Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 82 (2004)

Heft: 3

Artikel: Sicherheit in Wireless LANs

Autor: Sellin, Rüdiger

DOI: https://doi.org/10.5169/seals-876842

Sicherheit in Wireless LANs

RÜDIGER SELLIN **Private drahtlose Netze (Wireless Local Area Networks, WLANs) erfreuen sich zunehmender Beliebtheit. Fallende Preise für WLAN-Equipments tragen dazu bei, dass immer mehr Firmen und Privatpersonen eigene WLANs einrichten. Der vorliegende Beitrag zeigt auf, was beim Aufbau von privaten WLANs nach IEEE 802.11x zu beachten ist.**

Der bewährte Standard 802.11b hilft wesentlich mit, dass Endgeräte wie Laptops, PDAs und Drucker mit den WLAN-Sendern praktisch uneingeschränkt untereinander kommunizieren können. Weitere Standards beispielsweise für mehr Bandbreite oder verbesserte Sicherheit existieren bereits oder stehen kurz vor der Einführung. Generell gibt es besonders bei der WLAN-Security neue Entwicklungen.

WLAN-Standards nach 802.11x

Praktisch alle WLANs arbeiten auf Basis verschiedener Standards des amerikanischen Standardisierungsgremiums IEEE (Tabelle 1). Sie bieten mit einer Bandbreite von 11 bis 54 Mbit/s einen komfortablen mobilen Zugang zu drahtlosen lokalen Datenkommunikationsnetzen. Grundsätzlich kann es sich dabei entweder um private und Firmennetze oder um kommerzielle Hotspots an öffentlich zugänglichen Plätzen handeln. Basierend auf 802.11a (5-GHz-Band) oder 802.11g (2,4-GHz-Band) ist eine Reihe von Produkten mit höheren Bandbreiten zunehmend verfügbar. Im privaten Sektor (Firma, Campus, zu Hause) lösen diese die erste WLAN-Generation (802.11b) Schritt für Schritt ab. Für den zweiten Bereich, die PWLANs (Public Wireless LANs), wird eine ähnliche Entwicklung erwartet, wobei beispielsweise

Arbeitsgruppe	Arbeitsgebiet
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 regionenspezifische Regulatorien
802.11e	QoS- und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h (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 DFS und TPC
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES, 802.1x)

Tabelle 1. WLAN-Standards aus dem IEEE (Institute of Electrical and Electronic Engineers). Abkürzungen: AES: Advanced Encryption Standard, DFS: Dynamic Frequency Selection, TPC: Transmit Power Control.

Swisscom Eurospot neben 802.11b bereits den Standard 802.11g einsetzt.

Noch zu nachlässig bezüglich Sicherheit

Leider wird gerade in privaten WLANs Sicherheitsaspekten oft zu wenig Aufmerksamkeit gewidmet. Sicherheitslösungen sind zwar verfügbar, kommen aber nur selten mit der nötigen Konsequenz zum Einsatz. Untersuchungen haben ergeben, dass die herstellerseitig vorgesehenen Schutzmechanismen kaum oder gar nicht genutzt werden. Bisweilen zeigen sogar die Hersteller selbst ein naives Verhalten. So waren an der letztjährigen CeBIT fast 90% der bei den Ausstellern auf den Messeständen installierten WLANs ungeschützt. Mit der simplen Eingabe des ab Werk vorgesehenen Passworts konnten die Tester ungehindert eindringen. In den USA ist es zu einer Art Volkssport unter Hackern geworden, ungeschützte WLANs ausfindig zu machen («War Driving») und die betreffenden Häuser von aussen mit Kreide zu markieren («War Chalking»). Vermehrt werden auch in Deutschland die dazu nötigen Tools in einschlägigen Computerzeitschriften per CD-ROM verkauft. Auf diese Weise kann jeder WLAN-Pirat spielen – Laptop mit WLAN-Karte und die passende CD-ROM genügen.

Bei der Evaluation der Schutzmechanismen für WLANs wird deutlich, dass der Begriff Sicherheit kaum durchgängig gleich ausgelegt wird. Zu Zeiten des analogen Mobilfunks wurde unter Sicherheit oft Abhörsicherheit (Vertraulichkeit) verstanden. In WLANs müssen jedoch darüber hinaus die Zugangskontrolle (Zugang fremder Stationen) und die Datenintegrität (Manipulation oder Verfälschung übertragener Daten) gewährleistet sein. Zur Sicherstellung der Abhörsicherheit wird als Verschlüsselungsmechanismus in den meisten Fällen immer noch WEP (Wired Equivalent Privacy) eingesetzt. Ohne zusätzlichen Schutz, wie ihn praktisch alle PWLAN-Betreiber bieten (siehe Kasten), muss WEP sowohl für Firmen als auch für private Haushalte als zu schwach eingestuft werden. Die Hauptschwächen des WEP-Verfahrens sind die zu kurzen und dazu statischen Schlüssel, die regelmässig manuell geändert werden müssen. Der Schlüssel war ursprünglich nur 40, dann 64 Bit lang und wurde mittlerweile auf 128 Bit (WEP2) verlängert. Zu alledem ist der Einsatz von WEP optional und muss daher explizit eingeschaltet werden.

Sicherheitsstufen und Massnahmen

Aufgrund der beschriebenen und weiteren Sicherheitsmängel musste die gesamte WLAN-Sicherheitsarchitektur im IEEE neu definiert werden. Die dort für den neuen Standard verantwortliche Task Group i definierte ein neues Security Framework, um WEP zu ersetzen und die WLAN-Security umfassend zu erweitern. Weil die internationale Standardisierung aber generell ein eher langwieriger Prozess ist und die Zeit drängte, kamen Zwischenlösungen auf den Markt. Hier hat sich besonders das Wi-Fi-Konsortium (Wireless Fidelity) hervorgetan, eine nordamerikanische Herstellervereinigung. Aus der WiFi-«Küche» kamen TKIP (Temporal Key Integrity Protocol) und WPA (WiFi Protected Access) auf den Markt. Im Vergleich zu WEP bieten die Lösungen bereits wesentliche Verbesserungen. So eliminiert TKIP zwei der Hauptprobleme von WEP, nämlich den statischen Schlüssel und die fehlerhafte Integritätssicherung. TKIP und WPA dürfen als Vorstufen des neuen IEEE-Standards 802.11i betrachtet werden. Dessen Verabschiedung wird im Verlauf dieses Jahrs erwartet. 802.11i gewährleistet neben der Vertraulichkeit der Daten auch deren Authentizität und Integrität, automatisiert die Schlüsselverwaltung und ermöglicht die Unabhängigkeit von spezifischen Verschlüsselungsmechanismen und -algorithmen. Darüber hinaus sind auch Mechanismen für die gegenseitige Authentifizierung von Access Points und Endgeräten vorgesehen. Um eine sehr hohe Vertraulichkeit zu erreichen, wird mit 802.11i der Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) eingesetzt, mit dem die bislang höchste Sicherheitsstufe erklommen wurde (Tabelle 2). Bei Neubeschaffungen ist unbedingt darauf zu achten, dass das WLAN-Equipment mit SW-Updates, das heisst ohne Wechsel der Hardware, auf den Stand der neusten Sicherheitsstandards gebracht werden kann.

Für den Aufbau grösserer privater WLANs kommen Authentifizierungslösungen nach 802.1x in Frage, ein Portfolio verschiedener Optionen, die den Zugang zu Netzwerken aller Art regeln. Die Verknüpfung von 802.1x mit 802.11i löst praktisch alle Probleme von WEP. Über EAP (Extensible Authentication Protocol) und TLS (Transport Layer Security) findet eine beidseitige Authentifizierung zwischen dem mobilen Endgerät und dem Access Point

Sicherheitsniveau	Verschlüsselung	Authentifizierung
Eher tief	WEP	MAC
Sicher	TKIP (802.11i)	LEAP / EAP-TLS (802.1x)
Sehr sicher	WPA (802.11i)	PEAP (802.1x)
Extrem sicher	AES	PEAP und OTP (802.1x)

Tabelle 2. WLAN-Sicherheitsstandards.

Massen begeistern.

X'04

Die Messe für Marketing, Kommunikation und Event
24. 25. 26. August Messe Zürich

www.xpage.ch

SWISS MARKETING

mch messe schweiz

Die einzige Schweizer Marketing-Messe präsentiert die neusten Ideen und beliebtesten Mittel, um einen Event zum Ereignis zu machen: Jetzt, da die Wirtschaft wieder in Schwung kommt. Ein Must für Entscheider, Marketing-Profis und alle, die es werden wollen. **Öffnungszeiten:** 24. August 10.00–18.30 Uhr, **25. August 10.00–20.00 Uhr,** 26. August 10.00–17.30 Uhr

Reed Exhibitions

Reed Messen (Schweiz) AG, Bruggacherstrasse 26, CH-8117 Fällanden, Telefon +41 (0)1 806 33 55, Fax +41 (0)1 806 33 43, E-Mail: info@xpage.ch

mittels Zertifikaten oder OTPs (One Time Passwords) statt. Die Zertifikate werden aus Sicherheitsüberlegungen auf Smartcards oder USB-Tokens abgelegt. Dieses Vorgehen folgt einem ähnlichen Ansatz wie beim Aufbau einer verschlüsselten Verbindung über die SSL (Secure Socket Layer) zwischen einem Browser und einem Webserver. Verschiedene herstellerspezifische EAP-Ansätze sind beispielsweise LEAP (Lightweight EAP) von Cisco oder PEAP (Protected EAP), eine gemeinsame Lösung von Microsoft, Cisco und RSA. Weitere EAP-Lösungen unter Einsatz der SIM-Karten von GSM-Mobiltelefonen sind ebenfalls im Einsatz, insbesondere bei PWLAN-Anbietern.

Praktische Tipps

Bei der Planung

- WLAN wenn möglich in ein geschlossenes Virtual Private Network (VPN) einbinden. VPNs werden für den geschützten Zugriff auf Firmennetze über das Internet eingesetzt. Über ein VPN kann die Authentifizierung und die Verschlüsselung der Daten bereits heute auf hoher Sicherheitsstufe erfolgen.
- WLAN Access Points (AP) ausserhalb der Firewall oder in einer eigenen Domäne einrichten, damit die Zugriffskontrolle der Firewall auf das interne LAN erhalten bleibt.

Bei der Einrichtung

- Herstellerseitige Voreinstellungen (z. B. Passwörter, Schlüssel) ändern.
- Herstellerseitige Verschlüsselung nutzen. Auch WEP ist besser als gar kein Schutz und erschwert einen Einbruchsversuch.
- Dynamic Host Routing Protocol (DHCP) abschalten. DHCP ordnet Arbeitsstationen im LAN eine IP-Adresse und weitere Parameter auf Anfrage dynamisch zu. Das Abschalten von DHCP erschwert das Vortäuschen einer echten Identität auf OSI-Schicht 3 und somit das Eindringen.

Im Betrieb

- WEP-Schlüssel regelmässig ändern. Durch Verwendung des immer gleichen Schlüssels steigt die Wahrscheinlichkeit, ihn zu knacken.
- SSID – die ID des WLAN Access Point (AP) – regelmässig ändern; die meisten APs broadcasten ihre SSID. Falls möglich, diese Funktion deaktivieren, weil sie das Auffinden eines AP erleichtert.
- Nicht zugelassene MAC-Adressen filtern. Viele APs speichern die in WLAN zugelassenen MAC-Adressen (dies ist die ID z. B. einer WLAN-Karte im Endgerät). Eine Anmeldung im WLAN gelingt nur über eine gültige MAC-Adresse. Liste besonders schützen, womit das Lesen und Ändern nur durch den Netzwerkadministrator möglich ist.
- WLAN beobachten. Logfile regelmässig checken und Intrusion-Detection-Systeme – falls vorhanden – nutzen. Unerlaubte Aktivitäten im Netz fallen so schneller auf.

Sicherheit bei Swisscom Mobile

Auch Swisscom Mobile als grösster Betreiber eines öffentlichen PWLAN-Service mit über 500 Hotspots in der Schweiz hat Überlegungen zur Sicherheit des Datenverkehrs angestellt. Die Datenübertragung zwischen den mobilen Endgeräten und dem Access Point (Luftschnittstelle) ist wie bei allen anderen Anbietern nicht mit dem in 802.11b beschriebenen Verfahren Wired Equivalent Privacy (WEP) verschlüsselt. WEP setzt voraus, dass die Benutzer dem WLAN-Betreiber bekannt sind. Diese Voraussetzung ist bei einem öffentlichen WLAN-Anbieter nicht erfüllt. Jeder Benutzer, der über ein PWLAN auf sein Firmennetzwerk zugreift, sichert diese Verbindung daher entsprechend beispielsweise über IP Sec. Für die Authentisierung und für die Datensicherheit (Datenintegrität und Verschlüsselung) setzen Firmen entsprechende VPN-Lösungen ein (z. B. SecuRemote mit CheckPoint Firewall-1). Der Zugriff auf Web, E-Mail und das Surfen auf dem Internet ist oft nicht verschlüsselt und ein Abhören dieser Daten über die «Luftschnittstelle» war unter gewissen Umständen möglich.

Damit eine gleich gute Sicherheit vergleichbar mit ADSL-Internet erreicht wird, ermöglicht Swisscom Mobile dem Kunden eine Verschlüsselung des Datenverkehrs mittels IPsec vom Client bis zum PWLAN-Datacenter. Zudem muss sich jeder PWLAN-Benutzer mit einem Passwort authentisieren, das er mit seinem Handy per SMS anfordert (festes NATEL®-Abo mit PWLAN-Zusatz) oder auf der Rückseite seiner Guthabenkarte nach dem Aufrubbeln der entsprechenden Fläche ablesen kann. Diese Login-Prozedur erfolgt über die Secure Socket Layer (SSL). Noch in diesem Jahr wird die Authentisierung mittels SIM-Karte möglich sein. Sie basiert auf dem 802.1x Standard und erlaubt das schnelle, sichere und automatische Anmelden des Kunden bei Public Wireless LAN von Swisscom Mobile. Gleichzeitig wird der Datenverkehr über die Luftschnittstelle verschlüsselt übermittelt.

Fazit

WLANs sind heute in vielen Unternehmen und Privathaushalten im Einsatz. Der Komfortgewinn der kabellosen Kommunikation hat gewisse Sicherheitsrisiken zur Folge. Daher müssen Sicherheitsfragen Priorität vor Aspekten der eigentlichen Kommunikation eingeräumt werden. Unter entsprechender Berücksichtigung der Vertraulichkeit, Zugangkontrolle und Datenintegrität lassen sich die gewählten Lösungen in bestehende IT-Systeme integrieren. Und neben technischen Fragen sollte auch die Organisation der Sicherheit etwa mit dem Aufbau des entsprechenden Know-hows Vorrang geniessen – und zwar nicht erst dann, wenn ein Einbruchsversuch bereits stattgefunden hat. Damit wird ein WLAN auch längerfristig ein echter Gewinn, beispielsweise durch neue Arbeitsformen, die mit WLANs erst möglich werden. ■

Rüdiger Sellin, Dipl.-Ing., PR-Manager, Marketing Communications, Swisscom Mobile und freier Autor