LANCOM™ Techpaper
Überblick WLAN- Sicherheitsfunktionen

Mit der immer breiteren Nutzung der WLAN-Technologie stiegen in den letzten Jahren auch stetig die Anforderungen an die Sicherheitsmechanismen, mit denen die übertragenen Daten gegen den Zugriff von Unbefugten geschützt werden können. Da sich die Daten in einem WLAN durch die Luft ausbreiten, ist eine Kontrolle bzw. eine Beschränkung des Zugriffs nicht so einfach möglich wie in einem kabelgebundenen LAN.

Nach den ersten Sicherheitsvorgaben aus dem IEEE 802.11-Standard haben sich in den letzten Jahren weitere Funktionen und neue Standards entwickelt, mit denen moderne WLANs geschützt werden.

Die Sicherheitsmechanismen in WLANs zielen in der Regel auf die folgenden Funktionen ab:

- Authentifizierung

  Nur autorisierte Benutzer sollen Zugriff auf das WLAN bekommen und sich dabei auch ausschließlich mit den gewünschten Access Points verbinden.
- Integrität

  Die übertragenen Daten sollen unverfälscht beim Empfänger ankommen, manipulierte Daten sollen erkannt und verworfen werden.
- Vertraulichkeit

  Unbefugte Dritte sollen nicht in der Lage sein, den Datenverkehr mitzuhören.

Dieses Techpaper gibt eine Übersicht über die Sicherheitsfunktionen, die von den LANCOM Wireless Access Points und LANCOM Wireless Routern unterstützt werden. Weitere Informationen über die zu Grunde liegende Technik erhalten Sie in anderen Techpapern, die konkrete Konfiguration der Funktionen in den LANCOM-Modellen ist im Referenzhandbuch zur jeweiligen LCOS-Version beschrieben.

LANCOM Systems empfiehlt die Ausnutzung **aller** verfügbaren Sicherheitsmechanismen zum Schutz Ihrer drahtlosen Netzwerke. Aktualisieren Sie regelmäßig die Firmware Ihrer LANCOM-Geräte, um alle Sicherheitsfunktionen nutzen zu können.

1 WEP64/128/152

WEP (**W**ired **E**quivalent **P**rivacy) ist die im ursprünglichen WLAN-Standard vorgesehene Funktion zur Verschlüsselung der übertragenen Daten. Die primäre Zielsetzung von WEP ist der Schutz gegen unbefugtes Mithören der Daten.

Dazu werden symmetrische Schlüssel verschiedener Längen eingesetzt. Im Standard verankert sind die Basis-Verschlüsselungsstufen WEP64 und WEP128, mit denen eine Kompatibilität zu allen am Markt erhältlichen, standardkonformen Client-Adaptern gewährleistet ist.

LANCOM Wireless Access Points und Router unterstützen darüberhinaus die Verschlüsselung mit WEP152, bei der ein noch längerer Schlüssel verwendet wird. Alle AirLancer Client-Adapter unterstützen dieses Feature.

Mit WEP wird eine grundlegende Verschlüsselung gewährleistet, die das Netzwerk vor Neugierigen und Unbefugten absichert. Gegenüber Hackern ist zumindest eine leichte Hürde vorhanden, die das Abhören der Daten erschwert.

Da das „Knacken" von nur mit WEP geschützten WLANs allerdings für Profis eine einfache Übung ist, wird dieses Verfahren nur noch für den Heimgebrauch mit regelmäßigem Wechsel der verwendeten WEP-Schlüssel empfohlen.

→Weitere Informationen zu WEP finden Sie auch im LANCOM-Techpaper „WPA und IEEE 802.11i". Anleitungen zum Einstellen der WEP-Verschlüsselung finden Sie im LCOS Referenzhandbuch und in den Benutzerhandbüchern zu den AirLancer Client-Adaptern.

2 MAC-Filterliste (ACL)

Eine einfache, aber effektive Lösung zur Authentifizierung stellt die Verwendung eines MAC-Adress-Filters dar. Dabei werden die MAC-Adressen der authorisierten Client-Adapter im Access Point in eine Liste (ACL - Access Control List) eingetragen, die nur den befugten Benutzern den Zugang zum WLAN erlaubt. In größeren Installationen kann die ACL zentral über einen RADIUS-Server gepflegt werden.

Da allerdings auch die Beschränkung durch eine ACL von einem erfahrenen Hacker überwunden werden kann, sollte diese Funktion nicht als einziger Sicherheitsmechanismus verwendet werden.

→Anleitungen zum Einstellen der ACL finden Sie im LCOS Referenzhandbuch.

3 Closed Network

Jede Zelle in einem Funknetzwerk wird durch einen Netzwerknamen repräsentiert, die SSID (**S**ervice **S**et **I**dentifier). Nur mit der Kenntnis dieser SSID kann sich ein Client-Adapter mit dem Funknetzwerk verbinden.

In der Grundeinstellung erlauben viele drahtlose Netzwerke die Anmeldung mit der SSID „any" und entledigen einen potenziellen Eindringling also von der Notwendigkeit, die SSID des WLANs zu kennen. Dies kann mit der Closed-Network-Funktion verhindert werden. Die Anmeldung mit der SSID „any" wird dabei ausgeschlossen, jeder Benutzer muss die verwendeten SSID genau kennen, um sich am WLAN anmelden zu können.

→Anleitungen zum Einschalten der Closed-Network-Funktion finden Sie im LCOS Referenzhandbuch.

LANCOM
Systems

4 SSID-Broadcast

Die Access Points in einem drahtlosen Netzwerk geben die verfügbaren WLANs über die Ausstrahlung der SSID bekannt. Diese öffentliche Bekanntmachung nutzen Unbefugte gerne als ersten Schritt zum Eindringen in ein fremdes WLAN mit dem „Scannen" der Umgebung, also der ungezielten Suche nach drahtlosen Netzwerken.

Um grundsätzlich zu verhindern, dass ein unbefugter Nutzer ein Netzwerk schon beim Scannen findet, kann der Broadcast der SSID unterdrückt werden. Der Name des WLAN-Netzwerks erscheint nicht mehr in der Ergebnisliste der scannenden Software. Versiertere Scan-Tools können die SSID allerdings trotzdem herausfinden. Da diese Tools aber kein Standardbestandteil von WLAN-Clients sind, stellt das Unterdrücken des SSID-Broadcasts eine weitere Hürde gegen das Eindringen in ein WLAN-Netz dar.

In drahtlosen Netzwerken nach dem IEEE 802.11a-Standard ist das Unterdrücken des SSID Broadcast nicht möglich.

→Anleitungen zum Unterdrücken der SSID finden Sie im LCOS Referenzhandbuch.

5 WPA & IEEE 802.11i

Die zunächst im IEEE 802.11-Standard vorgesehen Datenverschlüsselung nach WEP hat sich im Laufe der Zeit als nicht ausreichend zum Schutz gegen professionelle Angreifer erwiesen. Mit WPA und IEEE 802.11i sind inzwischen deutlich verbesserte Verschlüsselungsmethoden verfügbar, die die bekannten Sicherheitslöcher schließen und mit denen Sie Ihre Funknetzwerke zuverlässig gegen Angriffe schützen.

→Weitere Informationen zu WPA und IEEE 802.11i finden Sie auch im LANCOM-Techpaper „WPA und IEEE 802.11i". Anleitungen zum Einstellen der Verschlüsselung finden Sie im LCOS Referenzhandbuch und in den Benutzerhandbüchern zu den AirLancer Client-Adaptern.

5.1 WPA

WPA schließt mit Hilfe von eines verbesserten, softwarebasierten Verschlüsselungsverfahrens die Sicherheitslücken von WEP. Insbesondere wird nun der dynamische Schlüsselanteil (Initial Vektor) nicht mehr unverschlüsselt übertragen und ist mit 48 Bit doppelt so lang wie bei WEP. Darüber hinaus werden bei WPA die Schlüssel regelmäßig wechselt, es stehen echte Session-Keys auch ohne RADUIS-Server zur Verfügung.

WPA bietet in Zusammenhang mit IEEE 802.1x außerdem eine Möglichkeit der Authentifizierung in Unternehmensnetzwerken.

5.2 IEEE 802.11i

Mit dem hardwarebeschleunigten AES-CCK-Verschlüsselungsalgorithmus wird beim Einsatz von IEEE 802.11i gegenüber WPA ein noch höheres Verschlüsselungsniveau erreicht, das vergleichbar mit VPN ist. Durch die Hardwarebeschleunigung in den LANCOM Access Points und Wireless Routern sowie den AirLancer Client-Adaptern entsteht kein Performanceverlust: Die volle Bandbreite (z. B. bis zu 108 MBit/s im Turbomodus) kann weiterhin genutzt werden.

5.2.1 IEEE 802.11i mit Passphrase

Um in kleinen Netzwerken auf einfache Weise die WLAN-Verbindung mit IEEE 802.11i zu verschlüsseln, wird eine „Passphrase" für jedes drahtlose Netzwerk eingerichtet. Diese wird im Access Point und im Client-Adapter fest eingetragen. Aus dieser Passphrase wird pro Verbindung und Zeitraum der Schlüssel für die Verschlüsselung einer WLAN-Verbindung berechnet.

Die verwendeten Passphrases sollen idealerweise möglichst lang und kompliziert aufgebaut sein, nur den relevanten Personen zugänglich sein und regelmäßig gewechselt werden.

Schwachpunkt ist der 'menschliche' Faktor beim Verteilen und Verwalten der Passphrase. Ein regelmäßiger Wechsel der Passphrase und ihr möglichst komplizierter Aufbau werden empfohlen, um diese Schwäche zu verringern.

→Die Verschlüsselung mit Passphrases nach IEEE 802.11i ist ab LCOS-Version 3.50 verfügbar.

5.2.2 IEEE 802.11i für Point-to-Point-Verbindungen

Mit der Einführung von IEEE 802.11i können nun erstmals auch Point-to-Point-Strecken (P2P) direkt verschlüsselt werden, es ist keine zusätzliche VPN-Abschirmung mehr erforderlich. Durch die Hardwarebeschleunigung in den LANCOM- und AirLancer-Geräten kann diese Verschlüsselung ohne Performance-Verlust realisiert werden.

→Die Verschlüsselung mit Passphrases nach IEEE 802.11i für P2P-Verbindungen ist ab LCOS-Version 4.00 verfügbar.

6 IPsec over WLAN

Beim Einsatz eines VPN-Gateways im Access Points kann die WLAN-Strecke alternativ zu IEEE 802.11i auch über IPSec verschlüsselt werden. Point-to-Point-Strecken können auch auf diese Weise absolut sicher vor Angriffen gemacht werden.

Die Beherrschung der komplizierten Technik fällt mit den LANCOM-Geräten leicht. Assistenten und Management-Tools stehen für eine schnelle Konfiguration zur Verfügung.

LANCOM™ Techpaper
Überblick WLAN- Sicherheitsfunktionen

→Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt IPSec over WLAN nach wie vor als die sicherste WLAN-Absicherung.

→Die Absicherung mit IPsec over WLAN ist in den LANCOM-Modellen 18x1 Wireless (A)DSL und 3550 Wireless möglich.

7 IEEE 802.1x

Mit dem Protokoll IEEE 802.1x wird im Zusammenspiel mit IEEE 802.11i in großen Netzen die Möglichkeit geboten, für jede einzelne WLAN-Verbindung eine Authentifizierung durchzuführen. Der Austausch von Schlüsseln oder Passphrases ist dabei nicht nötig.

Das Aufsetzen einer IEEE 802.1x Infrastruktur setzt fortgeschrittene Netzwerkkenntnisse, einen CA-Server und einen IEEE 802.1x -Server voraus. Daher ist diese Anwendung vor allem in großen Firmennetzwerken sinnvoll.

→Weitere Informationen zu IEEE 802.1x finden Sie auch im LANCOM-Techpaper „IEEE 802.1x".

→Die Verschlüsselung nach IEEE 802.11i mit IEEE 802.1x ist ab LCOS-Version 3.52 verfügbar.

8 Public Spot

Mit der LANCOM Public Spot Option ist es möglich, eine Authentifizierung bei der Nutzung des WLAN-Netzes zu erreichen. Allerdings wird im Gegensatz zu IEEE 802.1x anschließend keine verbindungsabhängige Verschlüsselung veranlasst. Die LANCOM Public Spot Option ist daher gezielt zur Nutzungskontrolle, Abrechnung und Überwachung einsetzbar.

Die LANCOM Public Spot Option kann auch in kleinen Netzwerkumgebungen einfach realisiert werden, weitere Server sind nicht zwingend erforderlich. Mit Hilfe eines RADIUS-Servers und einer externen Abrechnungssoftware kann sie bis auf eine fast beliebige Größe ausgebaut werden.

9 LEPS

Mit LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Fehlerquellen beim Verteilen der Passphrase vermeidet.

Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zugeordnet – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen.

Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA oder 802.11i verwendet werden, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden.

LEPS funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installationen ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

→Die Einrichtung von individuellen Passphrases pro MAC-Adresse ist ab LCOS-Version 4.00 verfügbar.

10 MultiSSID

Mit der MultiSSID-Funktion ist es möglich, auf einer physikalischen WLAN-Schnittstelle bis zu acht logische WLAN-Netze zu realisieren – jede mit einer eigenen SSID. Auf diese Weise können von einem Access Point mehrere WLAN-Netzwerke aufgespannt werden, für die unterschiedliche Sicherheitseinstellungen gelten. Damit kann ein Access Point gleichzeitig ein völlig offenes WLAN und ein z. B. über IEEE 802.11i geschütztes WLAN verwalten.

→Die Verwendung von MultiSSID ist ab LCOS-Version 3.42 verfügbar.

→Weitere Informationen zu MultiSSID finden Sie auch im LANCOM-Techpaper „MultiSSID".

11 VLAN

Mit der Verwendung von virtuellen Netzwerken (VLANs) kann die Abschirmung von logischen WLANs bis in das kabelgebundene LAN „verlängert" werden. Dabei wird jedem logischen Funknetzwerk ein bestimmtes virtuelles Netz zugeordnet. Der Datenverkehr aus einem besonders sicherheitssensiblen Funknetzwerk kann so auch innerhalb des normalen LANs gegen unbefugte Mithörer abgeschirmt werden.