Security im WLAN

Drahtlose Sicherheitsmechanismen anwenden

Kai-Oliver Detken

Wireless LANs (WLAN) basieren auf dem definierten Standard IEEE 802.11, der 1997 spezifiziert wurde. Mit WLANs können mit geringem Aufwand und auf sehr flexibler Basis drahtlose lokale Netze aufgebaut werden. In den meisten Fällen werden sie als Erweiterung des bestehenden Festnetzes gesehen; ein WLAN kann aber auch als Alternative zu neuen Festinstallationen eingesetzt werden. In den letzten Jahren sind WLANs in verschiedenen Bereichen immer populärer geworden, insbesondere in der Medizin, etwa in Krankenhäusern, im Verkauf, in Herstellung und Forschung. Allerdings geriet die Sicherheit in der Vergangenheit immer mehr in Verruf. Da aber WLANs in sehr sensiblen Umgebungen eingesetzt werden, sollte gerade die Security kontinuierlich hinterfragt werden.

Dr. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Bei den WLAN-Basistechniken lassen sich je nach verwendetem Frequenzband zwei Hauptgruppen 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 im 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: Er bietet mit dynamischer Frequenzauswahl und variabler Sendeleistung zwei Zusatzmerkmale, die die ETSI für den europäischen Markt verlangt.
Inzwischen wurden einige ergänzende Standards festgelegt, etwa IEEE 802.11c. Dieser Standard behandelt die Verfahren für Wireless Bridging, also die drahtlose Kopplung verschiedener Netztopologien. Als „World Mode“ regelt der Standard 802.11d die regionsspezifischen technischen Unterschiede, etwa wie viele Nutzer welche Kanäle mit welchen der Basistechniken a, h, b oder 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 Quality-of-Service- 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 Laufzeitschwankungen 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).

Das Thema in Kürze

Immer wieder – und oftmals durch Leichtfertigkeit verursacht – gerät die (fehlende) Sicherheit von Wireless LANs auch ins Blickfeld der Öffentlichkeit. Mittlerweile haftet ihnen der Ruf an, insbesondere für Unternehmen ein Sicherheitsrisiko darzustellen. Der Autor diskutiert deshalb in dem Beitrag bereits verfügbare und künftige Security-Mechanismen, die ein WLAN sicher machen – vorausgesetzt, man nutzt die Möglichkeiten.

Sicherheitsschwächen

Aufgrund der Ausbreitungscharakteristik elektromagnetischer Wellen ist ein Abhören oder Senden auf der physikalischen Ebene möglich, ohne daß beispielsweise in das Gebäude eingedrungen werden muß. Hierin besteht ein wesentlicher Unterschied zur drahtgebundenen Übertragung. 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. Hier unterscheidet man zwischen passiven (Abhören) und aktiven Angriffen (Eindringen).
Angriffe auf WLANs sind mit herkömmlichen Geräten aus der Serienproduktion und selbst mit preiswerten

WLAN-Karten möglich. Passende Softwarewerkzeuge gibt es kostenlos im Internet. Sie messen Funkfelder sehr einfach aus und ermitteln grundlegende Informationen über nicht geschützte Netze. 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.

Der IEEE-802.11-Standard sieht in 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.

Im Rahmen der Authentifizierung wird die Identität von Stationen überprüft. Dabei stehen wiederum 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 (Wired Equivalent Privacy) und weist somit dessen Sicherheitslücken auf.

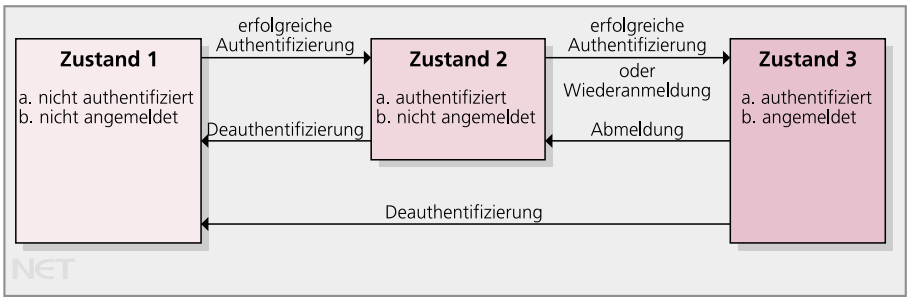
Auf der niedrigsten Ebene erfolgt die Zulassung der Teilnehmer anhand eines Schlüssels, der Electronic Service Set ID (ESSID oder SSID). Diese ID muß in allen mobilen WLAN-Geräten und Zugangspunkten eingetragen werden und zeigt die Zugangsrechte des Clients an, nicht aber die eindeutige Identifikation. Allerdings ist es häufig kein Problem, eine allgemeine Zugangsnummer herauszufinden, um den Verkehr auf dem Netz unberechtigt abzuhören.

Weiterhin können die MAC-Adressen der mobilen Teilnehmer in die Zugangslisten (ACL) der Access-Points eingetragen werden. Auch hier sind Einschränkungen zu verzeichnen. So läßt sich die MAC-Adresse des mobilen Teilnehmers bei den meisten Produkten verändern, so daß ein Mißbrauch möglich ist. Zusätzlich erfordern bei großen Netzen mit mehreren Zugangspunkten die Zugangslisten eine umfangreiche Administration jeder Station. Nur so ist für jeden Teilnehmer ein Wechsel zwischen den Funkzellen möglich (Roaming). Bislang bieten nur einige wenige Hersteller komfortable Werkzeuge zur Verwaltung größerer drahtloser Netze an.

Hinzu kommt die Verschlüsselung mittels WEP. Sie stellt einen optionalen Bestandteil des IEEE-802.11-Standards dar. Die im Standard vorgesehene Variante von WEP sieht eine Codierung mit einem 40 bit langen Schlüssel vor, was auf keinen Fall als ausreichend bezeichnet werden kann. Deshalb bieten heute alle Hersteller ebenfalls eine Codierung mit 128 bit an. Die Verschlüsselung bei IEEE 802.11 wird nicht nur für das Verschlüsseln 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 Netz. Der Generator basiert auf dem RC4-Verschlüsselungsalgorithmus, der mit einem statischen WEP-Schlüssel arbeitet. Bei der Stream Encryption wird für jedes Datenpaket ein neuer Schlüssel generiert.

Dies ist von zentraler Bedeutung, damit gleiche Klartextpakete nicht zu gleichen Schlüsseltextpaketen führen. 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 Schlüsselfolge generiert. Mit dieser erfolgt die bitweise Verknüpfung des Klartextes mit einem Exklusiv-Oder-Gatter (XOR). Das Verfahren verschlüsselt sowohl Klartext als auch die Prüfsumme und überträgt diese mit dem unverschlüsselten IV. Auf der Empfängerseite wird der verschlüsselte Text mit dem ebenfalls expandierten Schlüssel mit einer XOR-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. Die Verwendung eines statischen Schlüssels ist zwar vergleichsweise einfach zu realisieren, birgt aber ein signifikantes Sicherheitsrisiko, da nach seinem Bekanntwerden kein ausreichender Schutz mehr gegeben ist. Dabei sind zwei grundsätzliche Möglichkeiten zu unterscheiden, um an einen statischen Schlüssel zu gelangen: Der Schlüssel kann über den menschlichen Weg be-



Die Drei-Stufen-Sicherheitsarchitektur im Standard IEEE 802.11

kannt werden oder es kann ein Angreifer durch verschiedene Algorithmen versuchen, den Schlüssel zu rekonstruieren.
Die Verschlüsselung eines Pakets erfolgt ausgehend von einem IV. Dieser 24 bit lange IV wird anhand eines feststehenden Algorithmus mit jedem neuen Paket verändert. Dies bedeutet, daß nach 224 Paketen wieder mit der gleichen Abfolge von Initialisierungsvektoren begonnen wird. Entsprechend liegen dann der Verschlüsselung der nachfolgenden Pakete die gleichen Zeichenfolgen zugrunde. Bei sogenannten Known-Plain-Text-Angriffen 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 linearen 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.

Erhöhung des Sicherheitsgrades

Der 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 ebenso bestehen wie die Gefahr des Eindringens in das Netz.
Da die beschriebenen Mängel auch beim IEEE bekannt sind, wurde dort die Task Group i (TGi) ins Leben gerufen. Sie soll einen Nachfolger für WEP entwickeln und standardisieren, was aber bislang noch nicht umgesetzt wurde. 802.11i soll alle wichtigen Sicherheitsmerkmale integrieren. Dazu zählen die Authentifizierung gemäß IEEE 802.1x (EAP, RADIUS, Kerberos) sowie eine Verschlüsselung nach dem Rijndael-Algorithmus (AES).
Derweil versuchen die Hersteller im Industriekonsortium WiFi Alliance, die Schwächen von WEP durch eine Interimslösung WPA (WiFi Protected Access) aufzufangen. WPA umfaßt als Kernbestandteile die Weak Key Avoidance (WEPplus), EAP-gestützte Authentifizierung sowie Temporal Key Integrity Protocol (TKIP). TKIP soll die gravierendsten WEP-Schwächen umgehen: den konstanten Schlüssel sowie die fehlerhafte Integritätssicherung. Aus Kompatibilitätsgründen benutzt TKIP jedoch nach wie vor das anfällige Stromverschlüsselungsverfahren RC4.
Das Extensible Authentication Protocol (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 das im Jahr 2001 verabschiedete IEEE 802.1X gefunden, das die physische Übertragung auf LAN-Netze anpaßt. Die EAP-Messages werden hierzu in 802.1X-Messages verpackt (EAP over LAN – EAPOL). Ziel dieses Standards ist die portbezogene Zugangskontrolle in Netzen (Port-based Network Access Control).
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 sogenannten 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 Authentication Dial-In User Service) nach RFC-2138 die Rolle des Authentifizierungs-Servers. Das RADIUS-Protokoll wurde ebenfalls zur Authentifizierung von Benutzern ausgerichtet, die sich über einen Wählzugang in einem Netz anmelden wollen. Die EAP-Message wird dann als Attribut im RADIUS-Protokoll übertragen.
Der Standard IEEE 802.1X stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netze dar. Dennoch gibt es zwei Einschränkungen:

- 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.
- Es enthalten nach einer einmal erfolgten Authentifizierung die einzelnen Pakete keine Zuordnung mehr. Daher kann bei einem sogenannten 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 Netz erhalten kann.

Bei drahtlosen Netzen sind die bisher diskutierten Konzepte nicht ausreichend, was eine Reihe von Erweiterungen erforderlich macht. Eine wechselseitige Authentifizierung (Mutual Authentication) ist daher unabdingbar (z.B. mittels EAP-TLS). Zum anderen muß eine sichere Verschlüsselung der Pakete erfolgen, so daß weder ein Abhören der Nachrichten noch ein aktives Eindringen in das Netz möglich ist (z.B. mittels VPN).
Als Fazit bleibt, daß WLANs auf der Grundlage der beschriebenen Sicherheitsmechanismen zuverlässig abgesichert werden können. Dies setzt aber voraus, daß die bereitstehenden Sicherheitsmaßnahmen auch tatsächlich umgesetzt werden. Zu gewährleisten sind: umfassende Authentifizierung, Flexibilität der Sicherheitskonzepte, Mobilität bzw. Roaming, Vertraulichkeit und Skalierbarkeit der Systeme. Virtual Private Networks (VPN) übrigens ermöglichen einen noch umfassenderen Schutz, wobei als Alternative künftig IEEE 802.11i eingesetzt werden kann. *(we)*