WLAN-Sicherheit – von WEP bis CCMP

Dr. Kai-Oliver Detken[1], Prof. Dr. Evren Eren[2]

[1]DECOIT GmbH, Fahrenheitstraße 1, D-28359 Bremen
detken@decoit.de

[2]FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund
eren@fh-dortmund.de

Zusammenfassung

Dieser Beitrag behandelt das Thema WLAN Security. Hierzu wird zunächst die State-of-the-Art der WLAN-Technologien mit ihren verschiedenen Ausprägungen kurz wiedergegeben. Als Hauptbestandteils dieses Artikels wird ein breites Spektrum an gängigen und speziellen WLAN-Sicherheitsmechanismen und -Verfahren behandelt. Dieses umfasst WEP, dynamisches WEP, WPA-Varianten (WPA-PSK, WPA-RADIUS, WPA2), 802.1X, EAP, TKIP, Robust Secure Networks (802.11i) und CCMP. Diese werden bzgl. ihrer Schwachstellen und Verwundbarkeiten untersucht und verglichen. Der Artikel endet mit einer Gesamtbewertung, die als Grundlage für das Verständnis von Abwehrmaßnahmen und Schutzkonzepten dienen soll. Vorrangiges Ziel dabei ist es, das Verständnis zu vermitteln, das komplementäre und integrierte Sicherheitskonzepte, -strategien und -lösungen notwendig sind, um WLAN-Technologien im Unternehmen sicher einsetzen zu können.

1 Hintergrund und Problemstellung

Obgleich das Thema IT-Sicherheit bereits seit Jahren eine hohe Sensibilisierung sowohl im privaten Bereich als auch bei Unternehmen unterschiedlichster Größenordnung erfahren hat, sind Anwender relativ verhalten, wenn es um den Einsatz von mobilen Sicherheitsverfahren und -lösungen geht. Dieser Sachverhalt verwundert, da im klassischen IT-Sicherheitsbereich mittlerweile ausreichend Erfahrungen vorliegen sollten, um ähnliche Fehler und zögerliche Haltung zu wiederholen. Ungesicherte WLAN-Verbindungen bzw. Konfigurationen öffnen Türen und Tore für Angreifer und kompromittieren die Integrität von vertraulichen Daten.

Mobile Endgeräte mit WLAN-Connectivity werden relativ unsicher betrieben und sind damit einem höheren Angriffspotenzial ausgesetzt als Computer in Büroumgebungen. Unkontrollierte private Nutzung der mobilen Geräte (z.B. Downloads, E-Mails) sowie der Verzicht auf die notwendigen Sicherheitsvorkehrungen, verwandeln diese einfach und schnell zu gefährlichen Hintertüren, in die sonst gewissenhaft geschützte IT-Umgebung.

Die Verbreitung von Sicherheitsrisiken und Angriffspotenzialen löst keine ausreichende Besorgnis und entsprechendes Handeln bei Heimanwendern, Unternehmen und Organisationen aus. Man kann festhalten, dass der Grad der Sensibilisierung für das Thema WLAN Security de facto nicht ausreichend vorhanden ist und bei den Wenigen, die dieses thematisieren, sind strategische und technische Maßnahmen zur Eliminierung bzw. Reduktion von mobilen Sicherheitsrisiken nicht nachhaltig erkennbar. Wesentliche Hemmfaktoren für viele Unternehmen sind Unsicherheit oder fehlendes Wissen. Es wird sogar die Meinung vertreten, dass mo-

bile Sicherheit durch allgemeine IT-Sicherheitslösungen automatisch mit abgebildet wird oder bereits ausreichend in WLAN-Produkten und Betriebsystemen vorhanden ist.

1.1 WLAN-Technologien

Wireless LANs (WLAN) basieren auf dem definierten Standard IEEE 802.11, welcher 1997 spezifiziert wurde. Durch WLANs wird die Möglichkeit geboten, mit geringem Aufwand und auf sehr flexibler Basis drahtlose lokale Netzwerke aufzubauen. In den meisten Fällen wird es als Erweiterung des bestehenden Festnetzes gesehen; es kann aber auch als Alternative zu Festinstallationen eingesetzt werden. In den letzten Jahren sind WLANs in verschiedenen Bereichen immer populärer geworden, insbesondere in der Medizin (Krankenhäuser), dem Verkauf, der Herstellung und der Forschung. Allerdings ist die Sicherheit in der Vergangenheit immer mehr in Verruf geraten. Da aber WLANs in sehr sensiblen Umgebungen eingesetzt werden, sollte gerade die Sicherheit kontinuierlich hinterfragt werden.

Bei den WLAN-Basistechnologien lassen sich zwei Hauptgruppen nach dem verwendeten Frequenzband unterscheiden: Die einen arbeiten im klassischen 2,4-GHz-Band, die anderen im 5-GHz-Band. Zu Ersteren gehören das bislang verwendete IEEE 802.11b mit 11 MBit/s brutto sowie sein rückwärtskompatibler dezidierter Nachfolger 802.11g, für den Mitte Juni 2003 der Standard verabschiedet wurde. Im 5-GHz-Band operieren dagegen 802.11a und 802.11h mit jeweils einer Datenrate von 54 MBit/s brutto. Dabei stellt der Standard 802.11h lediglich die europäische Variante des amerikanischen 802.11a-Standards dar: Es bietet mit dynamischer Frequenzauswahl und variabler Sendeleistung zwei Zusatzmerkmale, die die ETSI für den europäischen Markt verlangt.

Tab. 1: Auswahl diverser WLAN-Standards

Standard	Beschreibung
802.11a	54 MBit/s WLAN im 5-GHz-Band
802.11b	11 MBit/s WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging
802.11d	World Mode, Anpassung an regionsspezifische Regulatoren
802.11e	Quality-of-Service (QoS) und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h mit dem Inter Access Point Protocol (IAPP)
802.11g	54 MBit/s WLAN im 2,4-GHz-Band
802.11h	54 MBit/s WLAN im 5-GHz-Band mit Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC)
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES und 802.1X)

Inzwischen wurden einige ergänzende Standards festgelegt, wie IEEE 802.11c. Dieser Standard behandelt die Verfahren für Wireless Bridging, also die drahtlose Kopplung verschiedener Netzwerktopologien. Als „World Mode“ regelt der Standard 802.11d die regionsspezifische technische Unterschiede, etwa wie viele und welche Kanäle welche der Basistechnologien a/h/b/g in welchem Land verwenden dürfen. Der Anwender muss lediglich das Land angeben, in dem er seine WLAN-Karte gerade benutzt; der Treiber regelt dann die entsprechende Anpassung. IEEE 802.11e definiert QoS- und Streaming-Erweiterungen, um die 54 MBit/s schnellen Netze für Multimedia-Applikationen und vor allem für Voice-over-IP (VoIP) vorzubereiten. Um dazu notwendige Merkmale wie garantierte Datenraten oder minimale Lauf-

zeitschwankungen sicherzustellen, muss aber noch am MAC-Layer nachgearbeitet werden. Mit standardisierten Verfahren zum Roaming mobiler Clients zwischen Access Points (vor allem solcher verschiedener Hersteller!) beschäftigt sich 802.11f. Die Abstimmung der Übergabe erfolgt dabei über das Inter Access Point Protocol (IAPP).

1.2 Allgemeine Sicherheitslücken in WLANs

Die aktuellen standardkonformen WLAN-Systeme bergen bzgl. der Sicherheit große Schwachstellen, die aktive wie passive Angriffe erlauben und damit zu einem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen können. Zudem sind WLAN-Komponenten im Auslieferungszustand oftmals so konfiguriert, dass keine oder nur einige der Sicherheitsmechanismen aktiviert sind.

Folgende allgemeine Sicherheitslücken lassen sich nennen:

- **SSID Broadcast:** Einige APs bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das WLAN vor Unbefugten zu verstecken (so genanntes „Closed System“). Dieser Schutz wirkt gegen diverse frei verfügbare Tools wie z.B. Netstumbler. Jedoch kann mittels WLAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.
- **Manipulierbare MAC-Adresse:** Jede Netzwerkkarte verfügt über eine eindeutige Hardwareadresse, die sog. MAC-Adresse (Media Access Control). Diese MAC-Adressen der WLAN-Clients können relativ einfach abgehört und manipuliert werden. Somit sind die in den APs zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar.
- **Fehlendes Schlüsselmanagement:** Schlüssel müssen in einem WLAN „von Hand“ verteilt werden, d.h. in jedem WLAN Adapter (Client) und im AP muss der gleiche statische Schlüssel eingetragen werden. Dies erfordert physischen Zugriff auf die Komponenten. Diese Art des „Schlüsselmanagements“ führt in der Praxis oft dazu, dass der geheime Schlüssel sehr selten oder überhaupt nicht gewechselt wird. Die Offenbarung eines Schlüssels, z.B. durch Verlust eines Clients oder mittels frei verfügbarer Tools, kompromittiert das gesamte WLAN. Der gemeinsame geheime Schlüssel eines WLAN-Clients wird, je nach Hersteller, entweder auf der WLAN-Karte oder auf der Festplatte des Client-Rechners gespeichert. Einige Hersteller schreiben diese Informationen sogar offen in die Registry-Datei eines Windows-Betriebssystems!
- **Bedrohung der lokalen Daten:** Auf den Client-Rechnern entstehen durch die Teilnahme eines Clients am WLAN zusätzliche Bedrohungen für die lokalen Daten. Lokale Datei- bzw. Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung meist auch über das WLAN Zugriffe auf diese Ressourcen. Ebenso sind bei eingeschaltetem WLAN Angriffe auf den Rechner zu befürchten, die Schwachstellen des verwendeten Betriebssystems ausnutzen. Diese Gefahren bestehen insbesondere bei der Nutzung von WLAN-Komponenten in öffentlichen Bereichen, in Hotspots und in Ad-hoc-Netzwerken.
- **Unkontrollierte Ausbreitung der Funkwellen:** Auch über die spezifizierte Reichweite von 10-150 Metern hinaus, breiten sich die Funkwellen der WLAN-Komponenten aus und können je nach Umgebungsbedingungen und der Leistungsfähigkeit der verwendeten Empfangsgeräte empfangen werden. Dies bedeutet, dass auch über die Nutzreichweite der WLANs hinaus eine konkrete Abhörgefahr besteht.

- **Bedrohung der Verfügbarkeit:** WLANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WLAN-Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z.B. Bluetooth-Geräte, andere WLANs, Mikrowellen etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-of-Service (DoS) Angriff erfolgen. Darüber hinaus sind DoS-Angriffe auch möglich durch wiederholtes Senden bestimmter Steuer- und Managementsignale.
- **Erstellung von Bewegungsprofilen:** Da die Hardwareadresse einer WLAN-Karte bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können Bewegungsprofile über mobile Nutzer, die sich in öffentliche Hotspots einbuchen, erstellt werden. Da die MAC-Adresse grundsätzlich unverschlüsselt übertragen wird, ist das Erstellen von Bewegungsprofilen keinesfalls nur den Betreibern der Hotspots möglich. Prinzipiell kann jeder, der an geeigneten öffentlichen Plätzen eine WLAN-Komponente installiert, die MAC-Adressen anderer Nutzer mitlesen. Sendet der Nutzer zusätzlich personenbezogene Daten unverschlüsselt über das Funknetz, können auch diese mitgelesen und mit dem Bewegungsprofil zusammengeführt werden.

2 Sicherheitsmechanismen und Verfahren für WLANs

An dieser Stelle werden die unterschiedlichen Sicherheitsverfahren für WLANs kurz behandelt und vorgestellt:

1. **Wired Equivalent Privacy (WEP):** WEP basiert auf dem symmetrischen RC4-Algorithmus, bei dem folglich ein gemeinsamer Schlüssel (der sog. WEP-Key) zum Einsatz kommt. RC4 ist ein Stromverschlüsselungsalgorithmus, der den Klartext über XOR-Funktion mit einer Folge von Pseudo-Zufallszahlen verknüpft. Der Algorithmus wird, zusammen mit einem zufällig festgelegten Initialisierungsvektor (IV), in den RC4-Zufallszahlengenerator eingegeben. In diesem Generator kommt der Key Scheduling Algorithm (KSA) zum Einsatz, der entweder mit 40 Bit (WEP64) oder 104 Bit langen Schlüsseln (WEP128) arbeitet.
2. **Wi-Fi Protected Access (WPA):** WPA wurde durch die Wi-Fi-Allianz etwas später als 802.1X eingeführt und beruht auf dem dritten Draft von 802.11i. WPA benutzt folgende Mechanismen: 802.1X mit einer der Standard-EAP-Methoden zur Zugangssteuerung und Temporal Key Integrity Protocol (TKIP) für Vertraulichkeit und Datenintegrität. Um den Sicherheitsschwachstellen in WEP zu begegnen, implementiert WPA dynamische Schlüssel für jedes versendete Paket. Dabei besitzt jeder Benutzer einen eigenen Schlüssel. Um die dynamischen Schlüssel zu generieren, nutzt WPA das TKIP. Um die Verschlüsselungssicherheit zu erhöhen und um Angriffe zu erschweren, setzt WPA auf 48 Bit lange Initialisierungsvektoren (IV). Diese waren bei WEP nur 24 Bit lang. Um die Integrität von Paketen zu sichern, setzt WPA zusätzlich zu dem Integrity Check Value (ICV) des 802.11-Standards noch den Message Integrity Check (MIC), der auch „Michael“ genannt wird, ein. Für die Authentisierung der Benutzer stehen in WPA zwei verschiedene Modi zur Verfügung: WPA Personal (WPA-PSK) und WPA Enterprise

(WPA RADIUS). WPA-PSK[1] ist die einfachste Variante von WPA und ist für den Heimbetrieb ausgelegt, also für Anwender, die keine 802.1X -Infrastruktur besitzen. Deshalb wird dieses Verfahren auch als SOHO-Mode bezeichnet. PSK steht für Pre-Shared-Keys. Diese müssen sowohl auf dem Access Point als auch auf den Clients eingetragen sein. Der Access Point übernimmt dann die Authentifizierung und das Key-Management ohne weitere zusätzliche Netzwerkkomponenten. Für den Betrieb von WPA-PSK werden lediglich eine Client WLAN-Karte und ein WPA-konformer Access Point benötigt.

3. **WPA2:** Im Frühjahr 2004 verabschiedete die Wi-Fi-Allianz WPA2 als vollständige Umsetzung des IEEE802.11i-Standards. Bei WPA2 wurde voll auf einen neuen Verschlüsselungsstandard gesetzt. Bei WEP und WPA mit TKIP kam noch der als unsicher geltende RC4-Algorithmus zum Einsatz. WPA2 dagegen nutzt das neuere Verfahren AES (Advanced Encryption Standard), bietet jedoch zur Wahrung der Abwärtskompatibilität zu WPA alternativ TKIP (und damit RC4) an.
4. **802.1X:** IEEE 802.1X wurde mit dem Ziel entwickelt, möglichst viele Sicherheitslücken aus 802.11 zu schließen wie fehlendes Schlüsselmanagement, fehlende Benutzeridentifikation, und -Authentisierung, insbesondere erweiterte Authentisierungsmethoden (Token, SmartCards, Zertifikaten, One-time-Passwörtern, etc.) und die fehlende Möglichkeit einer zentralen Authentisierung und Autorisierung. In 802.1X kommt eine Port-basierte Authentisierung zum Tragen. Um den Sicherheitsansprüchen in Funknetzen gerecht zu werden, wurde das Extensible Authentication Protocol (EAP) entwickelt und soll im Zusammenspiel mit einem Authentisierungsserver das Sicherheitsniveau erhöhen. 802.1X basiert auf EAP. Es wurde schnell erkannt, dass 802.1X auch für 802.11b-Netzwerke angewandt werden kann. Ein Port bei 802.1X ist die Zugangsschnittstelle für den Client, also eine Einheit, die zwei verschiedene Netze miteinander verbindet. Am Beispiel von WLANs ist ein Access Point ein Port im Sinne von IEEE 802.1X. Ein Benutzer muss sich authentisieren, um Zugang ins Funknetz zu bekommen. Im Kontext mit EAP kann 802.1X als ein Protokoll aufgefasst werden, das EAP über drahtgebundene und drahtlose Netze kommunizieren lässt.
5. **Extensible Authentication Protocol (EAP):** EAP nach RFC-2284 stellt eine grundlegende Basis für eine umfassende und zentralisierte Sicherheitskonzeption dar. Es wurde ursprünglich für PPP-Verbindungen entwickelt, um eine zuverlässige Authentifizierung von Remote-Access-Usern bereitzustellen. EAP ist ein allgemeines Protokoll, das mehrere Authentifizierungsmöglichkeiten bietet. Von PPP ausgehend hat EAP mittlerweile auch Zugang in den im Jahr 2001 verabschiedeten IEEE802.1X gefunden, das die physische Übertragung auf LAN-Netzwerke anpasst. Die EAP-Nachrichten werden hierzu in 802.1X-Messages verpackt (EAP-over-LAN – EAPOL). Ziel dieses Standards ist die portbezogene Zugangskontrolle in Netzwerken (Port-Based Network Access Control).
6. **Temporal Key Integrity Protocol** (**TKIP**): Da die Sicherheitsmechanismen der Standards IEEE 802.11a und 802.11b nicht ausreichen, um Funknetze auch in sensiblen Bereichen zu nutzen, wurden diese Standards durch die Wireless Ethernet Compatibility Alliance (WECA) verbessert. Hierbei sollten die Schwachstellen eines konstanten WEP-Schlüssels sowie die fehlerhafte Integritätssicherung eliminiert werden. Aus Kompatibilitätsgründen wurde jedoch vom Verschlüsselungsalgorithmus RC4 nicht ab-

[1] identisch mit der Pre-Shared Key Authentisierung in 802.11i

gewichen. Da die Sicherheitsprobleme von WEP nicht an RC4 liegen, war dieses Konzept auch vertretbar. Durch die Kompatibilität können bestehende Verfahren aktualisiert werden. D.h. viele der bereits in Gebrauch befindlichen Karten und Access Points können TKIP mit neuen Treibern oder einem Firmware-Update nutzen.

7. **802.11i und Robust Security Network (RSN):** In 802.11i wird ein zweispuriger Ansatz verfolgt, um die Schwachstellen in der Verschlüsselung der Verbindungsschicht anzugehen. Dabei kommen zwei Verschlüsselungsprotokolle in der Verbindungsschicht als wesentliche Komponenten zum Tragen: Das Temporal Key Integrity Protocol (TKIP), was auch bei WPA eingesetzt wird, und das CBC-MAC Protocol (CCMP). Die Architektur von 802.11i wird von der IEEE Task Group i (TGi) Robust Security Network (RSN) genannt. Dies ist ein Satz von Prozeduren, die festlegen, wie Schlüssel abgeleitet und verteilt werden.

Vergleicht man IEEE 802.11i mit WPA2, dann fällt auf, dass beide bezüglich der verwendeten Protokolle und Verfahren ähnlich sind. 802.11i bietet einen geschützten Ad-hoc-Modus, Secure Fast Handoff und Pre-Authentication, sicheres De-Authentication and Disassociation sowie den Einsatz von sicheren Verschlüsselungsprotokollen auf Basis von AES-CTR und CCMP. 802.11i ist abwärtskompatibel zu WPA, sodass auf Aufrüsten der Merkmale über ein Firmware-Update möglich sind. Jedoch schließt dies nicht AES-CCMP ein. Neuere WLAN-Karten sind aber teilweise auf AES-CCMP vorbereitet. Wie bei WPA stützt sich 802.11i auf EAP, wobei lediglich die Varianten EAP-TLS, PEAP und EAP-TTLS (EAP Tunneled TLS Authentication Protocol) zu empfehlen sind. Ungleich zu TKIP, wird bei CCMP ein und derselbe Schlüssel zur Rahmenverschlüsselung als auch zur Integritätsprüfung benutzt. Dies reduziert den Rechenaufwand erheblich.

3 Sicherheitsbewertungen

Das Ziel mittels **WEP** Vertraulichkeit, Integrität und Authentizität im WLAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert; es existieren sogar frei verfügbare Tools für passive Angriffe. Die Schwachstellen von WEP kann man in zwei Kategorien einteilen: Schwachstellen im Protokoll und im RC4-Design.

Bei **WPA-PSK** besteht das Risiko von Wörterbuchattacken. Dies liegt daran, dass der Pre-Shared Master Key direkt aus der Passphrase und der SSID abgeleitet wird. In den meisten Fällen wird ein einziger Pre-Shared Key für alle Stationen einer SSID benutzt. Ein Angreifer kann den 4-Wege-Handshake beobachten und die Schlüssel ableiten, die denselben Pre-Shared Key teilen. Des Weiteren wäre ihm möglich, Nachrichten zu fälschen, die eine Re-Authentisierung herbeiführen um dann den 4-Wege-Handshake zu übernehmen. Auch die Passphrase ist ein Problem. Der Pre-Shared.Key wird in den meisten Implementierungen in Form einer Passphrase generiert. Die Qualität der Passphrase bestimmt die Sicherheit von WPA-PSK erheblich. Der Annex der Spezifikation 802.11i behandelt diesen Sachverhalt. Sehr kurze Passphrasen können durch Wörterbuchattacken kompromittiert werden.

IEEE 802.1X ist keine vollständige Spezifikation, sondern ein Rahmenwerk. Der Authentisierungsmechanismus erfordert einen Authentisierungsserver (AAA-Server). Änderungen der Authentisierungsmethode erfordern keine komplexen Änderungen im Client oder in der Netzwerkinfrastruktur. Folgende Stärken lassen sich nennen:

1. Client-Authentisierung: Ein Access Point gibt den Netzzugang erst dann frei, wenn der Benutzer sich gegenüber dem Authentifizierungsserver erfolgreich authentisiert hat.
2. Session-basierte Verschlüsselung mit dynamischen Schlüsseln: Durch die Kombination von 802.1X , EAP-TLS und RADIUS können pro Verbindung und Sitzung (Session) zwischen Client und Access Point die Daten verschlüsselt ausgetauscht werden. Dabei ist der Schlüssel pro Session dynamisch.
3. 802.1X kann zur sicheren Verteilung von sitzungs- und stationsbasiertem Schlüsselmaterial eingesetzt werden. Somit kann jeder Client einen eigenen und von den anderen unabhängigen Schlüssel zugestellt bekommen. Auch wenn es einem Angreifer gelingen sollte, einen Schlüssel zu kompromittieren, so beschränkt sich der Angriff auf die eine Sitzung oder einen Client.
4. Durch das Rekeying, also dem Schlüsselaustausch, werden Clients aufgefordert, Ihre Schlüssel zu aktualisieren, was periodisch erfolgen kann. Damit wird die Wahrscheinlichkeit von IV-Kollisionen drastisch gesenkt.
5. Mittels eines zentralisierten AAA-Mechanismus werden Benutzer einzeln identifiziert und authentisiert. Hierdurch ist auch Policy-basierter Netzwerkzugang einfach abzubilden.

Der Standard IEEE802.1X stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netzwerke dar. Dennoch gibt es folgende Einschränkungen

1. Client-Authentisierung: Zwar muss sich der Client gegenüber dem Access Point authentisieren, aber nicht umgekehrt. Aufgrund der fehlenden Überprüfung der Datenintegrität lassen sich nur der die Daten zwischen Client und Access Point, sondern auch Management-Pakete (Frames), für welche bei 802.11 kein Integritätsschutz und keine Authentifizierung existieren, kompromittieren.
2. Der 802.1X -Standard bietet nur einen geringen Schutz gegen unerwünschte Teilnehmer. Es sind zusätzliche Maßnahmen zur eindeutigen Identifizierung von WLAN-Teilnehmern sowie Vertraulichkeit der übertragenen Daten zu ergreifen.
3. Die IEEE802.1X sieht nur eine Authentifizierung des Clients vor, indem der Access Point den Verkehr über den kontrollierten Port erst nach der erfolgreichen Authentifizierung freigibt. Der Access Point selbst braucht seine Identität nicht nachzuweisen. Dies öffnet den Weg für Man-in-the-Middle-Attacks.
4. Es enthalten nach einer einmal erfolgten Authentifizierung die einzelnen Pakete keine Zuordnung mehr. Daher kann im Rahmen eines so genannten Session Hijacking ein Angriff erfolgen, indem eine andere Station dem erfolgreich authentifizierten Client eine Disassociate-Meldung sendet, die diesen zur Beendigung der Verbindung auffordert. Der Access-Point behält aber den kontrollierten Port weiterhin offen, sodass der Angreifer einen Zugang zum Netzwerk erhalten kann.

Auch der Einsatz einer **EAP-Variante** für WPA sollte genau auf die individuellen Bedarfe abgestimmt werden, da hier ein Trade-off zwischen Simplizität in der Anwendung und der Sicherheit gefunden werden muss. Die Modularität und Flexibilität von EAP in der Authentisierungsmethode birgt Gefahren, da der Anwender selbst entscheiden muss, welche der Methoden für ihn in Frage kommen und die von ihm gewünschte Sicherheit abbilden können.

Das reine EAP-Protokoll kann nicht als ausreichend sicher bezeichnet werden. Es überträgt die Nutzerdaten und Passwörter im Klartext und der Autorisierungsprozess findet unverschlüsselt statt. Auch wird keine Authentisierung des Authenticator gegenüber dem Suppli-

cant[2] gefordert. Ferner unterstützt es auch nicht die Erzeugung dynamischer Schlüssel für den WEP-Algorithmus. Aufgrund dieser genannten Einschränkungen wurden spezielle Erweiterungen, proprietäre und standardisierte, entwickelt. Sie bieten EAP-basierte Authentisierungsmethoden für 802.1X-Architekturen. Diese Authentisierungsmethoden bilden einen Satz von Regeln zur Authentisierung von Benutzern und Maschinen.

Es ist zu beachten, dass EAP-Methoden von Herstellern, entsprechend ihrer eigenen Interessen, unterschiedlich propagiert und vermarktet werden: LEAP von Cisco, PEAP von Microsoft, Cisco und RSA und EAP-TTLS von Funk Software und Certicom:

1. **EAP-MD5:** EAP-MD5 in WLANs ist nicht ausreichend robust, sodass von einem Einsatz ohne zusätzliche Sicherheitsmaßnahmen abgeraten wird. Im Vergleich zu den anderen vorgestellten EAP-Varianten ist EAP-MD5 die am einfachsten zu installierende, jedoch auch die mit der niedrigsten Sicherheitsstufe ausgestattete Methode. Es fehlt eine gegenseitige Authentisierung, sodass das Verfahren gegen Man-in-the-Middle-Attacks ungeschützt ist. Sitzungs- und Client-basierte Schlüssel fehlen gänzlich. Darüber hinaus fehlt bei EAP-MD5 auch die Authentisierung des Authentisierungsservers, sodass Man-in-the-Middle-Attacks möglich sind. Der Angreifer kann sich gegenüber dem Supplicant als RADIUS-Server und gegenüber diesem als Supplicant ausgeben und die Kommunikation nach Belieben manipulieren. Nachteilig ist auch der Sachverhalt, dass EAP-MD5 ein reines Authentisierungsprotokoll ist, d.h. die der Authentisierung nachfolgende Kommunikation ist unverschlüsselt.
2. **LEAP:** Auch Ciscos LEAP, was EAP-MD5 sehr ähnlich ist, birgt Risiken. LEAP kann dynamische WEP-Keys erzeugen. Es gelten aber die Schwächen von MS-CHAP, die Anfälligkeit für Wörterbuchangriffe. Zwischen Client und AP wird der Benutzername im Klartext übertragen, sodass eine Wörterbuchattacke möglich wäre. Das Passwort wird mittels MS-CHAP verschlüsselt. Abhilfe würde eine sinnvolle Anmelderichtlinie für das Netzwerk schaffen, beispielsweise über Active Directory und Netzwerkauthentisierung mittels Domänenbenutzerkonten. Hierdurch wären starke Passwörter über die Benutzerrichtlinie und Kontensperren durch entsprechende Kontensperrrichtlinien realisierbar. Obgleich für Netzwerke mit einer großen Zahl von Windows-Clients PEAP eine gute Wahl darstellt, da keine zusätzliche Software vonnöten, ist vom Einsatz abzuraten. Es ist prorietär und relativ schwach. Stattdessen sollte ein Protokoll auf Basis von TLS (EAP-TLS, PEAP und TTLS) eingesetzt werden, da es eine gegenseitige Authentisierung sowie Schlüsselverteilung unterstützt.
3. **EAP-TLS:** EAP-TLS basiert auf dem Austausch von Zertifikaten und ist ein sehr sicheres Verfahren, was jedoch mit einem hohen infrastrukturellen Aufwand verbunden ist. Unternehmen mit einer PKI können EAP-TLS sehr einfach einsetzen. Wird das Zertifikat des Authenticator auf einem sicheren Weg zum Supplicant übertragen, oder kann er es über eine Certification Authority überprüfen, so gilt diese Variante von EAP als sicher. In dieser Form wird es jedoch bisher selten eingesetzt. EAP-TLS erfordert für jeden Client ein Zertifikat. Ohne eine PKI ist der Betrieb nahezu undenkbar. Für EAP-TLS gilt, dass die Sicherheit dieser Variante von den Zertifikaten abhängt. Die Zertifikate müssen auf einem sicheren Weg vom Zertifikataussteller zum Supplicant übertragen und von einer Passphrase geschützt werden. Ein weiterer Nachteil ist, dass die Zertifikate nur die Authentizität der Maschine auf der sie installiert sind bescheinigen können, aber nicht die des Be-

[2] Client, der bei 802.1X Zugriff auf Dienste beantragt

nutzers. Abhilfe kann hier das Installieren der Zertifikate auf einer SmartCard sein. Nachteilig ist, dass unverschlüsselt übermittelte Daten wie das Identity-Response-Paket sowie die Zertifikate die Identität des Supplicant für einen potenziellen Angreifer preisgeben. Der Supplicant überträgt seine Identifikation vor dem Austausch der Zertifikate im Klartext. Ein Angreifer kann hieraus auf den Benutzernamen schließen.

4. **EAP-TTLS und PEAP:** EAP-TTLS und PEAP begegnen dem Problem, dass der Supplicant seine Identität im Klartext überträgt, sodass ein Angreifer den Benutzernamen erlangen kann, indem sie für die Client-Authentisierung einen eigenen TLS-Tunnel aufbauen. Dadurch werden die Client-Authentisierungsdaten geschützt durch den Tunnel transportiert. Durch die Attribute Value Pairs[3] (AVP) ist EAP-TTLS wesentlich flexibler, da AVPs Authentisierungsmethoden ermöglicht, die durch EAP-Methoden nicht abgebildet werden können. Bei EAP-TTLS und PEAP können in der „Inneren“ und „Äußeren“ Authentisierung unterschiedliche Benutzernamen zum Tragen kommen. Außerdem unterstützen beide einen anonymen Benutzernamen für die „Äußere Authentisierung“, sodass der eigentliche Benutzername (im Klartext) in der „Inneren Authentisierung“ geschützt übertragen wird. Jedoch wird dieses Merkmal nicht von allen Herstellern unterstützt.

Auch **TKIP** weist Sicherheitslücken auf. Der Message Integrity Check (MIC) nutzt einen Hash-Algorithmus, um eine Prüfsumme zu bilden. Diese ist jedoch relativ schwach. Bei der Entwicklung musste darauf geachtet werden, dass der Algorithmus nicht zu kompliziert und damit rechenintensiv wird, da er ja noch auf älterer Hardware laufen soll. Ein Angreifer kann sich nun diese schwache Prüfsumme zu nutzen machen und könnte einen Access Point mit von ihm generierten Paketen überschütten (Flooding Attacke). Diese Pakete können einen vom Angreifer festgelegten Inhalt haben aber unterschiedliche Prüfsummen. Ein Paket könnte zufällig die richtige Prüfsumme beinhalten und somit akzeptiert werden. D.h., der Angreifer beobachtet den Access Point, der irgendwann ein Paket durchlassen wird, der die richtige Prüfsumme enthält.

Ein Vorteil von **AES-CCMP** ist, dass es nicht nur zur Verschlüsselung von Daten, sondern auch zur Integritätsprüfung genutzt werden kann. Dabei entfallen die individuellen Schlüssel für die Integritätsprüfung der Daten und Gruppendaten, da ihre Aufgabe bereits von den normalen Schlüsseln übernommen wird. Somit existieren nur noch vier temporäre, 128 Bit lange Schlüssel zur Datenverschlüsselung, Datenintegritätsprüfung, EAPOL-Verschlüsselung und -Integritätsprüfung sowie Gruppendatenverschlüsselung und Integritätsprüfung. CCMP ist derzeit das sicherste Verfahren, stellt jedoch auch die höchsten Anforderungen an Hard- und Software. Aus diesem Grunde wird CCMP derzeit vorrangig in externen Karten implementiert. Inzwischen kann AES sehr gut in Hardware ausgeführt werden. Dies und die reduzierte Schlüsselanzahl beschleunigen die Berechnung der PMK und GMK gegenüber WPA mit TKIP. Auch sind geringere Schlüssellängen nötig. Die meisten Hersteller bieten keine Unterstützung für einen Mischbetrieb von CCMP und RC4-basierten Verfahren wie TKIP, da Treiber den gleichzeitigen Betrieb von CCMP für Unicast-Verkehr und eines RC4-basierten Protokolls für Broadcast-Verkehr nicht ohne weiteres erlauben. Es ist zu beachten, dass im Vergleich zu WPA, bei dem lediglich der „Infrastructure Mode“ funktioniert, RSN auch für den „Ad-Hoc Mode“ ausgelegt ist. CCMP hat sich bereits in sensiblen Anwendungen der U.S. Regierung behaupten können.

[3] definieren Eigenschaften des RADIUS-Protokolls und speichert Informationen

802.11i ist nahezu identisch mit WPA, außer dass es für die Verschlüsselung nicht TKIP, sondern CCMP benutzt. Prinzipiell ist 802.11i abwärtskompatibel zu WPA, sodass das Aufrüsten der Features über ein Firmware-Update möglich ist. Jedoch schließt dies nicht AES-CCMP ein. Neuere WLAN-Karten sind teilweise auf AES-CCMP vorbereitet. Wie bei WPA stützt sich 802.11i auf EAP, wobei lediglich die Varianten EAP-TLS, PEAP und EAP-TTLS zu empfehlen sind. Mit der Verabschiedung von 802.11i hat man einen hinreichend sicheren Standard, mit einer starken Verschlüsselung (AES-CCM) der Luftschnittstelle, die zudem auch als Authentisierung dient. Lediglich die Inkompatibilität in Bezug auf alte Hardware und die dem Funkmedium inhärenten Gefahren können nach dem heutigen Kenntnisstand noch als wesentliche Nachteile betrachtet werden.

4 Vergleich der Verfahren und Gesamtbewertung

Die „802.11i Security Task Group“ sowie der „WiFi WPA“ Standard erachten folgende Punkte als notwendig:

- gegenseitige Authentisierung
- dynamische Sitzungsschlüssel
- Message Integrity Check (MIC)
- TKIP
- schnelles Re-Keying

Der **802.1X-Standard** bildet für diese Punkte die Basis. Aus diesem Grunde sollten Unternehmen ihre WLAN-Infrastruktur auf Basis von 802.1X aufbauen. Damit werden sie durch die einheitliche Authentisierungsmethodik mittels EAP flexibel in der Zugangstechnik, da die AAA-Infrastruktur nicht nur für das WLAN, sondern auch für das LAN sowie VPN eingesetzt werden können. Zudem bietet diese Integrationsmöglichkeit noch eine zentralisierte Benutzerverwaltung, wodurch ein verteiltes und redundantes Management von Benutzerdaten obsolet wird.

Wird die Benutzerauthentisierung nach dem 802.1X-Standard eingesetzt, verhindert der Access Point den Netzwerkzugriff für jene Benutzer, die sich weder durch Name/Passwort, noch durch ein Zertifikat ausweisen können. Darüber hinaus werden nach einer erfolgreichen Benutzerauthentisierung Clients und Access Point mit einmaligen Sitzungsschlüsseln versorgt.

802.11i (WPA, WPA2) bietet Mittel zur Absicherung der Luftschnittstelle eines WLANs. Dabei können Authentisierung und Schlüsselmanagement entweder in Verbindung mit 802.1X oder über Pre-Shared-Keys (PSK) erfolgen, wobei statische PSK nur in Heim- und SOHO-Umgebungen Einsatz finden sollten, zumal in größeren WLANs der administrative Aufwand nicht mehr beherrschbar wäre. Die Kombination mit 802.1X bedingt eine genaue Untersuchung der für die individuelle Security Policy in Frage kommenden EAP-Methode(n).

Bei der Auswahl der Produkte sollte genauestens darauf geachtet werden, welche Verfahren zur Auswahl stehen. WPA benutzt zur Verschlüsselung TKIP, das weiterhin auf WEP und RC4 basiert. TKIP bietet bereits eine Grundsicherheit auf der Bitübertragungsschicht, welche kombiniert mit dem Sicherheitsstandard von 802.1X als ausreichend sicher bezeichnet werden kann.

Im Vergleich zu WPA ist WPA2 mit CCMP (AES als Verschlüsselungsverfahren) deutlich sicherer. CCMP erlaubt Verschlüsselung und Integritätsprüfung und ist im Vergleich zu TKIP

wesentlich leistungsfähiger (höherer Durchsatz). WPA und WPA2 hat diverse Untersuchungen und Prüfungen von Kryptoanalytikern bestanden und entspricht dem Stand der Technik.

Ausgehend von **WEP** ist auch das „dynamische WEP“ eher eine Übergangslösung, die nur von Geräten benutzt werden sollte, die TKIP nicht unterstützen. Um mit diesen eine relativ sichere Verbindung herzustellen, sollte, natürlich in Abhängigkeit von den ausgetauschten Datenmengen, nur eine relativ kurze Schlüssellebensdauer von maximal 15 Minuten eingestellt werden.

Die richtige Wahl des **EAP-Verfahrens** bzw. der Methode ist eine infrastrukturelle Frage, insbesondere eine Frage der Client-Unterstützung:

1. **Schlüsselmaterial:** Essenziell ist, dass die EAP-Methode Schlüsselmaterial zur Verfügung stellen sollte. Es scheidet aus diesem Grunde EAP-MD5 aus.
2. **Gegenseitige Authentisierung:** Auch sollte eine gegenseitige Authentisierung möglich sein. Bei WPA und WPA2 wird gegenseitige Authentisierung empfohlen. Hier bietet sich EAP-TLS an, was jedoch eine PKI erfordert und infrastrukturellen Aufwand impliziert.
3. **EAP-PEAP:** Eine gute Alternative für gegenseitige Authentisierung ist der Einsatz von EAP-Methoden, die mit zwei Tunneln (äußerer und innerer Tunnel) arbeiten und im inneren Tunnel schwächere Authentisierungsverfahren schützen. Solch ein Verfahren ist EAP-PEAP. Bei einer bestehenden Authentisierungsdatenbank in einer Windows-Domäne oder Active Directory ist MS-CHAPV2 die wohl einfachste Wahl für die „Innere Authentisierung“. In EAP-TTLS ist MS-CHAPv2 eingebaut.
4. **LEAP:** Durch die Nutzung von Cisco-Hardware oder anderen Komponenten zwischen Endpunkten kann mit LEAP eine robuste und skalierbare Sicherheitslösung erstellt werden. Die Verschlüsselung des Netzwerkverkehrs sowie die Authentisierung der Benutzer trägt zu einer ausreichend sicheren Lösung bei, womit auf eine relativ aufwändige VPN-Implementierung verzichtet werden kann. Falls auf LEAP verzichtet werden kann, ist ein Protokoll auf Basis von TLS (EAP-TLS und EAP-TTLS) vorzuziehen, da es eine gegenseitige Authentisierung sowie Schlüsselverteilung unterstützt.
5. **EAP-TLS (PKI):** Setzt man eine PKI ein, so ist EAP-TLS zu empfehlen. Active Directory bietet eine PKI auf Basis eines Microsoft Certificate Server mit X.509-Zertifikaten für EAP-TLS. Selbstverständlich ist es auch möglich, weitere Zertifikatsserver in der PKI aufzustellen, falls die Sicherheit weiter ausgebaut werden soll oder aus Gründen der Lastverteilung. Schließlich ist die Herausgabe von Zertifikaten an die Clients und RADIUS-Server ressourcenintensiv, wenn die Clients auch gleichzeitig in der Windows-200x-Domäne sind. Aber auch EAP-TTLS/PEAP mit nach gelagerter EAP-TLS-Authentisierung ist für eine PKI geeignet.
6. **EAP-TLS/PEAP (ohne PKI):** Entscheidet man sich gegen eine PKI, so ist eine Alternative zu EAP-TLS zu suchen, z.B. EAP-TTLS/PEAP. EAP-TTLS ist die richtige Wahl, wenn es sich um ein heterogenes Netzwerk handelt. Die Flexibilität in der Wahl der Authentisierungsmethode sowie in der Möglichkeit, mehrere zu kombinieren, spricht für eine Lösung auf Basis dieses Verfahrens. Das Zertifikat für den RADIUS-Server, und das ist auch das einzig benötigte Zertifikat, kann leicht selbst erstellt oder günstig kommerziell erworben werden. Für die notwendige nach gelagerte Authentisierung könnte bei Windows „PEAP mit Active Directory“ in Frage kommen.

Es ist zu beachten, dass EAP-Methoden von Herstellern, entsprechend ihrer eigenen Interessen, unterschiedlich propagiert und vermarktet werden: LEAP von Cisco, PEAP von Micro-

soft, Cisco und RSA und EAP-TTLS von Funk Software und Certicom. Authentisierungsserver mit Unterstützung von EAP-Methoden existieren zuhauf. Alle benutzen als Authentisierungsprotokoll RADIUS, wobei dem Benutzer überlassen wird, gegen welche Benutzerdatenbank die Authentisierung geprüft wird. Die wichtigsten technischen Auswahlkriterien für den Authentisierungsserver sind Serverbetriebssystem, verwendete EAP-Typen (Methoden) sowie die Schnittstelle(n) zur Benutzerdatenbank.

Wird ein Mischbetrieb von **WPA und 802.11i** beabsichtigt, so sollte man beachten, dass dies sicherheitstechnisch problematisch werden kann. Die unterschiedlichen Clients assoziieren sich nicht mit den Access Points, auf denen auch unverschlüsselter Verkehr oder nur WEP zulässig ist, weil die Verschlüsselung entweder per TKIP (WPA) oder AES-CCMP (WPA2) erfolgen müsste. In diesem Zusammenhang sollte auch TSN (Transition Security Network) erwähnt werden. Gemäß 802.11i ist TSN ein WLAN mit Access Points, die einen Mischbetrieb von 802.11i und schwachen Verfahren wie WEP unterstützen.

Abhilfe für o.g. Problematik schafft eine zweigleisige Lösung. Mittels eines Access Points mit Funktionalitäten wie Dual-Band oder SSID/VLAN-Mapping können in einer WLAN-Funkzelle AES-CCMP (5 GHz-Bereich) und in einer anderen WPA eingesetzt werden. Während die Dual-Band Access Points gleichzeitig sowohl den 5-Ghz-Bereich mit 802.11a/h als auch den 2,4- Ghz-Bereich mit 802.11b/g unterstützen, operieren die Access Points mit niedrigerer Sicherheit im niederfrequenten Band. Mit der SSID/VLAN-Mapping-Funktion dagegen wird mit mehreren SSIDs gearbeitet und Funkzellen logisch voneinander getrennt, sodass sich pro SSID unterschiedliche Sicherheitslevel abbilden lassen. Der Access Point leitet dann die Benutzer der einzelnen SSIDs in verschiedene VLANs.

In der Praxis tritt das Problem auf, wann und wie nach **802.11i** migriert werden kann. Obwohl sehr starker Wert auf Kompatibilität gelegt wurde, erweist sich die Migration zu 802.11i als schwieriger, wenn CCMP zum Einsatz kommen soll. Hierzu ist es notwendig, die Clients zu identifizieren, die in der Lage sind, 802.1X zu unterstützen. Dies ist eine Frage des Client-Betriebssystems und Endgeräts. Problematisch wird es bei mobilen Geräten wie z.B. PDAs und VoIP-Telefonen. Wenige Geräte sind heute in der Lage AES-CCMP hardwareseitig zu unterstützen und bei wenigen lässt sich dieses Problem durch ein Firmware-Update lösen.

In den meisten Fällen muss für einen gewissen Zeitraum ein Parallelbetrieb von alter und neuer Technik möglich werden. Neue Sicherheitsmechanismen werden parallel zu bestehenden eingesetzt und sukzessive umgestellt, da eine sofortige Umstellung sehr hohe Anforderungen an das Roll-out stellt und weitere organisatorische Maßnahmen nach sich zieht, wie Schulungen von Administratoren und Benutzern. Darüber hinaus bedingt dies die Anpassung der Sicherheitsrichtlinien an die neuen Technologien und Verfahren.

Ein wichtiger Punkt für den Mischbetrieb von 802.11i und anderen Sicherheitsmechanismen wie WEP und späterer kompletter Migration nach 802.11i ist die Bildung von Benutzergruppen auf Layer 2 durch Einsatz von Wireless VLANs. Diese bilden unterschiedliche Sicherheitslevels ab und trennen damit sichere und weniger sichere Kommunikation. Während ein VLAN, der durch eine Firewall abgesichert wird, nur einen eingeschränkten Zugang zum LAN erlaubt, wird ein anderes VLAN durch ein VPN geschützt und erlaubt daher uneingeschränkten Zugang zum LAN. Somit existieren zwei Fraktionen nebeneinander: die 802.11i-konformen Clients und die anderen, die noch nicht zu 802.11i migriert sind. Die VLANs müssen an den Access Points für die beiden unterschiedlichen Sicherheitsstufen entsprechend konfiguriert werden. Sukzessiv können dann die Clients, die nicht 802.11i-konform sind, auf-

gerüstet bzw. ersetzt werden, sodass irgendwann das entsprechende VLAN obsolet wird und abgeschaltet werden kann und muss.

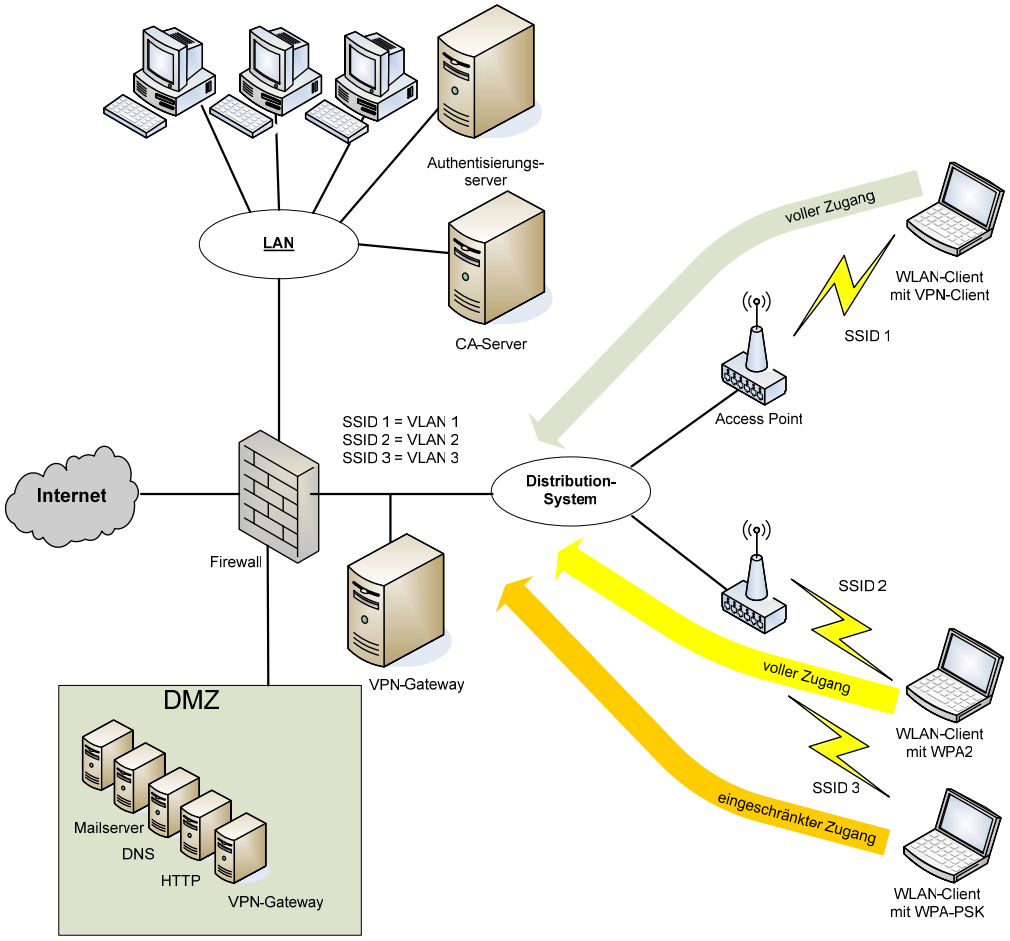

Abb. 1: **WLAN-Mischbetrieb**

Beabsichtigt man **RADIUS** innerhalb einer IEEE 802.1X-Umgebung einzusetzen, so bedient man sich der EAP-Erweiterung des RADIUS-Standards. Ob dabei eine kabelgebundene oder kabellose Infrastruktur zum Tragen kommt, spielt für 802.1X keine Rolle. RADIUS-Client und RADIUS-Server authentifizieren sich gegenseitig über einen MD5-Hash-Wert, der aus dem Shared-Secret, dem Paketinhalt und einer Zufallszahl errechnet wird. Dasselbe Shared-Secret muss dabei sowohl auf dem RADIUS-Client als auch auf dem RADIUS-Server eingetragen sein. Das RFC geht zwar nur auf PAP oder CHAP als Benutzer-Authentisierungsmethoden ein, doch die RADIUS-Erweiterung, die in RFC-2869 spezifiziert wird, erlaubt auch den Einsatz von EAP.

In Verbindung mit den erweiterten EPA-Varianten bietet RADIUS die Bereitstellung von dynamischen WEP-Schlüsseln an. Sie werden mit Hilfe einer „Re-Keying“ Funktion vom Access Point via EAPoL auf die WLAN-Clients übertragen. Die WLAN-Clients benötigen dabei keine spezielle Hardware, um dynamische WEP-Schlüssel nutzen zu können. Verwaltung und Austausch der Schlüssel ist Sache des Betriebssystems. Alle modernen Betriebssysteme unterstützen das Empfangen der WEP-Schlüssel vom Access Point.

Dynamische WEP-Schlüssel haben den Vorteil, dass man nicht den Verkehr aller angeschlossenen Stationen mithören kann. Bei dynamischen WEP-Schlüsseln erhält jede Station einen individuellen Schlüssel, der den für ihn eingehenden und von ihm ausgehenden Verkehr verschlüsselt. Allerdings darf man selbst von dynamischen WEP-Schlüsseln keinen hohen Sicherheitsstandard mehr erwarten. Von der Länge des eingestellten „Re-Keying"-Intervalls, also der Zeitspanne für den Austausch der Schlüssel, hängt es ab, ob ein Angreifer Zeit genug hat, sich Zugang zum Netz zu beschaffen. Extrem verkürzen darf man das „Re-Keying-Intervall" auch nicht, da es sowohl dem RADIUS-Server als auch den RADIUS-Client Rechenlast aufbürdet. Die Anzahl der Clients spielt dabei natürlich auch eine Rolle.

Als Alternative zu dynamischen WEP-Keys existiert WPA oder auch WPA2 (IEEE 802.11i). Beide Verfahren ermöglichen eine optionale Authentisierung via RADIUS. Da WPA und WPA2 grundsätzlich individuelle Schlüssel für jedes übertragene Paket verwenden, gelten sie als sicherer als einfache dynamische WEP-Keys. Die Authentisierung erfolgt hier über EAP analog zu den bereits beschrieben Variante, nur das nach erfolgter Authentisierung WPA als Verschlüsselung eingesetzt wird und nicht WEP.

Eine gesicherte Authentisierung sollte durch Einbringung eines Authentisierungsservers, beispielsweise durch einen RADIUS-Server, erreicht werden. Entsprechend der Vorgabe von WPA sollte dieser als Authentisierungslogik via LAN mit dem Access Point bzw. den Access Points verbunden werden. In einer Unternehmensinfrastruktur darf dies jedoch nicht direkt erfolgen, sondern nur über ein Distribution-System und eine Firewall. Die Ausprägungen können je nach Schutzbedarf variieren. Die gemeinsame Geheiminformation (Shared Secret) zwischen RADIUS-Client und RADIUS-Server muss ausreichend lang und komplex sein. Empfehlenswert ist die Nutzung von unterschiedlichen Shared Secrets für jedes Client-Server-Kommunikationspaar. Darüber hinaus ist die RADIUS-Kommunikation auf die offiziell freigegebene Ports 1812 bzw. 1813 zu beschränken. Bei einem hohen Schutzbedarf wird die Absicherung der RADIUS-Kommunikation per IPsec empfohlen.

5 Fazit

Die Auswahl der zu verwendenden Authentisierungsverfahren orientiert sich an der Security Policy, der u. a. durch den Schutzbedarf der mobilen WLAN-Clients bzw. Benutzer sowie der im WLAN zu transportierenden Daten bestimmt wird. Mit einer gegenseitigen Authentisierung können Angriffe dahingehend abgewehrt werden, als dass beispielsweise keine Rogue Access Points[4] gefährlich werden könnten. Damit wird Angreifern die Möglichkeit genommen, Verbindungen zu übernehmen oder sogar in Clients einzudringen, um Daten zu kompromittieren bzw. schadhaften Code einzuschleusen. Bei einer gut funktionierenden gegenseitigen Authentisierung ist ein Angreifer nicht mehr in der Lage, Benutzerdaten (Credentials) zu benutzen oder eine Brute-Force-Attack auszuführen.

Viele Netzwerke auf Basis von Microsoft Technologien erfordern in der Regel Microsoft-Rechnerauthentisierung. Um sicherzustellen, dass ein Benutzer mit einer autorisierten Maschine mit geeignetem Schutz arbeitet, müssen Authentisierungsserver die Benutzerauthentisierung mit der Rechnerauthentisierung koppeln. Einige 802.1X-Authenticators wie Access Points vereinen beide Authentisierungsvarianten, was jedoch aufgrund der nicht vorhandenen

[4] Access Points, die ohne Wissen der IT-Abteilung in Betrieb genommen wurden

kryptographischen Kopplung der Varianten unsicher und daher nicht zu empfehlen ist. Einige Hersteller von RADIUS-Servern haben ähnliche Ansätze.

Gegen passive Angriffe gibt es generell keine Abwehrmöglichkeiten, da das Funkmedium nur eine begrenzte Kontrolle der Signalausbreitung zulässt. So ist im Vorfeld bei der Auswahl der Antennen und deren Standorte die Überdeckung so auszuwählen, dass ein Angreifer sich entweder in einen überwachten Bereich begeben muss oder dass er keinen oder nur unzureichenden Empfang hat. Werkzeuge wie FakeAP[5], die einem Angreifer hunderte von Access Points vorgaukeln und ihn dazu verleiten sollen seine Attacke vorzeitig abzubrechen, sind sehr hilfreich aber leider auch kein wirklicher Schutz.

Gegen Lauschangriffe, Datenmanipulation oder unerlaubte Zugriffe auf das Netzwerk hilft nur, wie bereits beschrieben, eine starke Verschlüsselung. Zusammen mit einer sicheren Authentisierung des Benutzers, können alle weiteren Attacken abgewehrt werden. Sie verhindert, dass ein Angreifer sich in irgendeiner Form als legitimierter Benutzer oder Bestandteil des Firmennetzwerks ausgibt.

Letztlich müssen immer nur zwei Punkte sichergestellt werden, nämlich erstens, dass die Kommunikationspartner sich gegenseitig sicher authentisieren und zweitens, dass sämtliche Kommunikation geschützt (verschlüsselt) stattfindet. Wenn ein mobiles Kommunikationssystem diese beiden Punkte ausreichend berücksichtigt, können nahezu alle Angriffe abgewehrt werden, bei denen Daten kompromittiert werden könnten. Lediglich bei Denial-of-Service (DoS) Attacken sind die genannten Maßnahmen nicht immer erfolgreich. Dies liegt dann aber in der Spezifikation der benutzten Kommunikationsprotokolle, die andere Schwerpunkte als die Sicherheit setzen. Als Beispiel sei hier ein Access Point genannt, der im Falle einer Attacke zeitweise den Betrieb einstellt. Eine DoS-Attacke ist in diesem Fall nur möglich, weil der Access Point sich gerade so verhält.

Literatur

[BSI03] BSI: Sicherheit im Funk-LAN (WLAN, IEEE 802.11); Informationsschrift des Bundesministeriums für Sicherheit in der Informatik; Projektgruppe „Local Wireless Communication“; Bonn 2003

[DETK05a] K.-O. Detken: Drahtlos, na und...Neue WLAN-Standards für eine sichere Kommunikation; NET 10/05; NET Verlagsservice GmbH; Woltersdorf 2005

[DETK05b] K.-O. Detken: WLAN Security: Drahtlose Sicherheitsmechanismen; Deutscher Wirtschaftsdienst; 118. Ergänzungslieferung; Dezember 2005; ISBN 3-87156-096-0; Köln 2005

[KOCH04] W. Koch: Wireless-LAN – Stand und Entwicklungspotenzial, Nutzungsansätze für KMU. Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, Schriftreihe der Landesinitiative hessen-media, Wiesbaden, 2004

[5] http://www.blackalchemy.to/project/fakeap/