation ausgehenden Datenverkehr abzufangen, einzukapseln und zum Gateway umzuleiten, welches den Verkehr wieder entkapselt und zum ursprünglichen Ziel weiterleitet. In der Rückrichtung werden Antworten des Applikationsservers vom Gateway entgegengenommen, eingekapselt und zum Client gesendet, der diese wiederum entkapselt und der Applikation zur Verfügung stellt. Statt eines Java-Applet oder ActiveX-Control kann je nach Hersteller auch ein vollwertiger 32-Bit-Client installiert werden, der im Vergleich zum browser-basierten Ansatz erweiterte Funktionen bietet.

Bezüglich der Art und Weise, wie letztlich die Umleitung und Kapselung des Datenverkehrs durchgeführt wird, sind zurzeit mehrere verschiedene Implementierungen zu finden, von denen die gängigsten im Folgenden kurz skizziert werden:

### Port Forwarding (Loopback Address/Listener)

Hierbei sorgt das Applet im ersten Schritt für die Änderung der lokalen „hosts"-Datei – und zwar erstellt es dort einen Eintrag mit FQDN (Fully Qualified Domain Name) für die von einer Applikation angefragte Ressource (beispielsweise einen von einem Email-Client angeforderten POP3-Server) und weist diesem FQDN die Loopback-Adresse 127.0.0.1 unter Angabe eines bestimmten Ports zu. Im zweiten Schritt hört das Applet genau diesen Port ab – um herauszufinden, ob Applikationen hiermit kommunizieren wollen. Sobald dieser Fall eintritt, kapselt das Applet den zugehörigen Verkehr in HTTPS und leitet diese Pakete über die bestehende Verbindung zum Gateway. Die Mechanismen zur Kapselung sind i.d.R. herstellerspezifisch. Nach dem Beenden der Applikation wird die modifizierte „hosts"-Datei wieder bereinigt.

Alternativ zur Manipulation der „hosts"-Datei kann ein solches Applet die DNS-Abfragen abfangen und nach „localhost" umleiten. Hierdurch wird dem grundsätzlichen Problem begegnet, dass für Änderungen der „hosts"-Datei üblicherweise Administratorrechte erforderlich sind. Auch hat dieser Vorgang im Fehlerfall keine bleibenden Auswirkungen, beispielsweise beim Absturz eines Client-Rechners – eine nicht bereinigte „hosts"-Datei würde Probleme bereiten, falls dieser Rechner anschließend im LAN benutzt werden soll.

Durch diese Vorgehensweise wird eine für die Applikationen transparente Lösung geschaffen, mit der zunächst jedoch lediglich TCP-basierende Kommunikation mit festen Ports unterstützt wird – weitergehende Unterstützung für populäre, auch komplexeren Verkehr durchführende Applikationen wird i.d.R. durch die Hersteller als Spezialkomponente dediziert eingebaut. Zum Ausführen der Java-Applets oder ActiveX-Controls sind zumeist keine Administratorrechte erforderlich.

### SOCKSv5

Beim SOCKSv5-Ansatz für SSL-VPNs wird ein spezieller Agent auf den Rechner geladen, der mehrere Aufgaben übernimmt: Er überwacht die von zugelassenen Applikationen generierten Socket-Aufrufe (Winsock oder BSD Socket API) und fängt diese ab, um sie in einer durch SSL geschützten SOCKS-Verbindung an einen SOCKS-Proxy weiterzuleiten. Der SOCKS-Proxy ist in diesem Fall das VPN-Gateway, das die ursprünglich vom Client generierten Socket-Aufrufe an dessen Stelle durchführt. Die vom Application-Server erhaltenen Antworten leitet das Gateway über die SOCKS-Verbindung durch den Agent an die Client-Applikation weiter.

Durch diese Vorgehensweise wird eine für die Applikationen transparente, auf bestehenden Standards basierende Lösung geschaffen, mit der nahezu beliebige Applikationen unterstützt werden.

### Virtuelle PPP-Adapter

Bei diesem Ansatz wird vom Web-Portal des VPN-Gateways ein virtueller PPP-Adapter installiert, über den bei Zugriffen auf Ressourcen, die das Gateway bereitstellt, eine PPP-Verbindung zum Gateway aufgebaut wird. Dieser virtuelle Adapter erscheint als zusätzliche Netzwerkverbindung in der Konfiguration des Endgeräts. Ähnlich wie bei IPSec-basierten VPN wird die PPP-Verbindung bei Bedarf auf- bzw. abgebaut; bei bestehendem Tunnel wird der übertragene Datenverkehr mittels SSL geschützt. Nach Abbau des Tunnels wird die auf dem virtuellen PPP-Adapter basierende Netzverbindung wieder aus der Systemkonfiguration entfernt.

Vorteilhaft bei diesem Ansatz ist vor allem die Transparenz des so etablierten VPN-Tunnels: da jeglicher an die jeweiligen Remote-Netze gerichteter Datenverkehr durch diesen Tunnel geroutet werden kann, ist ein Zugriff beliebiger Desktop-Applikationen auf beliebige Ressourcen technisch möglich; eine entsprechende Steuerung erfolgt durch das Gateway.

Nachteilig ist vor allem, dass zur Installation des virtuellen PPP-Adapters i.d.R. Administratorrechte erforderlich sind.

### 15.4.2 OpenVPN als Alternativansatz

OpenVPN ist ein Open Source Projekt und verfolgt einen technologisch anderen Ansatz als die bisher beschriebenen kommerziellen Lösungen.

Anders als die meisten Anbieter von SSL-VPN-Lösungen fokussiert OpenVPN nicht die Notwendigkeit eines speziellen Clients als Hauptproblem IPSec-basierter VPN, sondern die Komplexität, die damit verbundenen Inkompatibilitäten und die technischen Probleme und Einschränkungen von IPSec.

Folgerichtig nutzt auch OpenVPN einen entsprechenden Client, der allerdings zum einen SSL als Schutzmechanimus nutzt, und zum anderen Kernel-nahe Systemmodifikationen und damit verbundene technische wie auch administrative Probleme vermeidet.

Das Grundprinzip dieses Ansatzes ist die Verwendung virtueller Netzadapter (TUN-Interface), welche die zu übertragenden Bits aus dem Kernel-Bereich des Systems in den so genannten User Space transferieren, wo sie durch „beliebige“ Applikationen modifiziert werden können. Beim VPN-Ansatz stellt diese Modifikation das Verkapseln in UDP und Sichern mittels SSL dar[42].

Da die entsprechende VPN-Applikation nicht im Kernel Space residiert, gestaltet sich die Installation erheblich konfliktärmer als bei IPSec, das zwangsläufig den IP-Stack selbst modifiziert (nicht wenige Systeme waren nach fehlgeschlagenem Installationsversuch eines IPSec-Clients nicht mehr zu fehlerfreiem Arbeiten zu bewegen...). Ein weiterer Vorteil ist, dass die OpenVPN-Applikation mit anderen VPN-Mechanismen koexistieren kann – sogar mit einem IPSec-Client.

Bei der Einrichtung des OpenVPN wird das TUN-Interface wie ein normales Netzinterface konfiguriert und als Routingpfad für das über das VPN erreichbare Netz eingerichtet. Der Ablauf der Paketverarbeitung eines zu tunnelnden Datenpakets lässt sich dann wie folgt kurz beschreiben:

Die von der jeweiligen Anwendung generierten Daten werden an das TUN-Interface gesendet. Dieses wiederum übermittelt diese an die OpenVPN-Applikation, die die Kapselung und Absicherung vornimmt. Anschließend sendet die OpenVPN-Applikation das gekapselte Paket an die echte Netzwerkschnittstelle, die sie über das Netz überträgt. Auf der Empfängerseite läuft dieser Prozess in umgekehrter Reihenfolge ab.

Neben OpenVPN existieren noch diverse weitere ähnliche Projekte, die nach dem gleichen Prinzip arbeiten.

### 15.4.3 Authentifizierung und Verschlüsselung bei SSL-VPNs

HTTPS (Hypertext Transfer Protocol Secure) ist ein Protokoll zur Übertragung sensitiver, d. h. schützenswerter Informationen über das Web. Es basiert auf HTTP, schützt jedoch die übertragenen Informationen mit Hilfe der SSL-Technologie (Secure Sockets Layer).

SSL ist als zusätzliches Protokoll zwischen TCP und HTTP angesiedelt. Es leistet sowohl eine gegenseitige Authentifizierung von Client und Server als auch den Schutz der Vertraulichkeit sowie der Integrität der übertragenen Daten durch kryptografische Verfahren. SSL verwendet wie praktisch alle aktuellen Verschlüsselungslösungen eine Hybridtechnik: Die Datenübertragung erfolgt auf der Basis

[42] Rein technisch gesehen wäre die Verwendung von SSL nicht nötig; bereits die Kapselung mittels UDP schafft ein VPN, ähnlich wie bei Verwendung von GRE-Tunneln. Allerdings wäre dann keinerlei Sicherheit für die übertragenen Daten gegeben.

eines zwischen Client und Server auszuhandelnden symmetrischen Kryptoalgorithmus (typischerweise RC4); der dazu erforderliche symmetrische Schlüssel wird während der Verhandlungsphase unter Einsatz asymmetrischer Kryptoalgorithmen (RSA, DH) zwischen den Kommunikationspartnern vereinbart. Während dieses Handshakes erfolgt gleichzeitig die (optional gegenseitige) Authentifizierung.

Bei SSL-VPNs kommt genau diese Verfahrenweise zum Einsatz, wobei die Authentifizierung üblicherweise mehrstufig implementiert ist. Den ersten Schritt stellt hierbei wie oben beschrieben die Authentifizierung des SSL-Servers durch den SSL-Client während des SSL-Handshake dar. Sofern der Benutzer ebenfalls über ein geeignetes Zertifikat verfügt, kann er, wie bereits angedeutet, optional in seiner Funktion als SSL-Client auf die gleiche Weise durch den SSL-Server authentifiziert werden. Von dieser Funktion wird in SSL-VPN-Szenarien allerdings selten Gebrauch gemacht.

Analog zum Verfahren bei TLS (siehe EAP-TLS, Kapitel 7.2.3) sendet der Server sein Zertifikat, woraufhin der Client dieses auf Gültigkeit überprüft, ein sog. Pre-Master Secret kreiert und Public Key-Mechanismen nutzt, um dieses Secret für den Server zu verschlüsseln und anschließend an diesen zu übermitteln. Auf diese Weise wird einerseits die Authentifizierung des Servers, andererseits der Austausch eines Secret erreicht, welches im nächsten Schritt als Grundlage für den Aufbau einer verschlüsselten SSL-Verbindung genutzt wird. Voraussetzung hierfür ist, dass der Server über ein gültiges X.509-Zertifikat verfügen muss, dessen Aussteller der Client vertraut.

Statt die Benutzerauthentifizierung während des SSL-Handshake durchzuführen, wird diese üblicherweise in einer zweiten Stufe nachgeholt: Beim Zugriff auf Ressourcen, beispielsweise auf das Webportal des VPN-Gateways. Hierbei können je nach Gateway-Produkt eine Vielzahl verschiedener Authentifizierungsmerkmale eingesetzt werden, beispielsweise OTPs, X.509-Zertifikate, AD-Benutzer und -Passwort – als Authentifizierungsprotokoll wird häufig RADIUS eingesetzt.

Da der Entwickler der Browser-Software natürlich nicht im Vorfeld weiß, welche Ziele der Anwender mit seinem Browser ansteuern wird, besitzt dieser in der Regel Zertifikate der gängigen Certificate Authorities, denen er vertraut. Auf Windows-Rechnern sind hierzu CA-Zertifikate vieler öffentlicher Trust-Center (z. B. VeriSign, Deutsche Telekom, TC TrustCenter) bereits im Lieferumfang des Betriebssystems enthalten. Kann der Server ein Zertifikat vorlegen, das von einer dieser CAs ausgestellt wurde, wird es vom Browser akzeptiert. Ansonsten muss der Browser (d. h. der Anwender) dem Server-Zertifikat ohne Beglaubigung vertrauen oder ggf. ein neues Zertifikat einer weiteren CA importieren.

An dieser Stelle offenbart sich übrigens eine Schwäche (nämlich eine Entscheidung durch den Benutzer) im System, die für Angriffe auf SSL-geschützte Kommunikationsbeziehungen genutzt werden kann (Man-in-the-Middle-Attacke).

Genauso wie beim IP-VPN gilt: werden native Client-Applikationen in Kombination mit einem für die Applikation transparenten (in diesem Fall durch SSL geschützten) Tunnel genutzt, so finden weitere Authentifizierungsvorgänge statt, die völlig unabhängig von den zuvor geschehenen sind – welche Protokolle und Verfahren hierbei genutzt werden, ist wieder davon abhängig, welche Clienttypen auf welche Ressourcen zugreifen.

## 15.5 Smartcards und Sicherheitstoken

### 15.5.1 Smartcards

Smartcards sind sozusagen Single-Chip-Computer mit einem Speicher von derzeit üblicherweise ca. 8-32 KB[43], die in eine flache Plastikkarte eingebettet sind. Für Authentifizierungszwecke kommen intelligente Karten im ICC-Format (Integrated Circuit Cards) oder im USB-Formfaktor zum Einsatz. Für solche Karten gibt es Chips, die in der Lage sind, komplexe (kryptografische) Operationen wie z. B. digitale RSA-Signaturen durchzuführen.

[43] Es sind auch Karten mit höherem Speichervolumen verfügbar.

Werden Smartcards zur Benutzeranmeldung genutzt, schiebt der User seine Smartcard in den an seinen Computer angeschlossenen Smartcard-Reader und gibt seine zur Smartcard passende PIN ein.

### Ansteuerung von Smartcards

- PKCS #11

  Bei PKCS #11 handelt es sich um die Definition einer Schnittstelle (API, Application Programming Interface) mit dem Namen Cryptoki über die Applikationen auf sogenannte Cryptographic Token zugreifen können. Diese Token sind zunächst einmal abstrakte Gebilde, die Funktionen wie Ver- und Entschlüsselung sowie Signatur und Verifizierung von Daten ermöglichen. Über PKCS #11 wird eine einheitliche Schnittstelle definiert, die den normierten Zugriff auf die Token erlaubt. Für die Programme spielt es dabei keine Rolle mehr, ob es sich um Hardware (Chipkarten und Ähnliches) oder rein software-basierte Token handelt.

  PKCS #11 wurde von RSA Security in Zusammenarbeit mit anderen Firmen entwickelt und stellt den de-facto-Standard dar.

- Java Cryptography Architecture

  PKCS #11 wird seit J2SE 5.0 auch von der Java Cryptography Architecture (JCA) unterstützt, um entsprechende Tokens bzw. Smartcards in die Java-Plattform zu integrieren. Es ist davon auszugehen, dass die JCA eine wichtige Rolle für die Programmierung und Anwendung von Smartcards spielen wird.

- CryptoAPI und CSPs

  Hierbei handelt es sich um eine in das Betriebssystem integrierte Lösung von Microsoft, die Applikationen den Zugriff auf kryptografische Funktionen ermöglicht.

  CryptoAPI stellt eine Schnittstelle für die kryptografischen Funktionen der installierbaren CSP-Module (Cryptographic Service Provider) dar. CryptoAPI und somit CSP-Dienste stehen allen Applikationen und Diensten zur Verfügung, die kryptografische Dienste benötigen, beispielsweise den mit VPN zusammenhängenden Diensten (z. B. IPSec) oder den verschiedenen Outlook-Versionen. Auch bei der Installation der Windows 2000/2003 Zertifikatsdienste muss ein CSP gewählt werden, wodurch unter anderem der Speicherort und die maximale Schlüssellänge des Schlüsselpaars der Zertifizierungsstelle beeinflusst werden.

## 15.5.2 Sicherheitstoken

Solche Token sind im Prinzip Generatoren für Einmal-Passwörter, d. h. Passwörter, die nur für einen einzigen bestimmten Login-Vorgang gültig sind. Sie erzeugen die Passwörter auf der Basis eines geheimen Schlüssels, der das Token eindeutig kennzeichnet, sowie einer zusätzlichen Information mit Einmaligkeitscharakter – die beiden am weitesten verbreiteten Verfahren nutzen für diesen Zweck die aktuelle Systemzeit bzw. eine zufällig erzeugte Challenge.

Diese Token können entweder in Form einer speziellen Hardware – z. B. in der Art einer Scheckkarte oder als Schlüsselanhänger – oder als Software realisiert sein. Aus Sicherheitserwägungen heraus ist die Hardware-Variante eindeutig zu bevorzugen, da sie die geheimen Schlüssel optimal gegen Auslesen und Kopieren schützt und außerdem prinzipiell am ehesten der Anforderung der Bindung der Authentifizierung an eine Person anstelle eines Gerätes gerecht wird.

Allerdings funktioniert dieses Prinzip nur, wenn die Anwender sorgfältig mit den Token umgehen: wird das Token z. B. zusammen mit dem Client-System aufbewahrt, so verhindert nur noch das bei diesen Systemen verwendete zweite Authentifizierungsmerkmal, eine nur dem Benutzer bekannte PIN, einen Missbrauch. Die PIN allein ist allerdings ein schwacher Authentifizierungsmechanismus, da sie statisch und mit üblicherweise 4 Ziffern sehr kurz ist, und Anwender mitunter dazu neigen, diese PIN zu notieren oder in anderer Weise leichtfertig damit umzugehen. An dieser Stelle sei nochmals

auf die Möglichkeit der Verwendung biometrischer Verfahren hingewiesen, speziell auf die Erkennung eines Fingerabdrucks als Alternative zur PIN.

Anstatt eines echten Hardware-Token kann auch eine Software-Implementierung eingesetzt werden, sofern diese auf einer separaten Hardware erfolgt – etwa einem PDA. Da die Token unabhängig von ihrer physikalischen Realisierung ganz normale Passwörter generieren, können sie in nahezu allen Bereichen eingesetzt werden, in denen Authentifizierung zu leisten ist. Es muss lediglich eine Schnittstelle zwischen den betroffenen Systemen und dem Token-Server, der die Korrektheit der Passwörter überprüft, existieren; in der Praxis geschieht dies meist über einen RADIUS-Server.

## 15.6 Public Key Infrastructure

### 15.6.1 Schlüsselmanagement

Alle Verschlüsselungsverfahren, ob symmetrisch oder asymmetrisch, verwenden Schlüssel zur Chiffrierung des Klartextes; der Schlüssel stellt sogar – einen guten Chiffrier-Algorithmus unterstellt – das maßgebliche Element des Verschlüsselungssystems dar: von ihm, seinem Schutz und seiner Integrität hängt die Sicherheit des gesamten Kryptosystems ab. Bei symmetrischen Schlüsseln bedeutet dies, dass sie stets geheim zu halten sind und nur geschützt übertragen werden dürfen. Bei der Alternative – der Verwendung asymmetrischer Schlüsselpaare – kommt es zwar nicht auf Geheimhaltung, wohl aber auf Integrität des öffentlichen Schlüssels an. Wie kann nun die Bereitstellung integrer öffentlicher Schlüssel erfolgen?

Am einfachsten ist es in den meisten Fällen, auf die Dienste so genannter Trust-Center zurückzugreifen, welche die notwendigen Dienste des Schlüsselmanagements, d. h. der zentralen Verwaltung und Administration der Schlüsselinformationen zur Verfügung stellen. Im Folgenden sollen einige Aspekte den Aufbau einer derartigen Verwaltungsstruktur – einer so genannten Public Key Infrastructure (PKI) – dargestellt werden.

Eine solche Aufgabe stellt gewisse Herausforderungen an Planung und Administration, aber auch an Anbieter entsprechender Lösungen und/oder Produkte. Grundsätzlich gilt es in jedem Fall, beim Aufbau einer eigenen derartigen PKI alle aktuellen und zukünftigen Einsatzgebiete von Verschlüsselungstechniken mit zu berücksichtigen, um etwa das Entstehen mehrerer PKI-Inseln, die zueinander inkompatibel sind, zu vermeiden.

### 15.6.2 Aufgaben einer Public Key Infrastructure

Die Aufgaben einer Public Key Infrastructure (PKI) lassen sich folgendermaßen beschreiben:

Eine PKI muss das Schlüsselmanagement für (möglichst) alle eingesetzten asymmetrischen Verschlüsselungstechniken leisten. Dazu gehören insbesondere Aufgaben wie die Erstellung, die Verteilung bzw. Bereitstellung sowie die Sperrung bzw. den Widerruf von Schlüsseln.

Eine PKI muss die notwendigen kryptografischen Dienste zur funktional geeigneten und sicheren Abbildung dieses Schlüsselmanagements bzw. der damit verbundenen Aufgaben auf eine Client-Server-Struktur bereitstellen.

Eine PKI muss in geeigneter Weise die Erstellung sowie die Verifikation von Zertifikaten ermöglichen.

### 15.6.3 Zertifikate

Zertifikate sind – kurz gesagt – beglaubigte öffentliche Schlüssel. Öffentliche Schlüssel unterliegen zwar nicht der Geheimhaltung, wohl aber muss sichergestellt sein, dass sie echt sind, d. h. dass sie wirklich demjenigen zugeordnet sind, von dem man das annimmt.

Kann man dies nicht mit Hilfe des Schlüsselbesitzers selbst sicherstellen, so verlässt man sich auf eine vertrauenswürdige Instanz, die die Korrektheit des Schlüssels bestätigt. Dazu erstellt diese Instanz einen Datensatz, aus dem die Identität des Schlüsselbesitzers sowie der Wert des öffentlichen Schlüssels hervorgehen, und signiert diesen Datensatz digital. Ein derartiger signierter Datensatz wird als Zertifikat bezeichnet, die ausstellende Instanz als Certificate Authority (CA). Jeder, der den öffentlichen Schlüssel des Besitzers eines solchen Zertifikats auf Integrität prüfen möchte, kann dies einfach dadurch tun, dass er die Authentizität der digitalen Signatur der CA prüft. Für diese Prüfung benötigt er den öffentlichen Schlüssel dieser CA, dessen Echtheit wiederum mittels eines Zertifikats – diesmal einer übergeordneten CA – beglaubigt wird. Auf diese Weise lässt sich nach und nach die Integrität eines beliebigen öffentlichen Schlüssels verifizieren, sofern es in der Kette der CAs mindestens eine gibt, der man vertraut und deren öffentlichen Schlüssel man als echt akzeptiert. Schlimmstenfalls muss man den öffentlichen Schlüssel der obersten CA manuell verifizieren, d. h. vor Ort vorsprechen und sich dort eine Kopie des Schlüssels besorgen. Dies ist ein Aufwand, den man für eine oder wenige CAs durchaus betreiben kann, nicht hingegen für jeden öffentlichen Schlüssel, den man irgendwann einmal zur Kommunikation benötigen könnte.

Der aktuell gültige Standard für solche digitalen Zertifikate ist X.509 in der Version 3. Der Aufbau eines Zertifikats nach der X.509-Spezifikation ist in Abbildung 55 illustriert.

### 15.6.4 PKI-Komponenten

Eine PKI besteht im Wesentlichen aus den folgenden Elementen:

- Certificate Authority (CA)

  Die CA ist diejenige Instanz innerhalb einer PKI, die digitale Zertifikate ausstellt und verwaltet.

- Registration Authority (RA)

  Die RA ist diejenige Instanz innerhalb einer PKI, welche die Endnutzer der PKI identifiziert und registriert.

- Zertifikate

  Ein Zertifikat stellt die beglaubigte Zuordnung eines asymmetrischen Schlüsselpaares zu einem Endnutzer dar.

- Zertifikats-Sperrlisten (Certificate Revocation List, CRL)

  Aus unterschiedlichen Gründen als ungültig anzusehende Zertifikate müssen entsprechend gekennzeichnet bzw. ihre Ungültigkeit muss publik gemacht werden können. Hierzu dienen entsprechende Datensammlungen in Listenform.

- Key Server

  Ein Key Server ist diejenige Instanz innerhalb einer PKI, auf der die CA die Schlüsselinformationen ablegen und von der diese Informationen bei Bedarf abgerufen werden können.

- Directory-Dienste

  Directory-Dienste dienen dem Zugriff auf die Informationsbestände der PKI.

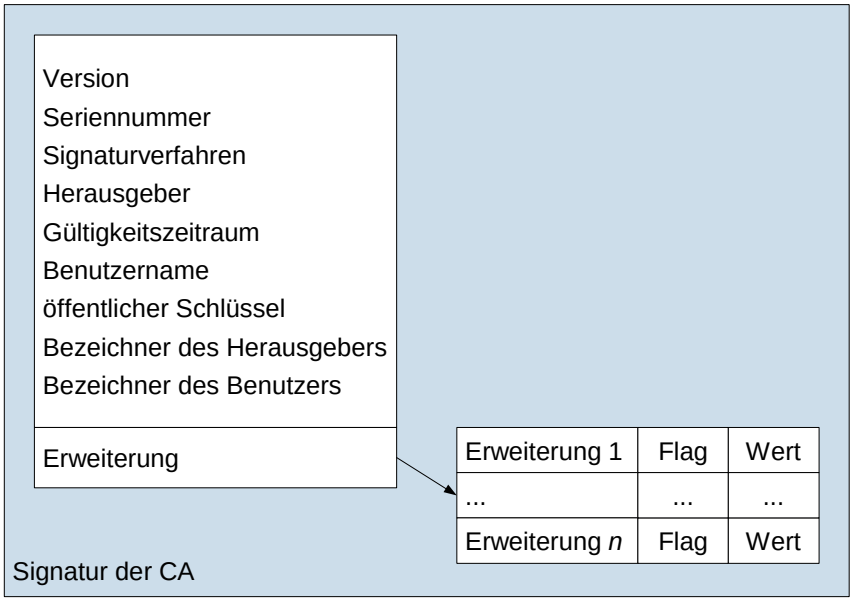



Abbildung 55: X.509-Zertifikat

### 15.6.5 Planung einer PKI

Überall dort, wo Zertifikate (und somit private/öffentliche Schlüssel) genutzt werden, spielt deren Management naturgemäß eine Rolle – je nach Nutzungsart und -intensität ist eine firmeninterne PKI sinnvoll bis beinahe unumgänglich, manche Einsatzgebiete erfordern allerdings eher Zertifikate, die von anerkannten öffentlichen Trust-Centern ausgestellt wurden. Weiterhin gilt grundsätzlich: Kommunikationspartner, die sich zertifikatsbasiert authentifizieren, prüfen das Zertifikat des Gegenübers auf Authentizität und Gültigkeit und bringen in Erfahrung, ob das Zertifikat von der ausstellenden CA zurückgezogen wurde. Zur Prüfung der Authentizität der Peer-Zertifikate müssen die Peers den CAs vertrauen, die die Zertifikate ausgestellt haben – hierzu benötigen sie die CA-Zertifikate, die ihnen auf gesichertem Wege zur Verfügung gestellt werden müssen. Auf Windows-Rechnern sind CA-Zertifikate vieler öffentlicher Trust-Center (z. B. VeriSign, Deutsche Telekom, TC TrustCenter) bereits im Lieferumfang des Betriebssystems enthalten. Unter Linux ist die Bereitstellung solcher Zertifikate den jeweiligen Anwendungen und/oder Libraries überlassen[44].

Der Aufbau einer internen PKI ist sorgfältig zu planen, es gibt eine Vielzahl von Fallstricken, viele Eventualitäten sind zu beachten – keinesfalls sollte hier ausschließlich mit Focus auf ein spezielles Thema (wie z. B. WLAN) implementiert werden. Mittlerweile weist der Markt viele verschiedene PKI-Lösungen auf, die sich allerdings in Anspruch, mögliche Einsatzgebiete, Funktionsumfang und Preis deutlich unterscheiden. Informationen zur Verwaltungs-PKI für Behörden findet man auf den Internetseiten des BSI, siehe [SPHINXa]. Dies beinhaltet insbesondere auch die Beschreibungen zur Struktur der Verwaltungs-PKI, siehe [SPHINXb], und zur European Bridge-CA, siehe [SPHINXc].

Im Folgenden wird ein Auszug wichtiger Themen/Fragestellungen hierzu wiedergegeben:

- Für welche Anwendungszwecke sollen Zertifikate ausgestellt werden?
- Welche konkreten Applikationen sollen mit der PKI zusammenarbeiten? Welche Schnittstellen sind notwendig bzw. werden unterstützt?
- Interoperabilität, Handling von Produkten unterschiedlicher Hersteller

---

44 Die SSL Library besitzt beispielsweise eine Datei namens cert.pem, die z. B. unter /user/share/ssl abgelegt ist. Hier finden sich die Zertifikate der vertrauenswürdigen CA. Bei dem Mozilla-Browser (firefox) sind die vordefinierten Zertifikate der CAs in den Code hinein kompiliert.

- Integration in Verzeichnisdienste, Mapping Zertifikat zu User
- Sind Zertifikatsbeantragung, -ausstellung und -erneuerung automatisierbar?
- Ablaufende Zertifikate bzw. Zertifikatserneuerung ist ein Thema, das oft nicht wahrgenommen oder unterschätzt wird.
- Unterstützung der Überwachung der Lebenszyklen von Zertifikaten
- CRL Distribution Point muss zugänglich sein. Wird ggf. OCSP (Online Certificate Status Protocol) unterstützt?
- Zertifikatsfluss allgemein, Administration, Organisation, Zuständigkeiten, Delegierung
- Umgang mit Schlüsselverlust, Wiederherstellbarkeit von verschlüsselten Daten
- Hohe Sicherheit bezüglich der verwendeten kryptografischen Verfahren
- Anbindung externer Kommunikationspartner
- Kopplung von PKIs (auch unterschiedlicher Hersteller)

### 15.6.6 Beispiele für zertifikatsbasierte Authentifizierung

Zur Absicherung von WLANs über VPN-Techniken sind u. a. die folgenden Szenarien denkbar, bei denen zertifikatsbasierte Authentifizierung eingesetzt wird:

**IP-VPN**

1. VPN-Gateway(s) und -Clients verfügen über IPSec-Zertifikate, die während der IKE-Aushandlungen zur Authentifizierung genutzt werden. Der Zugriff auf den privaten Schlüssel ist auf den Clients durch eine PIN oder Passphrase geschützt, die ausschließlich dem User bekannt ist und die dieser beim Aufbau der IPSec-Verbindung eingeben muss.

   Bei dieser Lösung wird eine große Zahl von Zertifikaten benötigt. Dies legt aus Kostengründen den Einsatz einer firmeninternen privaten PKI nahe.

2. VPN-Gateway(s) und -Clients verfügen über IPSec-Zertifikate, die während der IKE-Aushandlungen zur Authentifizierung genutzt werden. Im Gegensatz zum vorigen Szenario ist der private Schlüssel nicht an den Benutzer, sondern an den Computer gebunden, wodurch sich nun der Computer authentifiziert. Nach Aufbau der IPSec-Verbindung wird ein L2TP-Tunnel aufgebaut, wobei der Benutzer sich gesondert authentifiziert (evtl. zertifikatsbasiert mit Smartcard).

   Bei dieser Lösung wird eine große Zahl von Zertifikaten benötigt. Sofern die Benutzer sich zertifikatsbasiert authentifizieren, ist diese Zahl noch deutlich höher als im vorigen Szenario. Dies legt aus Kostengründen den Einsatz einer firmeninternen privaten PKI nahe.

**SSL-VPN**

3. Lediglich das VPN-Gateway verfügt über ein SSL-Zertifikat. Während des SSL-Handshake sendet das Gateway dieses an die Clients, die es zur Authentifizierung des Servers sowie zum Austausch des Pre-Master-Secret nutzen. Die Benutzerauthentifizierung erfolgt nicht zertifikatsbasiert.

   Bei dieser Lösung wird lediglich ein Zertifikat benötigt. Aus diesem Grund sind die Kosten auch bei Verwendung eines Zertifikats eines öffentlichen Trust-Centers gering.

4. Das VPN-Gateway verfügt über ein SSL-Zertifikat. Während des SSL-Handshake sendet das Gateway dieses an die Clients, die es zur Authentifizierung des Servers sowie zum Austausch des Pre-Master-Secret nutzen. Die Benutzerauthentifizierung erfolgt zertifikatsbasiert über Smartcard.

   Bei dieser Lösung wird eine große Zahl von Zertifikaten benötigt. Dies legt aus Kostengründen den Einsatz einer firmeninternen privaten PKI nahe.

## 15.7 RADIUS

Der Remote Authentication Dial In User Service (RADIUS) ist ein Client-Server-Protokoll zur zentralen Verwaltung und Bereitstellung von Services für Remote User. RADIUS ist in RFC 2865 spezifiziert und als Draft Standard klassifiziert, siehe [RADI00a]. Das Protokoll wird von praktisch allen etablierten Anbietern von Lösungen für Remote Access-Szenarien implementiert und kann daher ausgezeichnet als gemeinsame Schnittstelle zwischen Produkten verschiedener Hersteller dienen.

Hauptanliegen beim Design des Protokolls war es, eine sichere und zuverlässige Möglichkeit zu schaffen, mit geringem Overhead die für RAS notwendigen Parameter auf zentralen Servern vorzuhalten, anstatt sie auf jedem einzelnen NAS einzurichten.

RADIUS unterstützt drei Dienste im Zusammenhang mit RAS: Authentifizierung, Autorisierung und Verrechnung bzw. Kontoführung (Accounting); ein RADIUS-Server wird daher mitunter auch als AAA-Server („Triple-A-Server“) bezeichnet.

Bei Einsatz von RADIUS agiert der NAS (oder allgemein: der Authenticator) als RADIUS-Client: er leitet die Benutzerinformation (User-ID, Kennwort-Information usw.) an den RADIUS-Server weiter und handelt bei der Zulassung oder Abweisung von Clients auf Anweisungen des RADIUS-Servers. Der RADIUS-Server kann seinerseits wiederum Client eines weiteren Authentifizierungs-Servers – entweder eines weiteren RADIUS-, Token- oder allgemein eines Security-Servers – sein; in diesem Fall agiert er als Proxy gegenüber dem Authenticator.

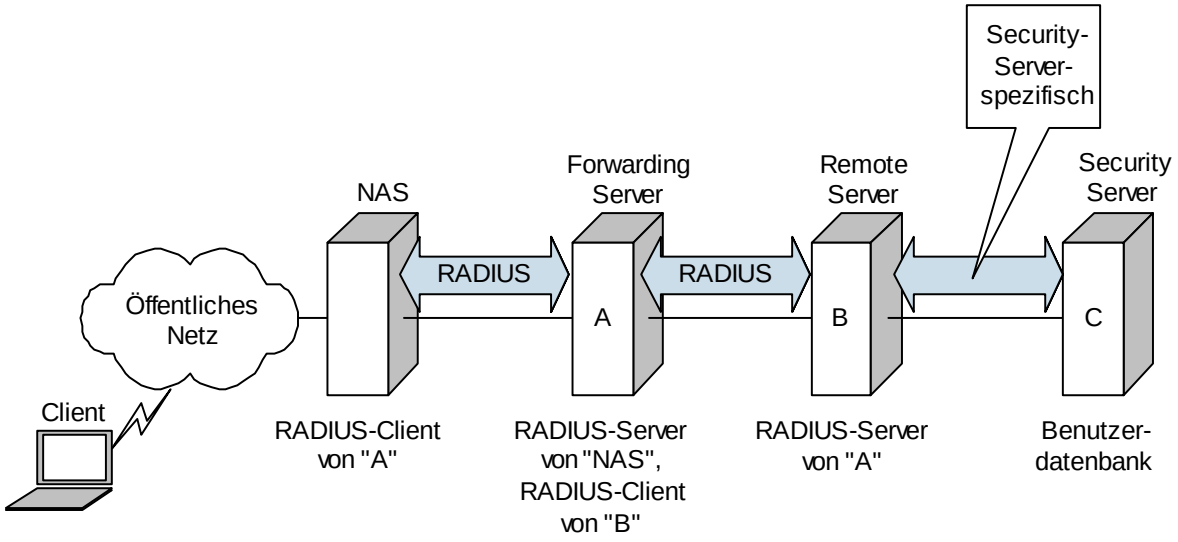



Abbildung 56: Client-Server-Architektur von RADIUS

Basis der Kommunikation zwischen RADIUS-Client und -Server ist UDP. Der offizielle Standard-Port für den Zweck Authentifizierung ist 1812, historisch bedingt verwenden aber viele Implementierungen nach wie vor den Port 1645. UDP wurde gegenüber TCP insbesondere wegen des geringeren Overheads und der Verbindungslosigkeit der Vorzug gegeben; letztere ermöglicht unter anderem auf einfache Weise sowohl ein Multithreading einer sehr großen Zahl paralleler Authentifizierungsvorgänge als auch einen simplen Redundanzmechanismus.

### 15.7.1 Authentifizierung

Den ersten Schritt der RADIUS-Kommunikation stellt immer eine vom RADIUS-Client an den RADIUS-Server gesendete Access-Request-Meldung dar, auf die der Server im nächsten Schritt meist direkt mit einer Access-Accept- oder Access-Reject-Meldung antwortet. Dieser Ablauf wird je nach

gewähltem Authentifizierungsverfahren um einen oder mehrere Zwischenschritte erweitert, bei dem der Server eine Access-Challenge-Meldung an den Client sendet, auf die der Client mit einer erneuten Access-Request-Meldung (inkl. Response auf die Challenge) antwortet.

Ein RADIUS-Server kann vielfältige Authentifizierungsschemata bedienen, darunter u. a.

- PPP-PAP
- PPP-CHAP
- Challenge/Response-Mechanismen
- Sonstige Token-Mechanismen
- EAP

Ursprünglich (RFC 2865) wurden lediglich PAP, CHAP und Challenge/Response innerhalb von RADIUS definiert, im Laufe der Zeit sind allerdings eine Vielzahl weiterer Verfahren hinzugekommen, von denen vor allem EAP (RADIUS Support For EAP, RFC 3579, siehe [RADI03a]) in letzter Zeit an Bedeutung gewonnen hat. Wie in Kapitel 7.2 bereits ausgeführt, können innerhalb des EAP-Gerüsts nahezu beliebige Authentifizierungsverfahren genutzt werden. Dies gilt auch im Zusammenhang mit RADIUS, sofern die folgenden Voraussetzungen erfüllt sind:

- NAS-Client ( = EAP-Client) und EAP-Server unterstützen das EAP-Gerüst und die gewählte EAP-Methode vollständig.
- Alle an der Authentifizierung beteiligten RADIUS-Clients und -Server unterstützen die Kapselung von EAP in RADIUS (im RADIUS-Attribute EAP-Message) und die Erstellung und Prüfung des sog. Message Authenticator. (im gleichnamigen RADIUS-Attribut).
- Soll Schlüsselmaterial, das zwischen EAP-Client und Server vereinbart wurde, zum RADIUS-Client gelangen, so müssen EAP-Server und RADIUS-Client sowie alle zwischen diesen beiden befindlichen RADIUS-Server eine Methode unterstützen, mit der dieses Schlüsselmaterial übertragen wird

Die Anzahl der zwischen EAP-Client und -Server fließenden und somit in RADIUS zu kapselnden EAP-Meldungen ist vom verwendeten EAP-Typ abhängig. Der EAP-Typ bestimmt hierbei, wie viele Folgen von Access-Request- und Access-Challenge-Paketen aus RADIUS-Sicht in die eine oder andere Richtung übertragen werden. Sämtliche EAP-Meldungen vom Client an den Server werden in Access-Request-Pakete gekapselt. Die Antwort-Meldungen des Servers werden in Access-Challenge-Pakete eingebettet. Dies geschieht abgesehen vom finalen EAP-Paket, das in ein Access-Accept- oder Access-Reject-Paket gekapselt wird.

### 15.7.2 Autorisierung

Die Komponente Autorisierung eines RADIUS-Servers ist das Resultat einer erfolgreichen Authentifizierung unter Berücksichtigung von Zugriffsrichtlinien für den nun authentifizierten und somit eindeutig zuordenbaren Benutzer. Zur Steuerung des Zugriffs steht je nach Produkt und Implementierung eine große Zahl von verschiedenen Bedingungen (z. B. Zugehörigkeit zu einer bestimmten Benutzergruppe, bestimmte Tageszeit/Wochentag, Einwahlmedium usw.) zur Verfügung, die in entsprechenden Richtlinien miteinander gekoppelt werden können. Abhängig von der Entscheidung des RADIUS-Servers, ob der Zugriff aufgrund der zu erfüllenden Bedingungen gestattet oder verweigert wird, stellt der NAS letztlich die Verbindung zum Client her oder trennt diese – üblicherweise unter Angabe des Grundes der Trennung.

Um miteinander erfolgreich kommunizieren zu können, müssen sich RADIUS-Client und -Server authentifizieren. Basis dieser Authentifizierung ist ein gemeinsames Geheimnis, mit dem Teile der zwischen Client und Server übermittelten RADIUS-Meldungen verschlüsselt werden. Welche Teile dies konkret sind, und ob hierdurch sowohl Client als auch Server authentifiziert werden, ist vom gewählten Authentifizierungsschema abhängig.

Bei PAP wird beispielsweise das RADIUS-Attribut User-Password einer Access-Request-Meldung mit einem Wert befüllt, der durch eine XOR-Verknüpfung des Benutzerkennworts mit einem Hash-

wert entsteht. Dieser Hashwert wiederum wird aus einer Verkettung des gemeinsamen Geheimnisses mit einer Zufallszahl (dem sog. Request Authenticator) mittels MD5 gebildet. Der gesamte Mechanismus wird auch als „User-Password hiding“ bezeichnet. In der umgekehrten Richtung enthalten Access-Accept-Pakete einen sog. Response Authenticator, der einen aus einer Verkettung verschiedenster Werte gebildeten MD5-Hashwert enthält – u. a. auch des gemeinsamen Geheimnisses. Somit kann bei PAP von einer gegenseitigen Authentifizierung von RADIUS-Client und -Server gesprochen werden.

Bei CHAP werden in Zusammenhang mit der Access-Request-Meldung keinerlei Maßnahmen durchgeführt, anhand derer der Server überprüfen kann, ob der Client über das gemeinsame Geheimnis verfügt – so muss der Server sich damit begnügen, die IP-Adressen der Absender solcher Pakete mit den Adressen der bei ihm eingetragenen RADIUS-Clients zu vergleichen. Analog zum Verfahren bei PAP kann der Client mittels des vom Server übermittelten Response-Authenticator aber zumindest den Server authentifizieren.

Bei der Erweiterung von RADIUS im Zusammenhang mit EAP (RADIUS Extensions, RFC 2869, siehe [RADI00b]) wurde schließlich ein weiter oben bereits erwähntes neues RADIUS-Attribut eingeführt, um die Authentizität sowohl von RADIUS-Client und -Server sicherzustellen: der Message-Authenticator. Dieses früher auch „Signature“ genannte Attribut enthält einen mit dem HMAC-MD5-Verfahren gebildeten Hash, wobei das gemeinsame Geheimnis als Schlüssel benutzt wird. Im Falle von EAP müssen sämtliche RADIUS-Meldungen einen solchen Message-Authenticator enthalten, bei allen anderen Authentifizierungsverfahren kann dies optional festgelegt werden. Gebildet wird dieser Hash bei Access-Request-Meldungen aus dem gesamten Paket, bei allen anderen Meldungen (Access-Accept, -Reject oder -Challenge) aus nahezu allen Werten der Pakte, jedoch kommt hier der empfangene Request-Authenticator hinzu und der Response-Authenticator fällt weg, da er erst zu einem späteren Zeitpunkt berechnet und dem Paket hinzugefügt wird. Somit trägt der Message-Authenticator nicht nur zur Gewährleistung der Authentizität von RADIUS-Client und -Server bei, sondern auch zur Sicherstellung der Integrität sämtlicher übermittelter RADIUS-Meldungen.

Bereits im März 1999 hat Microsoft eine Reihe von herstellerspezifischen RADIUS-Erweiterungen veröffentlicht (Microsoft RADIUS-Extensions, RFC 2548, siehe [MRA99]). Hiermit sollte anderen Herstellern von RADIUS-Produkten eine Möglichkeit gegeben werden, Interoperabilität mit Microsoft-proprietären Verfahren und Protokollen zu erreichen. Hiervon ist in der Folge auch Gebrauch gemacht worden, so dass heutzutage viele gängige RADIUS-Produkte mit Attributen zur Unterstützung von MS-CHAP, MPPE oder BAP umgehen können.

Bei der Absicherung von WLANs und auch beim Aufbau von PPTP-Tunneln spielen insbesondere die beiden Attribute MS-MPPE-Recv-Key und MS-MPPE-Send-Key eine große Rolle, da durch sie Schlüsselmaterial zum RADIUS-Client gelangt, das zuvor ein RADIUS-/EAP-Server mit einem NAS-/EAP-Client vereinbart hat. Sofern dieses Schlüsselmaterial in weiteren Schritten zum Aufbau einer verschlüsselten Verbindung zwischen NAS und Client genutzt werden soll, ist der NAS darauf angewiesen, dieses auch zu erhalten. Der Transfer vom RADIUS-Server zum RADIUS-Client verläuft im Rahmen des Access-Accept-Pakets, das in den entsprechenden Attributen das jeweilige Schlüsselmaterial enthält. Dieses Schlüsselmaterial wird über ein ähnliches Verfahren geschützt wie beim zuvor beschriebenen User-Password hiding bei RADIUS-PAP – also mittels MD5 und XOR-Verknüpfungen.

Zur Absicherung des zwischen RADIUS-Client und -Server fließenden Verkehrs wird für künftige RADIUS-Implementierungen zur Erhöhung der Sicherheit die Benutzung von IPSec empfohlen (RFC 3576, siehe [RADI03b], RFC 3579, siehe [RADI03a]). Dies gilt nicht nur für den Verkehr, der durch die RADIUS-Dienste Authentifizierung und Autorisierung generiert wird, sondern auch für den Bereich Accounting. Davon unabhängig sollten die gemeinsamen Geheimnisse mehrerer RADIUS-Client/-Server-Paare verschieden und so komplex sein, wie dies auch grundsätzlich von kritischen Passwörtern gefordert wird.

### 15.7.3 Accounting

RADIUS Accounting ist in einem gesonderten RFC beschrieben (RFC 2866, siehe [RADI00c]) und dient grundsätzlich dazu, Informationen zu den von Usern in Anspruch genommenen Diensten an einer zentralen Stelle zu sammeln, um diese ggf. später auswerten zu können. Hierzu generiert ein RADIUS-Client ein sog. Accounting-Start-Paket, das u. a. den User-Namen, die IP-Adresse und eine Bezeichnung des bereitgestellten Dienstes enthalten kann und sendet dieses Paket an den RADIUS-Server, woraufhin dieser eine Empfangsbestätigung schickt. Bei Service-Ende generiert der RADIUS-Client ein Accounting-Stop-Paket, in dem ebenso beispielsweise Angaben zur Art des Dienstes sowie statistische Daten enthalten sein können. Sowohl Accounting-Start"- als auch Accounting-Stop-Pakete fallen unter den Oberbegriff Accounting-Request, die zugehörigen Empfangsbestätigungen unter Accounting-Response. Ähnlich wie bei der Authentifizierung ist der offizielle Standard-Port für den Zweck Accounting 1813, historisch bedingt verwenden aber viele Implementierungen nach wie vor den Port 1646.

Auch zur Übermittlung von Accounting-Paketen müssen sich RADIUS-Client und -Server authentifizieren. Auch hier bildet ein gemeinsames Geheimnis die Grundlage, wobei es in den entsprechenden Paketen jeweils als ein Element eines Oktettstroms benutzt wird, aus dem mittels MD5 ein Hashwert erzeugt wird. Ähnlich wie bei den oben beschriebenen Verfahren setzt sich der Oktettstrom darüber hinaus aus weiteren Teilen der jeweils zu übertragenden Accounting-Pakete zusammen. Der nun jedem Paket hinzugefügte individuelle Hashwert wird von der Gegenseite auf Übereinstimmung geprüft und das Paket im Zweifelsfall verworfen.

# 16 Glossar

AAA

System von einem oder mehreren Servern, das für die Zugangskontrolle zum Netzwerk die Funktionen Authentication, Authorisation und Accounting (Authentifizierung, Autorisierung und Abrechnung) realisiert. Die Kommunikation mit einem AAA-System geschieht typischerweise über das Protokoll RADIUS. Umgangssprachlich werden daher oft RADIUS-Server und AAA-Systeme gleich gesetzt.

Access Point

Funkfeststation für den Client-Zugang in WLAN

Ad-hoc-Modus

Direkte Kommunikation zwischen Endgeräten über ein WLAN (also ohne Access Point)

Assoziation

Anmeldevorgang eines Clients an einem Access Point

Authentifizierung

Verifizierung der Identität einer Instanz, z. B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentifizierung ist i.A. keine sinnvolle Autorisierung möglich.

Authentication Server

Derjenige Server, der die vom Benutzer übermittelten Authentifizierungsdaten verifiziert. Im Fall von RADIUS ist dies ein RADIUS-Server.

Authenticator

Derjenige Server, der die vom Benutzer übermittelten Authentifizierungsdaten an einen Authentication Server weiterleitet. Im Falle von RADIUS ist dies ein RADIUS-Client.

BSS

Basic Service Set. Bezeichnet die durch einen Access Point aufgespannte Funkzelle.

Beacon Frame

Zyklisch von einem Access Point übertragenes Paket. Dient der Information für WLAN-Clients und enthält Daten zu Übertragungsparametern und optional den SSID.

Certificate Authority

Zertifizierungsstelle. Diejenige Instanz einer PKI, die digitale Zertifikate (üblich ist der X.509v3-Standard) ausstellt und verwaltet.

Certificate Revocation List

Zertifikatssperrliste. Eine von einer Certificate Authority generierte Liste, in der alle Zertifikate aufgeführt werden, die innerhalb ihres Gültigkeitszeitraums manuell für ungültig erklärt wurden.

Cyclic Redundancy Code

Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance. Kanalzugriffsverfahren in WLAN, welches auf dem Prinzip der zufälligen Verzögerung des Sendeversuchs und des Abhörens des Funk-

kanals vor einer Übertragung basiert. Erlaubt mehreren Stationen die simultane Nutzung des Shared Medium Funk mit einem vergleichsweise geringen Kollisionsrisiko.

Denial of Service

Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke

Eine Wörterbuch-Attacke, die typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt wird. Bei kryptografischen Schwächen eines Verschlüsselungsverfahrens oder bei schwachen Passwörtern geringer Komplexität kann durch geschicktes Raten der Suchraum erheblich verkleinert werden und das Verfahren kann schnell zum Erfolg führen.

Distribution System

Netzwerk, das Access Points untereinander und mit der weiteren Infrastruktur verbindet. Kann als physikalisch separates LAN oder als VLAN in einer bestehenden LAN-Infrastruktur realisiert werden.

DMZ

Demilitarisierte Zone. Bezeichnet eine Sicherheitszone, die typischerweise zwischen geschütztem (internen) Netz und externem Netz (z. B. Internet) eingefügt wird. Für diese Sicherheitszone gilt meist, dass in einem festgelegten Rahmen (d. h. kontrolliert durch eine Firewall) ein Zugriff aus dem externen Netz gestattet wird (öffentlich erreichbarer Bereich der IT-Infrastruktur).

DSSS

Direct Sequence Spread Spectrum. Bandspreiztechnik, die eine Bandspreizung erreicht, indem das übertragene Signal durch Verknüpfung mit einer Code Sequenz in der Chiprate des Systems entsteht. Der Empfänger kann durch die Kenntnis dieses Codes das Signal auch aus einer Überlagerung mit Störungen wieder herausfiltern.

EAP

Das Extensible Authentication Protocol (EAP) ist ein Rahmen (Framework) für die Verwendung von Authentifizierungsmethoden. Es wird u. a. für PPP oder auch in Verbindung mit EAPOL unter IEEE 802.1X verwendet.

EAPOL

EAP over LAN (EAPOL) ist ein Verfahren zur Verwendung von EAP auf Layer 2 über Lokale Netzwerke (LANs) wie z. B. IEEE 802.3 („Ethernet“).

ESS

Extended Service Set. Gesamtheit der Funkzellen eines WLAN.

Funkzelle

Geographischer Bereich um einen Sender (z. B. Access Point) herum, in dem ein genügend guter Empfang besteht. Was als „genügend gut“ zu bezeichnen ist und was nicht, ist Festlegungssache. Die Empfangsqualität in einem WLAN hängt unter anderem vom verwendeten Übertragungsstandard, von der Qualität der Hochfrequenz-Hardware in den Geräten und von der Charakteristik der Antennen ab. Die Ausdehnung einer Funkzelle wird weiterhin durch den verwendeten Frequenzbereich, die Sendeleistung und insbesondere durch die jeweiligen Umgebungsbedingungen (z. B. Material von Wänden, Türen, Fenstern und Decken) beeinflusst.

Handover

Wechsel von einem (physikalischen) Kommunikationskanal auf einen anderen unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung. Beispiel: Bei einem Telefonat über VoIP over WLAN darf bei einem (mobilitätsbedingten) Wechsel von einer Funkzelle in eine andere das Gespräch nicht signifikant gestört werden oder sogar abreißen.

Hotspot

Öffentlich zugänglicher Internet-Zugang über ein WLAN.

IEEE 802.11

WLAN-Standard des IEEE, der sich international durchgesetzt hat und inzwischen meist mit dem Begriff WLAN gleichgesetzt

IEEE 802.1X

Standard des IEEE zur portbasierten Netzwerkzugangskontrolle unter Verwendung von EAP. Findet auch Anwendung unter IEEE 802.11i zur Absicherung von WLANs.

Infrastruktur-Modus

In diesem Modus kommunizieren WLAN-Clients stets über einen Access Point. Dies gilt auch, wenn zwei Clients in einer Funkzelle miteinander kommunizieren.

Kerberos

In den 80er Jahren entwickeltes Authentifizierungsprotokoll; u. a. Standard in Windows 2000 und Windows 2003 (RFC 1510).

Man in the Middle

Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

PPP

Point to Point Protocol. Protokoll zur Übertragung von IP-Paketen über Punkt-zu-Punkt-Verbindungen (insbesondere Modemstrecken). Beinhaltet auch die Prozeduren für den Aufbau der Kommunikationsbeziehung, etwa die Authentifizierung mit PAP oder CHAP.

RADIUS Server

Ein RADIUS Server kommuniziert über das Protokoll RADIUS mit einem RADIUS-Client zum Zwecke der Authentifizierung, der Autorisierung und/oder des Accounting (AAA). Der RADIUS-Server nimmt die AAA-Funktionen selbst oder in Zusammenarbeit mit weiteren Diensten/Geräten wahr und gibt AAA-Informationen an den Client zurück.

Roaming

Möglichkeit eines Teilnehmers, sich in einem fremden Netz unter Nutzung der Authentifizierungsmittel seines Heimatnetzes zu registrieren und im fremden Netz unter Beibehaltung seiner Identität Kommunikationsdienste zu nutzen. Roaming in WLAN bedeutet immer den Wechsel von einem IP-Subnetz in ein anderes. Damit verbunden ist zumindest die Vergabe einer neuen IP-Adresse. Da ein WLAN nur Layer 1 und Layer 2 festlegt, findet Roaming außerhalb des WLAN statt. Roaming bedeutet also nicht, dass Kommunikationsbeziehungen beim Wechsel erhalten bleiben müssen, sondern lediglich, dass die Möglichkeit zur Kommunikation erhalten bleibt. Der Begriff Roaming wird oft mit dem Begriff Handover verwechselt.

Shared Secret

„Gemeinsames Geheimnis“. In der Praxis oftmals die einfachste Form, eine gesicherte Kommunikationsbeziehung zu etablieren, indem das gemeinsame Geheimnis für kryptografische Operati-

onen auf beiden Seiten benutzt wird, z. B. als symmetrischer Schlüssel zur Verschlüsselung der zu übertragenden Daten

SSID

Service Set Identifier. Durch den Netzadministrator vergebener Name des WLAN. Wird bei der Anmeldeprozedur und optional zyklisch in Beacon Frames übertragen.

Supplicant

Die Komponente eines Geräts (Clients), die sich über IEEE 802.1X an einem Port authentifiziert, wird als Supplicant bezeichnet.

VLAN

Logisches LAN, gebildet aus einer Gruppe von Stationen.

VLAN-ID

11 Bit lange VLAN-Nummer (Tag). Werden mehrere VLAN auf einem physikalischen Medium übertragen, werden die Pakete durch Kennzeichnung mit der VLAN-ID den verschiedenen VLAN zugeordnet. Diesen Vorgang bezeichnet man auch als VLAN-Tagging.

Wi-Fi

Wireless Fidelity. Gütesiegel der Wi-Fi Alliance. Bestätigt, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat (z. B. WPA). Die Wi-Fi Alliance ist ein Herstellerkonsortium, das basierend auf IEEE 802.11 mit Wi-Fi einen Industriestandard geschaffen hat.

Zelle

Siehe Funkzelle

Zertifikat

Von einer Certificate Authority beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist.

# 17 Literatur


[ArHa04] J. Arkko, H. Haverinen, “Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)”, Internet Draft, IETF, Dezember 2004 http://www.ietf.org

[ASW01] W. A. Arbaugh, N. Shankar, Y.C. J. Wan, “Your 802.11 Wireless Network has No Clothes”, University of Maryland, März 2001.
Verfügbar unter http://www.drizzle.com/~aboba/IEEE/

[BSI04] Bundesamt für Sicherheit in der Informationstechnik, „BSI für Bürger, Sicheres Internet“, http://www.bsi-fuer-buerger.de/

[CHAP96] RFC 1994, “PPP Challenge Handshake Authentication Protocol (CHAP)”, IETF, August 1996,
http://www.ietf.org/rfc/rfc1994.txt

[CMS05] N. Cam-Winget, D. McGrew, S. Salowey, H. Zhou, “EAP Flexible Authentication via Secure Tunneling (EAP-FAST)”, Internet Draft, IETF, April 2005.
http://www.ietf.org

[DaRi99] J. Daemen, V. Rijmen, “AES Proposal: Rijndael”, 1999.

[DIR00] X.509, “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks“, ITU, März 2000.

[EAP04] RFC 3748, “Extensible Authentication Protocol (EAP)”, IETF, Juni 2004,
http://www.ietf.org/rfc/rfc3748.txt

[EAP05] D. Stanley, J. Walker, B. Aboba, “EAP Method Requirements for Wireless LANs”, IETF, August 2004,
http://www.ietf.org/rfc/rfc4017.txt

[ETSI03] ETSI EN 301 893, “Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive”, V1.2.3, August 2003. Verfügbar unter http://www.etsi.org

[FBW04] P. Funk, S. Blake-Wilson, “EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0)”, Internet Draft, IETF, Februar 2005, http://www.ietf.org

[FMS01] S. Fluhrer, I. Mantin, A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4“. Verfügbar unter http://www.drizzle.com/~aboba/IEEE/

[Gri01] R. A. Grimes, “Malicious Mobile Code”, O’Reilly, 2001.

[GSHB04] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen“, 2004 (jährlich neu). Verfügbar unter
http://www.bsi.bund.de/gshb

[HaSa04] H. Haverinen, J. Salowey, “Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)”, Internet Draft, IETF, Dezember 2004,
http://www.ietf.org

[IEEE99] ANSI/IEEE Std 802.11, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, 1999.

[IEEE99a] IEEE Std 802.11a, „High-speed Physical Layer in the 5 GHz Band“, 1999.

[IEEE99b] IEEE Std 802.11b, „Higher-Speed Physical Layer Extension in the 2.4 GHz Band“, 1999.

[IEEE03F] IEEE Std 802.11F, “IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation”, Juni 2003.

[IEEE03g] IEEE Std 802.11g, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band”, Juni 2003.

[IEEE03h] IEEE Std 802.11h, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe”, September 2003.

[IEEE04a] IEEE Std 802.11i, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Method Control (MAC) Security Enhancements”, Juni 2004.

[IEEE04b] IEEE Std 802.1X, “Port-Based Network Access Control”, Dezember 2004 (Revision der ersten Auflage des Standards von 2001).

[IEEE04c] IEEE Std 802.16, “Part 16: Air Interface for Fixed Broadband Wireless Systems”, Juni 2004.

[IPSec98a] RFC 2401, “Security Architecture for the Internet Protocol”, IETF, November 1998, http://www.ietf.org/rfc/rfc2401.txt

[IPSec98b] RFC 2402, “IP Authentication Header”, IETF, November 1998, http://www.ietf.org/rfc/rfc2402.txt

[IPSec98c] RFC 2406, “IP Encapsulating Security Payload (ESP)”, IETF, November 1998, http://www.ietf.org/rfc/rfc2406.txt

[IPSec98d] RFC 2408, “Internet Security Association and Key Management Protocol (ISAKMP)”, IETF, November 1998, http://www.ietf.org/rfc/rfc2408.txt

[IPSec98e] RFC 2409, “The Internet Key Exchange (IKE)”, IETF, November 1998, http://www.ietf.org/rfc/rfc2409.txt

[KaPa04] V. Kamath, A. Palekar, “Microsoft EAP CHAP Extensions“, Internet Draft, IETF, April 2004, http://www.ietf.org

[L2TP99] RFC 2661, “Layer Two Tunneling Protocol "L2TP"”, IETF, August 1999, http://www.ietf.org/rfc/rfc2661.txt

[L2TP01] RFC 3193, „Securing L2TP using Ipsec”, IETF, November 2001, http://www.ietf.org/rfc/rfc3193.txt

[LEAP04] “Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability”, Revision 2.1, Juli 2004, http://www.cisco.com

[Mac01] C. Macnally, “Cisco LEAP protocol description”, September 2001 http://www.missl.cs.umd.edu/wireless/ethereal/leap.txt

[MiAr02] A. Mishra, W. A. Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard”, Februar 2002.

[MIP02] RFC 3344, “IP Mobility Support for IPv4”, IETF, 2002, http://www.ietf.org/rfc/rfc3344.txt

[MRA99] RFC 2548, “Microsoft Vendor-specific RADIUS Attributes”, IETF, März 1999, http://www.ietf.org/rfc/rfc2548.txt

[MSCH00] RFC 2759, “Microsoft PPP CHAP Extensions, Version 2”, IETF, Januar 2000, http://www.ietf.org/rfc/rfc2759.txt

[MSKB03] MS Knowledge Base Article – 309408.

[OTP97] RFC 2243, “OTP Extended Responses”, IETF, November 1997, http://www.ietf.org/rfc/rfc2243.txt

[OTP98] RFC 2289, “A One-Time Password System”, IETF, Februar 1998, http://www.ietf.org/rfc/rfc2289.txt

[PAP92] RFC 1334, “PPP Authentication Protocols”, IETF, Oktober 1992, http://www.ietf.org/rfc/rfc1334.txt

[PPTP99] RFC 2637, “Point-to-Point Tunneling Protocol (PPTP)”, IETF, Juli 1999, http://www.ietf.org/rfc/rfc2637.txt

[PSS04] A. Palekar, D. Simon, J. Salowey, et. al., “Protected EAP Protocol (PEAP) Version 2”, Internet Draft, IETF, Oktober2004, http://www.ietf.org

[RADI00a] RFC 2865, “Remote Authentication Dial In User Service (RADIUS)”, IETF, Juni 2000, http://www.ietf.org/rfc/rfc2865.txt

[RADI00b] RFC 2869, “RADIUS Extensions”, IETF, Juni 2000, http://www.ietf.org/rfc/rfc2869.txt

[RADI00c] RFC 2866, “RADIUS Accounting”, IETF, Juni 2000, http://www.ietf.org/rfc/rfc2866.txt

[RADI03a] RFC 3579, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”, IETF, September 2003, http://www.ietf.org/rfc/rfc3579.txt

[RADI03b] RFC 3576, “Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)”, IETF, Juli 2003, http://www.ietf.org/rfc/rfc3576.txt

[RSA99] RSA Laboratories, “PKCS #5 v2.0: Password-Based Cryptography Standard”, März 1999, http://www.rsasecurity.com/rsalabs/node.asp?id=2127

[SMW99] B. Schneier, Mudge, D. Wagner, „Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)”, Secure Networking - CQRE (Secure) '99, Series: Lecture Notes in Computer Science, Vol. 1740, Springer, 1999.

[SNMP90] RFC 1157, “A Simple Network Management Protocol (SNMP)”, IETF, Mai 1990, http://www.ietf.org/rfc/rfc1157.txt

[SPHINXa] Projekt SPHINX, http://www.bsi.bund.de/aufgaben/projekte/sphinx/index.htm

[SPHINXb] Struktur der Verwaltungs-PKI, http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/struktur.htm

[SPHINXc] European Bridge-CA, http://www.bsi.bund.de/aufgaben/projekte/sphinx/bridge.htm

[TLS99] RFC 2716, “PPP EAP TLS Authentication Protocol”, IETF, 1999, http://www.ietf.org/rfc/rfc2716.txt

[TKG04] „Telekommunikationsgesetz (TKG)“, Bundesgesetzblatt Jahrgang 2004 Teil I Nr. 29, Juni 2004.

[WPA04] Wi-Fi Alliance, “Wi-Fi Protected Access (WPA)”, Version 2.0, April 2003, http://www.wi-fi.org

# 18 Abkürzungen

| | |
|---|---|
| 3DES | Triple DES |
| 3GPP | 3rd Generation Partnership Project |
| AAA | Authentication, Authorization and Accounting |
| ACK | Acknowledge |
| ACL | Access Control List |
| AD | Active Directory |
| AES | Advanced Encryption Standard |
| AH | Authentication Header |
| AKA | Authentication and Key Agreement |
| AP | Access Point |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| AS | Authentication Server |
| AuC | Authentication Center |
| BAP | Bandwidth Allocation Protocol |
| BIOS | Basic Input/Output System |
| BSD | Berkeley Software Distribution |
| BSS | Basic Service Set |
| CA | Certificate Authority |
| CBC-MAC | Cipher Block Chaining Message Authentication Code |
| CCMP | Counter mode with CBC-MAC Protocol |
| CHAP | Challenge Handshake Authentication Protocol |
| CIFS | Common Internet File System |
| CN | Corresponding Node |
| COA | Care of Address |
| CRC | Cyclic Redundancy Code |
| CRL | Certificate Revocation List |
| CSMA/CA | Carrier Sense Multiple Access with Collision Avoidance |
| CSP | Crytographic Service Provider |
| CTR | Counter Mode |
| DAT | Dynamic Address Translation |
| DECT | Digital Enhanced Cordless Telecommunications |
| DES | Data Encryption Standard |
| DFS | Dynamic Frequency Selection |
| DH | Diffie-Hellman |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | De-Militarized Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DS | Distribution System |
| DSSS | Direct Sequence Spread Spectrum |
| EAP | Extensible Authentication Protocol |

| | |
|---|---|
| EAPOL | EAP over LAN |
| EFS | Encrypting File System |
| EK | Encryption Key |
| ESP | Encapsulating Security Payload |
| ESS | Extended Service Set |
| ETSI | European Telecommunications Standards Institute |
| FA | Foreign Agent |
| FAST | Flexible Authentication via Secure Tunneling |
| FCC | Federal Communications Commission |
| FCS | Frame Check Sequence |
| FHSS | Frequency Hopping Spread Spectrum |
| FQDN | Fully Qualified Domain Name |
| FTP | File Transfer Protocol |
| FW | Firewall |
| GMK | Group Master Key |
| GPO | Group Policy Object |
| GPS | Global Positioning System |
| GRE | Generic Routing Encapsulation |
| GSM | Global System for Mobile Communications |
| GTC | Generic Token Card |
| GTK | Group Transient Key |
| GW | Gateway |
| HA | Home Agent |
| HLR | Home Location Register |
| HMAC | Hashed Message Authentication Code |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | HTTP Secure |
| IANA | Internet Assigned Numbers Authority |
| IAPP | Inter Access Point Protocol |
| IBSS | Independent BSS |
| ICC | Integrated Circuit Cards |
| ICF | Internet Connection Firewall |
| ICMP | Internet Control Message Protocol |
| ICV | Integrity Check Value |
| IDEA | International Data Encryption Algorithm |
| IDS | Intrusion Detection System |
| IE | Information Element |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPSec | IP Security |
| ISAKMP | Internet Security Association and Key Management Protocol |

| | |
|---|---|
| ISDN | Integrated Services Digital Network |
| ISM | Industrial, Scientific and Medical |
| ISP | Internet Service Provider |
| IT | Information Technology |
| IV | Initialisierungsvektor |
| L2TP | Layer-2-Tunneling Protocol |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LEAP | Lightweight EAP |
| MAC | Medium Access Control |
| MD4 | Message Digest 4 |
| MD5 | Message Digest 5 |
| MDA | Mobile Digital Assistant |
| MIB | Management Information Base |
| MIC | Message Integrity Check |
| MitM | Man in the Middle |
| MK | MIC Key |
| MN | Mobile Node |
| MPPE | Microsoft Point-to-Point Encryption |
| MS | Microsoft |
| MSCHAP | Microsoft Challenge Handshake Authentication Protocol |
| MSDU | MAC Service Data Unit |
| MSISDN | Mobile Station ISDN |
| MSK | Master Session Key |
| NAPT | Network Address and Port Translation |
| NAS | Network Access Server |
| NAT | Network Address Translation |
| NDAP | Novell Directory Access Protocol |
| NT | New Technology |
| NTFS | New Technology File System |
| NTLM | NT LanManager |
| OCSP | Online Certificate Status Protocol |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OTP | One-Time Password |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| OWA | Outlook Web Access |
| PAC | Protected Access Credential |
| PAE | Port Access Entity |
| PAP | Password Authentication Protocol |
| PDA | Personal Digital Assistant |
| PEAP | Protected EAP |
| PF | Personal Firewall |

| | |
|---|---|
| PIN | Personal Identification Number |
| PKCS | Public-Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| PMK | Pairwise Master Key |
| PPP | Point to Point Protocol |
| PPTP | Point to Point Tunneling Protocol |
| PSK | pre-shared Key |
| PTK | Pairwise Transient Key |
| PRF | Pseudo-Random Function |
| QoS | Quality of Service |
| RA | Registration Authority |
| RADIUS | Remote Authentication Dial-in User Service |
| RAS | Remote Access Service |
| RC4 | Ron's Code 4 |
| RDP | Remote Desktop Protocol |
| RegTP | Regulierungsbehörde für Telekommunikation und Post |
| RFC | Request for Comments |
| RSA | Rivest, Shamir, Adleman |
| RSN | Robust Security Network |
| SA | Security Association |
| SHA-1 | Secure Hash Algorithm 1 |
| SIM | Subscriber Identity Module |
| SMB | Server Message Block |
| SMS | Short Message Service |
| SMSC | Short Message Service Center |
| SNMP | Simple Network Management Protocol |
| SOCKS | Sockets |
| SOHO | Small Office / Home Office |
| SPF | Stateful Packet Filtering |
| SPI | Stateful Packet Inspection |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| TFTP | Trivial FTP |
| TK | Temporal Key |
| TKG | Telekommunikationsgesetz |
| TKIP | Temporal Key Integrity Protocol |
| TLS | Transport Layer Security |
| TPC | Transmit Power Control |
| TTLS | Tunneled TLS |
| UDP | User Datagram Protocol |
| UMTS | Universal Mobile Telecommunications System |
| URL | Uniform Resource Locator |

| | |
|---|---|
| USB | Universal Serial Bus |
| USIM | Universal Subscriber Identity Module |
| VLAN | Virtual LAN |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |
| WAN | Wide Area Network |
| WEP | Wired Equivalent Privacy |
| WiMAX | Worldwide Interoperability for Microwave Access |
| Wi-Fi | Wireless Fidelity |
| WISP | Wireless ISP |
| WLAN | Wireless LAN |
| WPA | Wi-Fi Protected Access |
| XOR | Exclusive OR |

# 19 Index

# 20 Abbildungsverzeichnis

# 21 Tabellenverzeichnis