

Sicherheit im WLAN

› Selbst Laien können mit einfachen Tools in Funknetze eindringen. Speziell wenn es um sensible Daten geht, muss man Vorkehrungen treffen, die das Abhören und unerlaubte Nutzen des WLANs erschweren.

› VON DR. AXEL SIKORA

Drahtlose lokale Netze (Wireless LAN - WLAN) erfreuen sich steigender Beliebtheit und Verbreitung. Insbesondere der IEEE 802.11b-Standard setzt sich zunehmend durch. Neben der Planung, Installation und Administration ist dem Sicherheitsaspekt bei WLANs besondere Aufmerksamkeit zu schenken. Neben der grundlegenden Problematik der offenen Ausbreitung der Funkwellen kommt erschwerend hinzu, dass Teile der Funknetz-Standards prinzipbedingt nicht sicher sind.

Dieser Artikel beschreibt zunächst die Sicherheitslücken, insbesondere des aktuell boomenden IEEE 802.11-Standards. Anschließend zeigt er Wege, um sich gegen Angriffe zu schützen und gibt einen Ausblick auf die zukünftigen technischen und standardbezogenen Entwicklungen.

› Mangelhafte Sicherheit mangelhaft genutzt

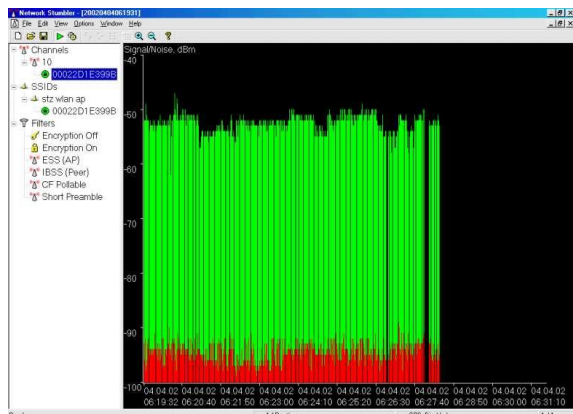
Die Sicherheitsproblematik ist bei allen drahtlosen Systemen besonders relevant. Auf Grund der Ausbreitungscharakteristik elektromagnetischer Wellen ist ein Abhören oder Senden auf der physikalischen Ebene möglich, ohne dass beispielsweise in das Gebäude eingedrungen werden muss (Parking Lot Attack). Hierin besteht ein wesentlicher Unterschied zu drahtgebundenen Übertragungsprotokollen. Bei diesen kann im Normalfall außerhalb des Firmengebäudes nur der für extern bestimmte Datenverkehr beobachtet werden.

Erschwerend kommt hinzu, dass WLAN-Systeme ein komfortables Ad-hoc-Networking ermöglichen sollen. Die Identifizierung, Authentifizierung und Anmeldung (Autorisierung) der Stationen muss dabei möglichst automatisch ablaufen. Die am Markt verfügbaren WLAN-Systeme sehen in der Regel zwar Sicherheitsmechanismen vor, doch haben diese zum Teil erhebliche Lücken. Dadurch sind Angriffe relativ leicht möglich. Dabei unterscheidet man zwischen passiven (Abhören) und aktiven Angriffen (Eindringen).

Von den Sicherheitslücken sind insbesondere die Systeme nach IEEE 802.11 betroffen. Deswegen wird die weitere Diskussion an diesem Beispiel geführt. Bei den anderen WLAN-Systemen sind vergleichbare Risiken bislang noch nicht öffentlich bekannt.

› Kostenlose Werkzeuge für den Angriff

Angriffe auf WLANs sind mit herkömmlichen Geräten aus der Serienproduktion und selbst mit preiswerten WLAN-Karten möglich. Passende Software-Werkzeuge gibt es kostenlos und öffentlich im Internet. Sie messen Funkfelder sehr einfach aus und ermitteln grundlegende Informationen über nicht geschützte Netze. Die Windows-Anwendung Network Stumbler kann man beispielsweise [hier](http://www.netstumbler.com) (<http://www.netstumbler.com>) herunterladen.



Gescannt: NetStumbler liefert zahlreiche Informationen aller gefundenen Funknetze.

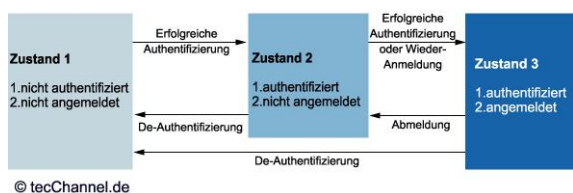
Mittlerweile stehen verschiedene Erweiterungen zur Verfügung, die einen sicheren Betrieb ermöglichen sollen. Diese Ansätze sind aber bislang herstellerspezifisch, da zum gegenwärtigen Zeitpunkt kein umfassender Standard existiert.

Ungeachtet der bekannten Risiken werden in der Praxis selbst die zur Verfügung stehenden Mechanismen nur unzureichend genutzt. Dies macht Angriffe selbst für Laien ohne weiteres möglich. Als populäres Beispiel sehen Sie [hier](http://www.sfrds.ch/news/aktuell_10vor10.html?year=2001&month=05&day=24) (http://www.sfrds.ch/news/aktuell_10vor10.html?year=2001&month=05&day=24) eine Reportage des Schweizer Fernsehens.

› Sicherheitsarchitektur und Authentifizierung

Der IEEE802.11-Standard sieht im Rahmen seiner Sicherheitsarchitektur drei verschiedene Zustände vor, um zwischen assoziierten und authentifizierten Stationen zu unterscheiden. Authentifizierung und Anmeldung bilden zusammen ein zweistufiges Zuordnungssystem:

- › Eine Station kann sich nur anmelden, wenn sie authentifiziert ist. Dabei versteht man unter Authentifizierung den Nachweis, dass eine Station auch diejenige ist, die sie vorgibt zu sein.
- › Eine Station kann das Verteilungssystem nur dann nutzen, wenn sie bei einer Zelle angemeldet ist.



Dreistufig: Die Sicherheitsarchitektur des 802.11-Standards sieht drei Zustände vor, um zwischen assoziierten und authentifizierten Stationen zu unterscheiden.

Im Rahmen der Authentifizierung wird die Identität von Stationen überprüft. Dabei stehen zwei Methoden zur Authentifizierung zur Verfügung:

- › Die offene Authentifizierung (Open Authentication) folgt einem sehr einfachen Algorithmus, der die Funktion einer Authentifizierung nur formal erfüllt.
- › Die Authentifizierung durch gemeinsame Schlüssel (Shared Key Authentication) beruht auf der Überprüfung, ob die beiden beteiligten Stationen denselben geheimen Schlüssel aufweisen. Er basiert auf dem WEP-Algorithmus und weist somit dessen Sicherheitslücken auf.

› Zugangskontrolle

Auf der niedrigsten Ebene erfolgt die Zulassung der Teilnehmer anhand eines Schlüssels, der als Electronic Service Set ID (SSID, ESSID) bezeichnet wird. Diese ID wird von einem Administrator in allen mobilen Teilnehmern und allen Zugangspunkten eingetragen. Dieser zeigt die Zugangsrechte des Clients an, aber nicht die eindeutige Identifikation. Dabei ergeben sich zwei Einschränkungen:

- › Es ist häufig kein Problem, eine allgemeine Zugangsnummer herauszufinden, um den Verkehr auf dem Netzwerk unberechtigt abzuhören.
- › Darüber hinaus erlauben die meisten Hersteller von mobilen Stationen die Angabe der Option "any" in ihren Konfigurationsdateien, wodurch der Einsatz in allen Netzwerken authentisiert ist.

Weiterhin können die MAC-Adressen der mobilen Teilnehmer in die Zugangslisten (ACL) der Access-Points eingetragen werden. Auch hier sind zwei Einschränkungen zu verzeichnen:

- › Die MAC-Adresse des mobilen Teilnehmers lässt sich bei den meisten auf dem Markt verfügbaren Produkten verändern, so dass ein Missbrauch möglich ist.
- › Im Bereich kleiner drahtloser Netzwerke sind ACLs recht problemlos umzusetzen. Bei großen Netzwerken mit mehreren Zugangspunkten erfordert dies jedoch eine umfangreiche Administration jeder Station. Nur so ist für jeden Teilnehmer ein Wechsel zwischen den Funkzellen möglich (Roaming). Bisher bieten nur einige wenige Hersteller komfortable Werkzeuge zur Verwaltung größerer drahtloser Netzwerke an.

› Mehr Sicherheit mit WEP

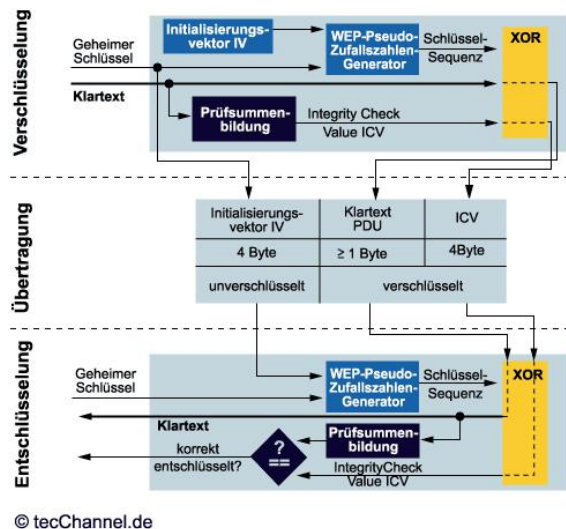
WEP stellt einen optionalen Bestandteil des IEEE802.11-Standards dar. Um ein 802.11-konformes System anzubieten, muss WEP also nicht zwingend implementiert sein. Die im Standard vorgesehene Variante von WEP sieht eine Kodierung mit einem 40 Bit-langen Schlüssel vor. Darüber hinaus bieten einige Hersteller eine Kodierung mit 128 Bit an. Hierbei handelt es sich unter Umständen um proprietäre Entwicklungen, die die Interoperabilität der Systeme unterschiedlicher Hersteller behindern.

Die Verschlüsselung im Rahmen des IEEE802.11 wird nicht nur für die Verschlüsselung der zu übertragenden Informationen eingesetzt, sondern auch für die Authentifizierung von Stationen. Die Kenntnis des Schlüssels ermöglicht also nicht nur das Abhören der versendeten Pakete, sondern auch das Eindringen in das Netzwerk.

Der Generator basiert auf dem RC4-Verschlüsselungsalgorithmus (Key Scheduling Algorithm - KSA), der mit einem statischen WEP-Schlüssel von 40 Bit oder 128 Bit (WEP2) arbeitet. Dabei wird im Rahmen eines so genannten Stromverschlüssellers (Stream Encryption) für jedes Datenpaket ein neuer Schlüssel generiert. Dies ist von zentraler Bedeutung, damit gleiche Klartext-Pakete nicht zu gleichen Schlüsseltext-Paketen führen.

› Unendlich langer Pseudo-Schlüssel

Für die Verschlüsselung wird auf der Grundlage eines vergleichsweise kurzen Schlüssels und eines zufällig bestimmten Initialisierungsvektors (IV) mit Hilfe eines Generators für Pseudo-Zufallszahlen eine unendlich lange Schlüsselreihe generiert. Mit dieser erfolgt die bitweise Verknüpfung des Klartextes mit einem Exklusiv-Oder-Gatter. Das Verfahren verschlüsselt Klartext als auch die Prüfsumme und überträgt diese mit dem unverschlüsselten Initialisierungsvektor.



WEP: Verschlüsselung, Übertragung und Entschlüsselung nach dem WEP-Algorithmus.

Auf der Empfängerseite wird der verschlüsselte Text mit dem ebenfalls expandierten Schlüssel mit einer Exklusiv-Oder-Verknüpfung entschlüsselt. Das WEP-Verfahren basiert also auf einem symmetrischen Algorithmus, bei dem Sender und Empfänger einen gemeinsamen Schlüssel (Shared Key) verwenden.

Der Vorteil des Verfahrens besteht darin, dass es jedes Paket mit einer anderen Zeichenfolge verschlüsselt. Rückschlüsse auf die übertragenen Zeichen durch Ausnutzen von statistischen Verteilungen werden auf diese Weise erschwert.

› WEP-Sicherheitsrisiken

Die Verwendung eines statischen Schlüssels ist zwar vergleichsweise einfach zu realisieren, birgt aber ein signifikantes Sicherheitsrisiko, da nach dessen Bekanntwerden kein Schutz mehr gegeben ist. Dabei sind zwei grundsätzliche Möglichkeiten zu unterscheiden, um an einen statischen Schlüssel zu gelangen:

Erstens kann der Schlüssel über den menschlichen Weg bekannt werden. Dies ist insbesondere dann kritisch, wenn in einem Unternehmen alle Stationen den identischen statischen Schlüssel besitzen. Allerdings ist das Auslesen an den mobilen Stationen meist nicht unmittelbar möglich, da der Schlüssel auf der Karte in einem geschützten Flash-Speicher abgelegt ist.

Zweitens kann ein Angreifer durch verschiedene Algorithmen versuchen, den Schlüssel zu rekonstruieren.

Hier sind folgende Ansätze zu beobachten:

- › Die Verschlüsselung eines Pakets erfolgt ausgehend von einem Initialisierungsvektor (IV). Dieser 24-Bit lange IV wird anhand eines feststehenden Algorithmus mit jedem neuen Paket verändert. Dies bedeutet, dass nach 2^{24} , rund 16,7 Millionen Paketen wieder mit der gleichen Abfolge von Initialisierungsvektoren begonnen wird. Entsprechend liegen dann der Verschlüsselung der folgenden Pakete die gleichen Zeichenfolgen zugrunde.
- › Im Rahmen der sogenannten Known-Plain-Text-Angriffe werden Rückschlüsse auf den verwendeten Schlüssel über Paare von bekannten und verschlüsselten Daten gezogen. Bekannte Daten kann ein Angreifer zum Beispiel aus der Struktur von IP-Paketen ableiten.
- › Darüber hinaus ist die Kombination einer Stromverschlüsselung, wie sie durch RC4 vorgegeben ist, mit einer Fehlererkennung durch einen lineare Cyclic Redundancy Check (CRC) unsicher. Zum einen treten nachvollziehbare Abhängigkeiten zwischen den zu übertragenden Daten auf. Zum anderen können Modifikationen in den Paketen unentdeckt bleiben, wenn die CRC-Daten entsprechend angepasst

werden.

Insbesondere auf der Schwäche der Initialisierungsvektoren basieren Werkzeuge wie [Airsnort](http://airsnort.sourceforge.net) (<http://airsnort.sourceforge.net>) und [Wepcrack](http://sourceforge.net/projects/wepcrack) (<http://sourceforge.net/projects/wepcrack>), die kostenlos und frei über das Internet verfügbar sind. Mit diesen finden Hacker die verwendeten Schlüssel innerhalb weniger Stunden heraus. Sowohl die hierfür benötigte kriminelle Energie als auch die erforderlichen Kenntnisse, Werkzeuge und Fähigkeiten sind vergleichsweise gering. Dabei ist zu vermerken, dass auf Grund dieser Schwäche die Sicherheit der Verschlüsselung nicht exponentiell zunimmt, wie dies bei der Verwendung eines linearen Schlüssels der Fall wäre. Die Komplexität steigt bestenfalls linear.

› Gegenmaßnahmen

Folgende Anforderungen muss ein sicheres WLAN in der Praxis erfüllen.

- › Umfassende Authentifizierung: In einer umfassenden Sicherheitsarchitektur müssen alle an einem Netzwerk beteiligten Stationen ihre Identität nachweisen (mutual authentication). Dies ist eine Anforderung, die insbesondere von drahtlosen oder mobilen Stationen gestellt wird. Denn nur durch eine wechselseitige Authentifizierung kann sichergestellt werden, dass sich ein mobiler Teilnehmer keinem "feindlichen" Netzwerk anvertraut. In einer bekannten und festverdrahteten Umgebung ist das Risiko, an einen feindlichen Partner zu gelangen, unvergleichlich geringer, da hierfür die bestehende Netzwerkinfrastruktur bereits modifiziert worden sein muss.
- › Flexibilität: Die Sicherheitskonzepte müssen die Anforderungen der unterschiedlichen Nutzergruppen erfüllen. So müssen beispielsweise in einem Firmennetz die Nutzer beschränkt werden, während ein Service Provider für alle Nutzer offen ist, aber dennoch den Verkehr der unterschiedlichen Nutzer getrennt "sichern" muss.
- › Mobilität: Darüber hinaus muss die Mobilität der Stationen im Rahmen eines Roaming unterstützt werden. Hierdurch kann praktisch nur eine zentralisierte Server-Realisierung zum Einsatz kommen.
- › Vertraulichkeit: Es ist ein Konzept erforderlich, dass nicht nur auf einer Information, wie einem statischen Schlüssel, basiert. Ein solcher Schlüssel kann über den menschlichen Weg oder beim Diebstahl einer mobilen Station bekannt oder durch intelligente Lauschangriffe herausgefunden werden. Eine dynamische Schlüsselverwaltung erscheint unumgänglich. Darüber hinaus müssen die Verwaltung und Verteilung der Schlüssel selbst auch wieder sicher sein. Bei der Verteilung der Schlüssel darf man keine Rückschlüsse auf die verwendeten Schlüssel ziehen können.
- › Skalierbarkeit: Die Systeme müssen skalieren. Dies bedeutet, dass auch der Einsatz mehrerer Hundert oder Tausend Stationen möglich sein muss. Diese für das allgemeine Unternehmensumfeld sicherlich sinnvolle Anforderung führt aber leider bei einer Reihe der vorgestellten Lösungen zu einem hohen Aufwand, der in kleineren SOHO-Netzen in der Regel nicht zu leisten ist.

› Aufwendigere Verschlüsselung

Die Einsatz einer stärkeren Verschlüsselung verringert zwar die Gefahr, dass durch Abhören Rückschlüsse auf den verwendeten Schlüssel gezogen werden können, da der Rechenaufwand für das Herausfinden des Schlüssels steigt. Das grundsätzliche Risiko eines statischen und symmetrischen Schlüssels bleibt aber bestehen, ebenso wie die Gefahr des Eindringens in das Netzwerk.

Da die beschriebenen Mängel auch beim IEEE bekannt sind, wurde dort die [Task Group i](http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm) (TG1) ins Leben gerufen. Sie soll einen Nachfolger für WEP entwickeln und standardisieren. Nach verschiedenen Ansätzen ist gegenwärtig jedoch leider keine große Bereitschaft dieser Task Force wahrzunehmen, einen einheitlichen Standard auf den Weg zu bringen. Verschiedene konkurrierende

herstellerspezifische Lösungen sind jedoch schon auf dem Markt verfügbar. Auf diese sind die Anwender gegenwärtig angewiesen. Hier zwei typische Beispiele, die andere Hersteller in ähnlicher Art verfolgen.

Lucent bietet mit WEPplus eine WEP-Erweiterung an, die speziell die Angreifbarkeit durch AirSnort eliminieren soll. Hierzu wird ein anderer Algorithmus für die Erzeugung der Initialisierungsvektoren (IV) eingesetzt. Diese Lösung erfordert lediglich ein Treiber-Update. Da der IV von der sendenden Station vorgegeben und im Datenpaket mit übertragen wird, ist WEPplus abwärtskompatibel.

Die Firma [RSA Data Security](http://www.rsasecurity.com/) (<http://www.rsasecurity.com/>), die den RC4-Algorithmus erfunden hat, bietet mit der als Fast Packet Keying (FPK) bezeichneten Erweiterung ebenfalls eine Lösung. FPK erzeugt aus dem konstanten, vorgegebenen Schlüssel sowie der ebenfalls konstanten Senderadresse und einem paketspezifischen IV mittels eines Hashing-Algorithmus für jedes Datenpaket einen individuellen 104 Bit langen Paketschlüssel. Auf diese Weise wiederholen sich die IV erst nach 2^{103} , statt wie bisher nach 2^{24} Paketen.

› Authentifizierung via EAP und 802.1X

Das Extensible Authentication Protocol (EAP - RFC 2284) stellt ein grundlegendes Fundament für eine umfassende und zentralisierte Sicherheitskonzeption dar. Es wurde ursprünglich für PPP-Links entwickelt, um eine zuverlässige Authentifizierung von Remote-Access-Usern bereitzustellen. EAP ist ein allgemeines Protokoll, das mehrere Authentifizierungsmöglichkeiten bietet. Die Auswahl des Verfahrens findet im Point-to-Point-Protocol erst nach der Link Control Phase (LCP) in der Authentifizierungsphase statt.

Rahmenformat der in Ethernet gepackten EAP-Pakete

Byte	Beschreibung	Anmerkung
1 - 7	Preamble	
8	Start Delimiter	
9 -14	Destination Address	
15 - 20	Source Address	
21 - 22	Length / Type	Port Access Entity (PAE) Ethernet Type
23	Protocol Version	0000 0001 als Standard
24	Packet Type	0000 0000 EAP-Packet 0000 0001 EAPOL-Start 0000 0010 EAPOL-Logoff 0000 0011 EAPOL-Key 0000 0100 EAPOL-Encapsulation-ASF-Alert
25 - 26	Packet Body Length	vorhanden nur für EAP-Packet, EAPOL-Key, EAPOL-Encapsulation-ASF-Alert
27 - N	Packet Body	vorhanden nur für EAP-Packet, EAPOL-Key, EAPOL-Encapsulation-ASF-Alert

Im Rahmen: Das Rahmenformat der in Ethernet eingepackten EAP-Pakete.

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-Messages 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).

An einer solchen portbezogenen Authentifizierung sind drei Elemente beteiligt:

- › der Client (Supplicant), der sich in einem Netzwerk authentifizieren möchte,

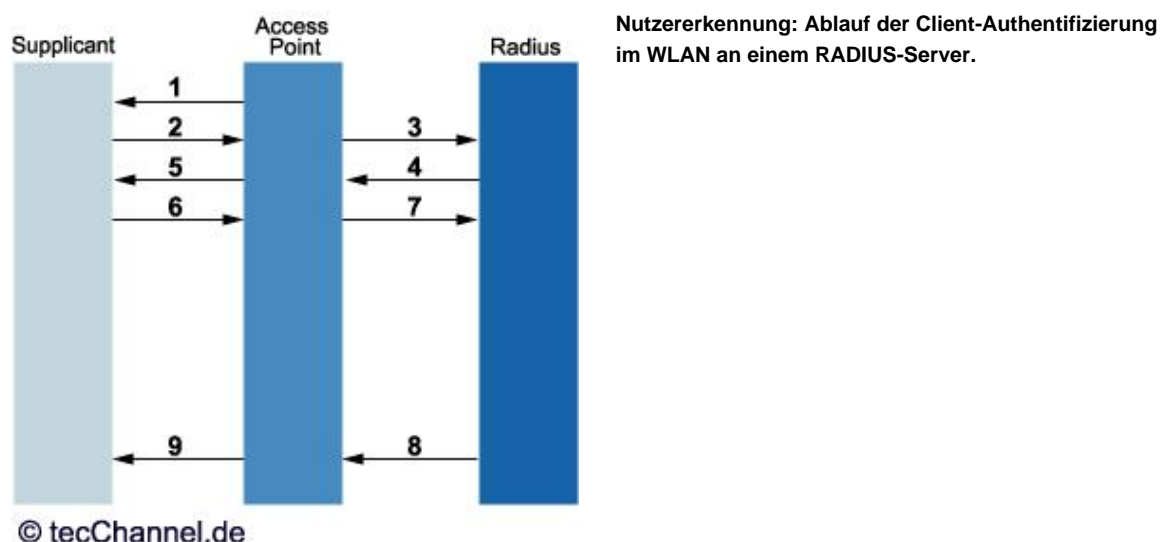
- › der Authentifizierer (Authenticator), der den Authentifizierungsvorgang mit dem Client durchführt, und
- › der Authentifizierungs-Server (Authentication Server), der dem Authentifizierer die zur Authentifizierung erforderlichen Informationen zur Verfügung stellt.

› IEEE802.1X im Detail

Die Idee hinter IEEE802.1X ist, dass einem physischen Anschluss zwei logische Anschlüsse (Ports) zugeordnet werden. Der physische Anschluss leitet die empfangenen Pakete grundsätzlich an den so genannten freien Port (Uncontrolled Port) weiter. Der kontrollierte Port (Controlled Port) kann nur nach einer Authentifizierung erreicht werden, die über den freien Port erfolgen kann.

In der Regel übernimmt ein RADIUS-Server (Remote Access Dial-Up User Service - RFC 2138) die Rolle des Authentifizierungs-Servers. Das RADIUS-Protokoll wurde ebenfalls zur Authentifizierung von Benutzern ausgerichtet, die sich über einen Wählzugang in einem Netzwerk anmelden wollen. Eine Beschreibung findet sich in den RFC 2138 und 2139, sowie 2865 bis 2868. Die EAP-Message wird dann als Attribut im RADIUS-Protokoll übertragen.

Für den Einsatz in einem WLAN ergibt sich folgender Ablauf, den Sie auch im folgenden Bild nachvollziehen können.



- › 1. Der Access Point fordert vom Client seine Identität.
- › 2. Der Client liefert seine Identität an den Access Point.
- › 3. Die Information über den offenen Port leitet der Access Point an den RADIUS-Server weiter.
- › 4. Eine Authentifizierung des Clients wird vom RADIUS-Server gefordert. Diese Anforderung (Challenge) sendet er zunächst an den Access Point.
- › 5. Weiterleitung der Anforderung vom Access Point an den Client.
- › 6. Der Client sendet eine Antwort auf die Anforderung an den Access Point. Diese Antwort enthält die geforderte Authentifizierung, beispielsweise ein bestimmtes Passwort oder eine korrekte Verschlüsselung einer in der Anforderung enthaltenen Zeichenfolge.
- › 7. Die Antwort leitet der Access Point an den RADIUS-Server weiter.
- › 8. Der RADIUS-Server überprüft die Antwort. Im Fall eines Erfolgs sendet er eine entsprechende Meldung an den Access-Point.

- › 9. Der kontrollierte Port wird vom Access-Point freigegeben. Darüber hinaus leitet er die Meldung an den Client weiter.

› Lücken in IEEE802.1X

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

Erstens sieht IEEE802.1X 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 einen Angriff eines "falschen Servers", der so genannten Man-in-the-Middle-Attack.

Zweitens 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, so dass der Angreifer einen Zugang zum Netzwerk erhalten kann.

Solche Angriffe sind bei einer Dial-Up-Verbindung nicht praktikabel, da dabei die Serverseite durch die Verfügbarkeit unter einer festen Telefonnummer bereits authentifiziert ist. Bei festverdrahteten und entsprechend nach außen abgesicherten Netzwerken erscheint das Risiko ebenfalls vergleichsweise gering.

› Erweiterungen

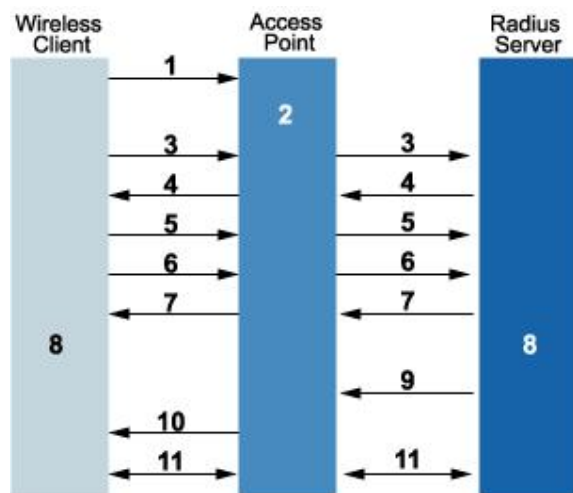
Bei drahtlosen Netzwerken sind die bisher diskutierten Konzepte nicht ausreichend, was eine Reihe von Erweiterungen erforderlich macht. Zum einen erscheint eine wechselseitige Authentifizierung (Mutual Authentication) unabdingbar. Zu den bekanntesten Verfahren mit wechselseitiger Authentifizierung zählen unter anderem:

- › das EAP-Transport Level Security (EAP-TLS in RFC 2716),
- › das PPP Challenge Handshake Authentication Protocol (CHAP in RFC 1994) und die Microsoft-Implementierung, das Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), sowie
- › das Lightweight EAP (LEAP), das vor allem Cisco unterstützt.

Zum anderen muss eine sichere Verschlüsselung der Pakete erfolgen, so dass weder ein Abhören der Nachrichten noch ein aktives Eindringen in das Netzwerk möglich ist. Als Beispiel für eine solche Verwaltung wird im Folgenden die Lösung vorgestellt, die Cisco für seine Produkte anbietet. Hierbei handelt es sich um eine Erweiterung eines Proxy-Servers, der die Rolle eines RADIUS-Servers übernimmt. Dieser Server wird von Cisco als ACS (Access Control Server) bezeichnet. Er verwendet für die Authentifizierung der WLAN-Terminals das MS-CHAP2 in Verbindung mit LEAP.

› MS-CHAP2 mit LEAP

Eine Anmeldung beim Cisco-Access-Control-Server umfasst die folgenden Schritte.



Proxy-Erweiterung: Beim Cisco-Access-Control-Server erfolgt eine sichere Verschlüsselung der Pakete, so dass weder ein Abhören der Nachrichten noch ein aktives Eindringen in das Netzwerk möglich ist.

© tecChannel.de

- › 1. Der IEEE802.11-Client meldet sich über den Uncontrolled Port beim Access Point an.
- › 2. Der AP blockiert alle Requests des Clients über den Controlled Port (z.B. IP Requests), bis dieser sich am Netzwerk angemeldet hat.
- › 3. Der User am IEEE802.11-Client meldet sich über seine normale Netzwerk-Anmeldung (Network Logon) mit Username und Passwort beim Radius-Server an, wobei der Access-Point diese Anfrage weiterleitet.
- › 4. Der Radius-Server authentifiziert den User. Hierzu wird ein MD5-Hash-Paket (Message Digest) mit einem zu verschlüsselnden Text (Challenge Text) über den Access Point an den Client übertragen.
- › 5. Der Client sendet seine Antwort (Response) über den Access Point an den Radius-Server.
- › 6. Auf diese Weise kann auch der Client den Radius-Server authentifizieren. Er sendet einen zu verschlüsselnden Text über den Access Point an den Radius-Server.
- › 7. Der Radius-Server sendet seine Antwort (Response) über den Access Point an den Client.
- › 8. Radius-Server und Client berechnen den Session Key, der für die WEP-Verschlüsselung eingesetzt wird. Dieser wird berechnet unter Einbeziehung des User-Passworts, sowie der Challenge Requests und Responses von Client und Server.
- › 9. Der Radius-Server sendet den Session Key an den AP.
- › 10. Der AP verschlüsselt seinen Broadcast-Key mit dem Session Key und sendet ihn an den Client.
- › 11. Radius-Server und Client haben sich nun wechselseitig authentifiziert und verfügen nun ebenso wie der Access-Point über einen User- und Sitzungsspezifischen Schlüssel. Die verschlüsselte Datenübertragung kann nun also beginnen.

Dabei ist hervorzuheben, dass die Übertragung der Broadcast-Schlüssel bereits gesichert mit Hilfe des Session-Keys erfolgt. Dieser kann durch die Rückführung auf Usernamen und Passwörter ohne manuellen Verwaltungsaufwand erzeugt werden. Zudem können die WEP-Schlüssel periodisch geändert werden.

Über die beschriebenen Gegenmaßnahmen hinaus können umfassende und bereits

bestehende Sicherheitskonzepte auf den höheren Protokollebenen eingesetzt werden. Insbesondere bietet das Konzept der Virtuellen Privaten Netzwerke (VPN) einen sinnvollen Rahmen. VPNs basieren auf dem so genannten Tunneling, schließen aber Sicherheitsmechanismen wie Firewalls, Authentifizierung und Verschlüsselung als integrale Bestandteile mit ein.

› Fazit

Wireless-LANs können auf der Grundlage der beschriebenen Sicherheitsmechanismen zuverlässig abgesichert werden - zumindest was die heutigen Angriffstechniken betrifft. Dies setzt aber voraus, dass die bereit stehenden Sicherheitsmaßnahmen auch tatsächlich umgesetzt werden. Dabei ist die Situation weiterhin dadurch geprägt, dass

- › die verfügbaren Lösungen proprietär sind und somit nur in einer homogenen Umgebung umgesetzt werden können,
- › ein Teil der Lösungen (RADIUS-Server, VPN) zwar praktikabel für größere Unternehmensnetze sind, für SoHo-Netzwerke aber kaum realisierbar erscheinen.

Heimnetzwerker sollten daher:

- › eine vorhandene Verschlüsselung unbedingt nutzen.
- › den statischen Schlüssel in regelmäßigen Abständen aktualisieren,
- › eventuell vorhandene neue Treiber mit aufwendigerer Verschlüsselung, die über den Standard hinausgeht, vom Hersteller herunterladen,
- › WLANs eine eigene SSID geben und ein SSID-Broadcast unterbinden,
- › Zugangskontrolllisten auf MAC-Ebene pflegen und
- › die Log-Dateien regelmäßig auf unbekannte MAC-Adressen überprüfen, um eventuelle Eindringversuche zu entdecken.

Bei größerem Engagement kann man auch über ein Auftrennen des Netzwerkes in einen WLAN- und einen "sicheren" Teil nachdenken, wobei die Kopplung über eine Firewall erfolgen kann. Diese Maßnahmen verringern das Risiko eines Eingriffs signifikant, auch wenn weiterhin Sicherheitslücken bleiben. (ala/fkh)

› Weiterführende Literatur

Arbaugh, W.A., Shankar, N, Wan, Y.C.J., Your 802.11 Wireless Network has No Clothes, University of Maryland, 30. März 2001.

*Borisov, N., Goldberg, I., Wagner, D., Intercepting Mobile Communications: The Insecurity of 802.11, Seventh Annual International Conference on Mobile Computing And Networking, 16.-21. Juli 2001, verfügbar unter:
<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>.*

*Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, Preliminary Draft, 25.7.01, verfügbar unter:
http://www.crypto.com/papers/others/rc4_ksaproc.ps.*

Mishra, A., Arbaugh, W.A., An Initial Security Analysis of the IEEE802.1X Standard, University of Maryland, 6. Februar 2002

Sikora, A., Wireless LAN - Protokolle und Anwendungen, Addison-Wesley, 2001, ISBN 3-8273-1917-X

Singh, S., Geheime Botschaften - Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet", Carl Hanser Verlag 2000, ISBN 3-446-19873-3

› Weitere Themen zu diesem Artikel:

802.11: Standard für drahtlose Netze (<http://www.tecchannel.de/hardware/680/index.html>)

Test: Funknetze nach IEEE 802.11 (<http://www.tecchannel.de/hardware/620/index.html>)

Wireless LANs im Überblick (<http://www.tecchannel.de/hardware/750/index.html>)

Bluetooth - der Kabel-Killer (<http://www.tecchannel.de/hardware/477/index.html>)

DECT: Die Alternative zu Bluetooth (<http://www.tecchannel.de/hardware/511/index.html>)

Elektromog: Gefahren durch Mobilfunk? (<http://www.tecchannel.de/hardware/628/index.html>)

Copyright © 2001
IDG Interactive GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Interactive GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in tecChannel unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von tecChannel aus gelinkt wird, übernimmt die IDG Interactive GmbH keine Verantwortung.



NETSTUMBLER.COM

Please Register to be a member

Login

Password

REGISTER

Advertisement for a "Complete Wardriving Kit" featuring the "wireless CENTRAL.NET" logo, a car, and a wireless antenna. The text lists prices: "..without PC Card \$99" and "..with PC Card \$160". An image of a wireless antenna is also shown.

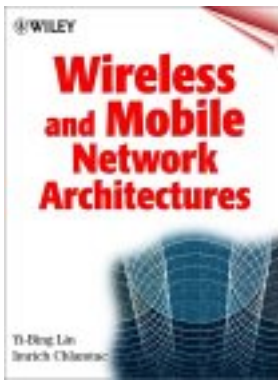
Main Menu

- [Home](#)
- [NetStumbler Uploads](#)
- [National Map](#)
- [MapPoint Converter](#)
- [Topics](#)
- [Forums](#)
- [Mapping Database](#)
- [Web Links](#)
- [Downloads](#)
- [Your Account](#)
- [Submit News](#)

Other Options

- [FAQ](#)
- [Members List](#)

Wireless LAN



FAQ

FAQ Topics include:

- Netstumbler
- Ministumbler
- Wifi
- Antennas

All logos and trademarks in this site are property of their respective owner. The comments are property of their posters, all the rest © 2001 & 2002 - W. Slavin (afr AT netstumbler DOT com)