Sicherheit von Wireless LAN

Attacken und Schutzmassnahmen

WLAN – Wireless LAN – eröffnen völlig neue Freiheiten in der mobilen und flexiblen Datenkommunikation. Die drahtlose Übertragung bringt aber auch beträchtliche Gefahren mit sich. In diesem Beitrag werden zwei Möglichkeiten beschrieben, wie Angreifer in verschlüsselte Netze eindringen können. Glücklicherweise existieren Schutzmassnahmen, mit denen WLAN mit vertretbarem Aufwand zuverlässig vor unbefugten Zugriffen geschützt werden können.

Andreas Steffen

Wireless LAN sind Allgemeingut geworden. Das Wi-Fi-Label[1)] der WLAN-Hersteller garantiert, dass die Geräte interoperabel gemäss dem IEEE 802.11-WLAN-Standard sind. Die neueren Rechnerbetriebsysteme bieten komfortable Plug-and-Play-Unterstützung bei der Installation und Konfiguration, so dass auch Laien ein drahtloses Netzwerk in Minuten aufsetzen und in Betrieb nehmen können. Viele Benutzer sind sich jedoch nicht bewusst, dass ein fundamentaler Unterschied zwischen einem verdrahteten LAN und einem WLAN besteht: Im Gegensatz zu Ersterem ist der Sende- und Empfangsbereich eines WLAN nicht auf die eigenen vier Wände beschränkt, sondern kann – bedingt durch die drahtlose Ausbreitung der durch den Access Point im 2,5-GHz- und neuerdings auch im 5-GHz-Bereich abgestrahlten Radiowellen – unter Umständen bis zu einer Entfernung von 100 bis 200 Metern problemlos empfangen werden (Bild 1).

War-Driving

Die Möglichkeit, ein WLAN aus sicherer Distanz unbemerkt abzuhören, hat weltweit zu einem neuen Volkssport geführt: dem War-Driving. Ausgerüstet mit einem Laptop, einer WLAN-Aussenantenne und einem GPS-Navigationssystem fahren die passionierten War-Driver in der Gegend herum, zeichnen alle gefundenen drahtlosen Netzwerke in einer Landkarte ein und publizieren dann die Standorte auf einschlägigen Webseiten. Aus solchen Erhebungen weiss man, dass immer noch über 70% Prozent aller WLAN unverschlüsselt betrieben werden – eine offene Einladung für jedermann, sich in ein Netzwerk einzuklinken, mitzusurfen oder noch viel schlimmer: Dateien zu entwenden oder böswillig zu verändern. Als Ableger der War-Driving-Kultur hat sich das War-Chalking entwickelt. Die in Bild 2 gezeigten Kreidesymbole, die an Hauswände oder auf das Trottoir gemalt werden, machen auf das Vorhandensein eines Access Points aufmerksam, so dass der weit gereiste Tourist jederzeit zum Nulltarif Zugriff auf das Internet hat.

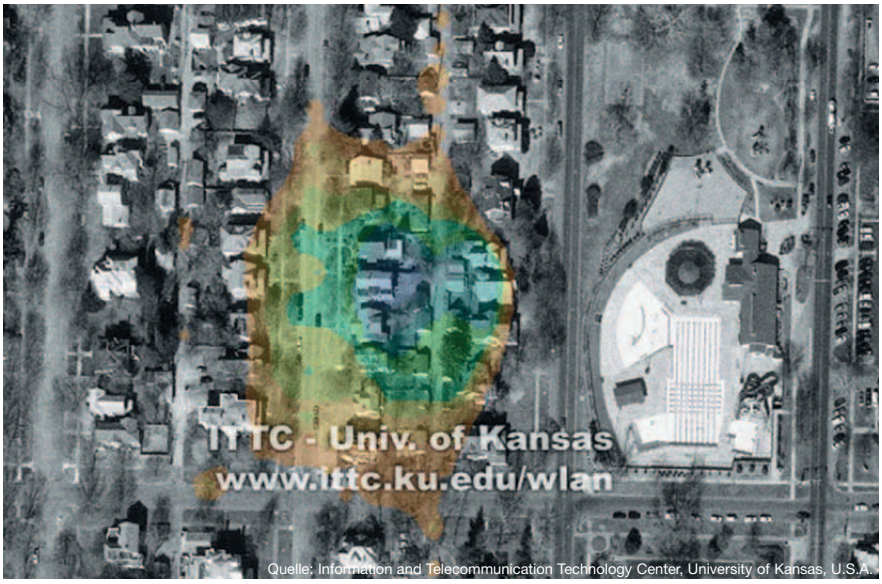


Bild 1 Abstrahlungscharakteristik eines WLAN Access Points in einem Wohnquartier

Wired Equivalent Privacy (WEP)

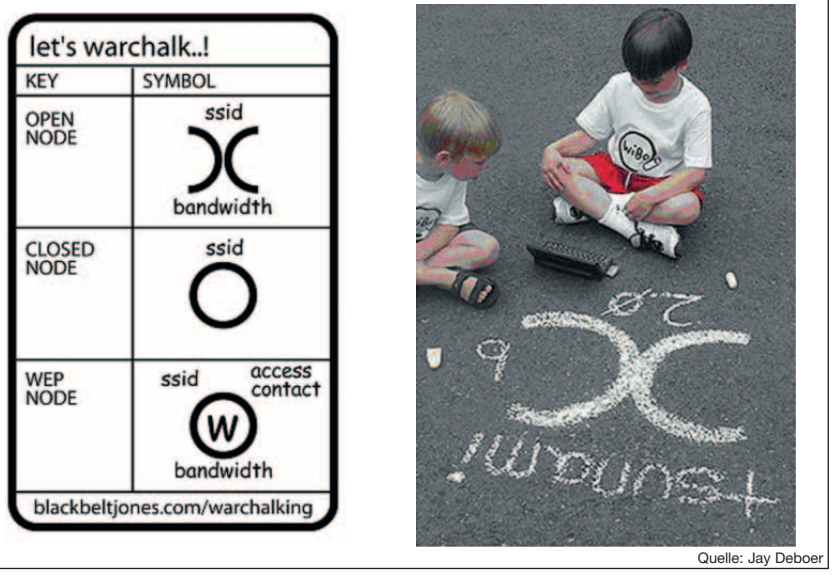
Wie die Statistik zeigt, werden die meisten WLAN-Netzwerke immer noch ohne jeglichen Schutz gegen Zugriff von aussen aufgesetzt. Dabei sah schon die Urausgabe des IEEE-802.11-WLAN-Standards von 1997 einen Verschlüsselungsmechanismus namens Wired Equivalent Privacy (WEP) vor, welcher, wie der Name sagt, den gleichen Vertraulichkeitsgrad wie bei der Kommunikation über eine Telefonleitung bietet, aber keine kryptografisch starke Sicherheit garantieren soll. Die Schlüssellänge wurde im Standard ursprünglich auf 40 Bit begrenzt, um den damaligen Exportrestriktionen der USA betreffend starker Kryptografie zu genügen. Damit waren amerikanische Geheimdienste wie zum Beispiel die National Security Agency (NSA) in der Lage, WEP-Schlüssel in relativ kurzer Zeit zu knacken. Dank der Zunahme der verfügbaren Rechenleistung über die letzten Jahre hinweg kann man heute mit relativ wenig Aufwand sämtliche 2^{40} Schlüsselkombinationen per «Brute Force» durchprobieren und so innerhalb Stunden bis Tagen solche kurzen WEP-Schlüssel knacken. Seit der Aufhebung der US-Exportschranken vor einigen Jahren können 104 Bit lange WEP-Schlüssel eingesetzt werden. Der

Was sind WLAN?

Mit WLAN-Technologien können Benutzer drahtlose Verbindungen innerhalb eines lokalen Bereichs herstellen (z.B. in einem Firmen- oder Campusgebäude oder einem öffentlichen Gebäude, z.B. einem Flughafen). Für den Betrieb von WLAN gibt es zwei unterschiedliche Methoden. Bei fest installierten WLAN stellen drahtlose Stationen (Geräte mit Funknetzwerkkarten oder externen Modems) Verbindungen mit drahtlosen Zugriffspunkten (Access Points) her, die Brücken zwischen den Stationen und dem vorhandenen Netzwerkbackbone bilden. Bei Peer-to-Peer (ad hoc) WLAN können mehrere Benutzer ohne die Verwendung von Zugriffspunkten innerhalb eines begrenzten Bereichs, zum Beispiel einem Konferenzraum, ein temporäres Netzwerk bilden, wenn kein Zugriff auf Netzwerkressourcen erforderlich ist.
1997 bestätigte das IEEE den Standard 802.11 für WLAN, der eine Datenübertragungsrate von 1 bis 2 Mbit/s (Megabit pro Sekunde) festlegt. Unter 802.11b, dem neuen gültigen Standard, beträgt die maximale Datenübertragungsrate 11 Mbit/s über ein Frequenzband von 2,4 GHz. Weitere neue Standards sind 802.11a, bei dem die Daten mit maximal 54 Mbit/s über ein Frequenzband von 5 GHz übertragen werden, so wie 802.11g, welcher die gleiche Datenrate im 2,4-GHz-Band ermöglicht. – Quelle: Microsoft Windows XP, Übersicht über drahtlose Netzwerke

damit riesige verfügbare Schlüsselraum von 2^{104} möglichen Schlüsseln schien eine ausreichend hohe Sicherheit zu bieten und wurde deshalb von allen neueren WLAN-Produkten unterstützt.

Das Grundprinzip der WEP-Verschlüsselung ist in Bild 3 grafisch dargestellt. Es wird standardmässig der RC4-Stream-Cipher[2] der Firma RSA Security[3] eingesetzt. Ein Pseudo-Zufallsgenerator wird vor dem Senden jedes WLAN-Pakets mit einem 64 Bit, respektive 128 Bit langen Schlüssel geladen, der sich aus einem 24 Bit langen, sich mit jedem Paket ändernden Initialisierungsvektor, plus dem 40 Bit, respektive 104 Bit langen geheimen WEP-Schlüssel zusammensetzt. Nach dieser Initialisierung kann ein beliebig langer pseudo-zufälliger Bitstrom generiert werden, der Bit für Bit mittels einer XOR-Funktion (Exklusiv-Oder) zu den Nutzdaten addiert wird. Die verschlüsselten WLAN-Pakete sehen dann wie Zufallsdaten aus und es kann nicht mehr auf den ursprünglichen Klartext geschlossen werden. Der jeweilige Initialisierungsvektor muss mit dem verschlüsselten Paket übertragen werden, damit der Empfänger den gleichen Schlüsselstrom erzeugen und durch nochmalige Anwendung der XOR-Funktion aus den verschlüsselten Daten wieder den Klartext gewinnen kann. Gemäss IEEE-802.11-Standard können in einem Netzwerk vier verschiedene WEP-Schlüssel verwendet werden. Das Key-ID-Feld teilt jeweils der Gegenstelle mit, mit welchem Schlüssel ein WLAN-Paket verschlüsselt wurde. In der Praxis wird in einem Netzwerk aber meistens nur ein einziger WEP-Schlüssel verwendet.



Quelle: Jay Deboer

Bild 2 War-Chalking

Spezielle Kreidesymbole an Hauswänden oder auf dem Trottoir machen auf das Vorhandensein eines WLAN Access Point aufmerksam und geben die Zugangsparameter an.

Abbildung von Passwörtern auf WEP-Schlüssel

Bild 4 zeigt die WEP-Schlüsseleingabe von Windows XP, das die Konfiguration von WLAN-Karten herstellerübergreifend unterstützt. Normalerweise wird aus exakt 5, bzw. 13 ASCII-Zeichen durch eine direkte Abbildung des 8-Bit-Codes der 40 Bit, bzw. 104 Bit lange WEP-Schlüssel gebildet, wie dies in der Tabelle dargestellt ist.

Diese Art der Schlüsselbildung hat zur Folge, dass der genutzte Schlüsselraum stark eingeschränkt wird, weil nur über die Tastatur eingebbare Zeichen im Passwort enthalten sein können und deshalb nicht alle 256 Kombinationen des 8-Bit-ASCII-Codes verwendet werden. Nur die wenigsten Benutzer wissen, dass Windows XP als Alternative die direkte Eingabe des WEP-Schlüssels als Folge von 10, respektive 26 hexadezimalen Zeichen erlaubt.

Gewisse herstellerspezifische Konfigurationstools bilden den WEP-Schlüssel aus dem eingegebenen Passwort mittels einer zusätzlichen Transformationsfunktion. Dabei wird meist Keygen für 40-Bit-WEP-Schlüssel und die MD5-Hashfunktion für 104-Bit-Schlüssel verwendet. Diese Transformationen erhöhen die Schlüsselstärke aber nur, falls mehr als 5, respektive 13 Passwortzeichen eingegeben werden, und verschleiern andererseits die ungenügende Sicherheit, falls weniger Zeichen eingegeben werden.

Wörterbuchattacke auf schwache Passwörter

Ein Tool, das WEP-Schlüssel knacken kann, heisst WepAttack und wurde im Oktober 2002 durch die Studenten Dominik Blunk und Alain Girardet im Rahmen ihrer Diplomarbeit [1,2] an der Zürcher Hochschule Winterthur (ZHW) entwickelt. Das Verfahren beruht auf einer Wörterbuchattacke, die im Jahr 2001 von Tim Newsham [3] beschrieben, aber bisher noch nicht in die Praxis umgesetzt

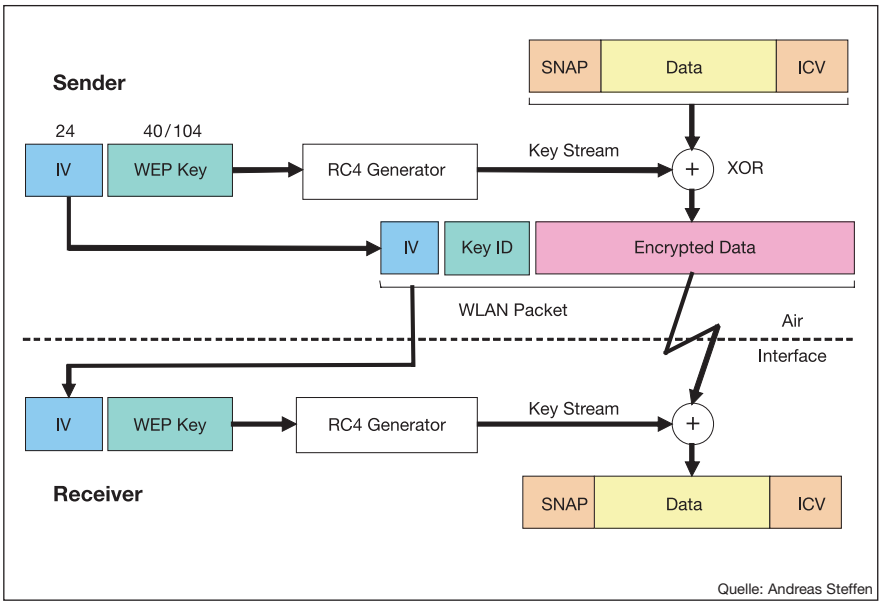


Bild 3 Funktionsweise der WEP-Verschlüsselung

Jedes zu übertragende WLAN-Paket wird zuerst mit einer ICV-Checksumme versehen und dann mittels einer XOR-Funktion Bit für Bit mit einem durch den RC4-Algorithmus erzeugten pseudo-zufälligen Schlüsselstrom kombiniert und dadurch verschlüsselt. Der RC4-Pseudo-Zufallsgenerator wird zu Beginn jedes WLAN-Pakets mit dem geheimen WEP-Key und einem ständig wechselnden Initialisierungsvektor (IV) neu initialisiert. Der IV wird mit übertragen, damit der Empfänger den eigenen RC4-Generator mit dem gleichen Startwert initialisieren und so mit einem identischen Schlüsselstrom durch bitweises XOR aus den verschlüsselten Daten wieder das Klartextpaket erhalten kann. Dank der ICV-Summe kann leicht überprüft werden, ob die Entschlüsselung erfolgreich war.

wurde. WepAttack läuft unter Linux und kann von sourceforge.net [4] runtergeladen werden.

Wie funktioniert nun WepAttack? Das Tool basiert auf der bekannten Tatsache, dass viele Benutzer schwache Passwörter als Ausgangspunkt für ihren WEP-Schlüssel wählen. Das menschliche Gedächtnis ist unzuverlässig und der Rufname der Hauskatze oder des Meerschweinchens ist deshalb naheliegend. Durch Ausprobieren von mehreren Millionen Passwörtern, die einem mehrsprachigen Wörterbuch entnommen werden, kommt WebAttack häufig schon innerhalb einer Stunde zum Ziel. Dazu wird nur ein einziges verschlüsseltes WLAN-Paket benötigt. Da die RC4-Entschlüsselung genau gleich funktioniert wie die Verschlüsselung, kann durch bitweise XOR-Verknüpfung der RC4-Pseudo-Zufallsfolge mit den verschlüsselten Daten wieder das ursprüngliche Klartextpaket erhalten werden. Der RC4-Generator wird nun durch WepAttack solange mit einer Abfolge von möglichen Passwörtern geladen, bis entweder der richtige WEP-Schlüssel gefunden wird oder das gesamte Wörterbuch ergebnislos durchsucht wurde.

Zwei Eigenheiten im Aufbau der WLAN-Pakete erlauben es schnell und eindeutig festzustellen, ob das richtige Passwort gefunden wurde. Bei eingeschalteter WEP-Verschlüsselung wird mit jedem Paket ein Integrity Check Value (ICV) übertragen, welcher als CRC-32-Prüfsumme über die Nutzdaten gebildet wird. Ist diese 32-Bit-Checksumme nach der Entschlüsselung korrekt, so kann mit sehr hoher Wahrscheinlichkeit angenommen werden, dass der richtige Schlüssel gefunden wurde. Da jedoch für jedes getestete Passwort das gesamte WLAN-Paket zuerst entschlüsselt werden muss, um die Prüfsumme berechnen zu können, müsste sehr viel Rechenleistung für die Attacke aufgebracht werden. Dank der zweiten Eigenheit kann man sich diesen Aufwand bei den meisten falschen Passwörtern sparen. Ein IEEE-802.11-WLAN-Paket besitzt nämlich auf der OSI-Schicht 2 immer einen IEEE 802.2 Sub Network Access Protocol (SNAP) Header, dessen erste sechs Bytes bei der Übertragung von IP- oder ARP-Paketen die konstanten HEX-Werte AA AA 03 00 00 00 besitzen. Beim Ausprobieren eines WEP-Schlüssels wird nun zuerst nur das erste Byte entschlüsselt und auf den Wert AA überprüft. Falls dies zutrifft, und dies ist im Mittel nur alle 256 Passwortkombinationen der Fall, hat man einen möglichen Kandidaten gefunden, der nun durch schrittweises Entschlüsseln des zweiten bis sechsten Bytes und schliesslich dem Berechnen der gesamten ICV-Prüfsumme weiter getestet werden kann. Sobald aber ein SNAP-Byte nicht übereinstimmt, kann der Test sofort abgebrochen und zum nächsten Passwort übergegangen werden. Unter der Annahme, dass die Entschlüsselung eines WLAN-Paktets ungefähr nochmals so viel Zeit in Anspruch nimmt wie die vorgängige Initialisierung des RC4-Generators mit dem zu testenden WEP-Schlüssel, können durch den vorzeitigen Abruch doppelt so viele Schlüssel pro Zeiteinheit getestet werden.

WepAttack kann mit einem Passwort-Cracker-Tool, wie zum Beispiel dem bekannten John the Ripper [5] gekoppelt werden. Damit hat man zusätzlich die Möglichkeit, eine fast unbegrenzte Anzahl von Regeln auf die Einträge eines Wörterbuchs anzuwenden. Passwörter können ganz oder teilweise in Grossbuchstaben gesetzt, rückwärts geschrieben oder mit Zahlen und/oder Sonderzeichen am Wortanfang oder Wortende ergänzt werden. Dadurch vervielfacht sich natürlich die Anzahl der Passwörter, die getestet werden können. Allerdings wächst auch der Rechenaufwand proportional mit der Anzahl der Regeln. Eine Wörterbuchattacke mit 2 Millionen Wörtern und zum Beispiel 50 John-the-Ripper-Regeln kann in ungefähr einer Stunde durchgeführt werden.

Sniffen von WLAN-Netzwerken

Um WepAttack einsetzen zu können, muss vorgängig mit einem Netzwerk-Sniffer mindestens ein verschlüsseltes Paket des zu attackierenden WLAN aufgezeichnet werden. Grundsätzlich sind dazu alle Sniffer geeignet, welche die Daten im PCAP-Format abspeichern können. Darunter fallen Kismet, tcpdump oder Ethereal. Es ist darauf zu achten, dass ein Sniffer eingesetzt wird, der das ICV-Feld nicht abschneidet, da sonst WepAttack die CRC-32-Checksumme nicht überprüfen kann. Das unter Linux verfügbare Kismet [6] eignet sich dazu

Schlüssellänge	Passwort	WEP-Schlüssel (HEX)
40 Bit	anna9	61 6E 6E 61 39
104 Bit	unterseeboot1	75 6E 74 65 72 73 65 65 62 6F 6F 74 31

Tabelle Direkte Abbildung von ASCII-Zeichen auf den WEP-Schlüssel

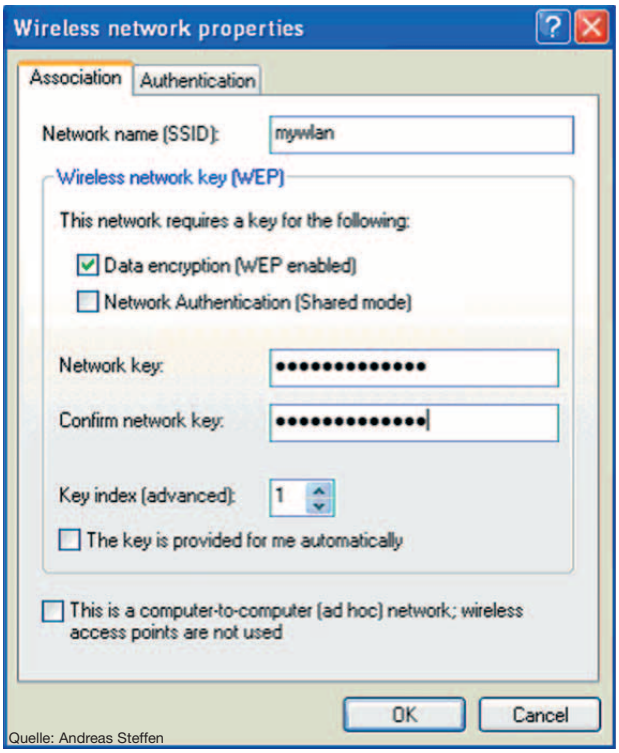


Bild 4 WEP-Schlüsseleingabe von Windows XP

besonders gut, weil es nicht nur alle WLAN-Netzwerke in seiner Reichweite anzeigt, sondern auch eine Fülle von Optionen bietet, wie beispielsweise das Zählen von verschlüsselten WLAN-Paketen. Somit ist sofort ersichtlich, ob das Sammeln von Netzwerkdaten erfolgreich war.

Damit WepAttack angewendet werden kann, muss zuerst verschlüsseltes Rohmaterial gesammelt werden. Dies gestaltet sich in der Praxis schwieriger als angenommen. Erstens werden nur 20 bis 30% aller WLAN mit WEP-Verschlüsselung betrieben. Zweitens wird beim War Driving oft nur das periodische Bakensignal der Basisstation registriert, aber es wird gerade kein verschlüsselter Nutzverkehr übermittelt. Es muss also längere Zeit an einem WEP-gesicherten Standort verweilt werden, bis ein verschlüsseltes Paket aufgenommen werden kann. In Rahmen der ZHW-Diplomarbeit [1] wurde der Verkehr von 15 WEP-geschützten Netzen aufgenommen. WepAttack gelang es, 3 Schlüssel davon zu knacken, d.h. die Erfolgsquote war etwa 20%. Die gefundenen Passwörter waren «choieraient», «beauty» und «schuetzenstra».

Attacke auf schwache Initialisierungsvektoren

Der relativ kurze IV ist der Angriffspunkt einer anderen bekannten WEP-Attacke, die im August 2001 publiziert wurde [7] und ziemlich viel Aufsehen erregte, weil damit die Untauglichkeit des WEP-Algorithmus bewiesen wurde. Es wurde nämlich bekannt, dass im WEP-Anwendungsfall der RC4-Generator ungenügend initialisiert wird, so dass gewisse schwache Bitmuster des Initialisierungsvektors Rückschlüsse auf den geheimen WEP-Schlüssel auf der Basis der ersten Bytes des generierten Schlüsselstroms erlauben. Um einen beliebigen 104 Bit langen WEP-Schlüssel knacken zu können, werden in der Praxis ungefähr 3000 bis 5000 schwache Initialisierungsvektoren benötigt. Dazu muss der gesamte WLAN-Verkehr über einen Zeitraum von mehreren Stunden (bei hohem Verkehrsaufkommen) bis einigen Tagen (bei spärlichem Verkehr) mit dem AirSnort Tool [8] aufgenommen werden, das schliesslich in jedem Fall den vollständig geknackten WEP-Schlüssel liefert.

Schutz durch starke WEP-Schlüssel

Um eine Wörterbuchattacke zu vereiteln, sollte der WEP-Schlüssel völlig zufällig gewählt und als hexadezimaler Wert eingegeben werden. Für einen 104 Bit langen Schlüssel sind dies 26 Zeichen, zum Beispiel die Folge 47 3c 42 23 7d 2e f3 85 bd 94 54 7f c8. Falls eine HEX-Eingabe nicht möglich ist, sollte das Passwort aus einer zufälligen Kombination von 13 ASCII-Zeichen, bestehend aus Gross- und Kleinbuchstaben, Zahlen und Satzzeichen zusammengesetzt werden, beispielsweise nkYI?uJ6FV4+C. Die Anfälligkeit gegenüber AirSnort-Attacken bleibt zwar bestehen, jedoch muss ein Angreifer sehr viel WLAN-Verkehr mitschneiden bis er am Ziel ist.

Schutz durch WiFi Protected Access (WPA)

Als Reaktion auf die aufgedeckten Schwächen der WEP-Verschlüsslung ist

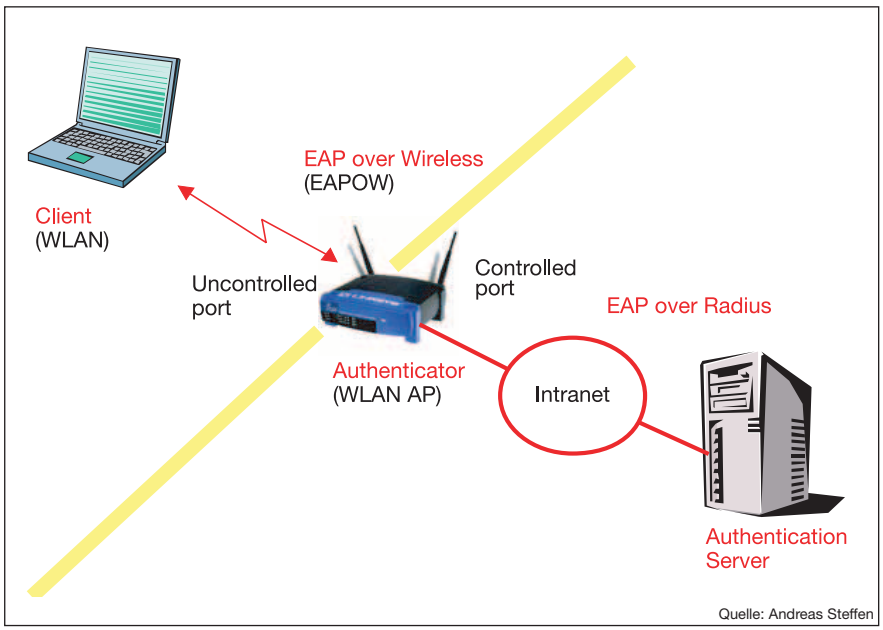


Bild 5 IEEE 802.1x Port-Based Access Control

Ein WLAN-Client meldet sich über den unsicheren drahtlosen Port beim Access Point an, der als Authenticator den Zugang ins Intranet kontrolliert. Es wird eine EAP-TLS gesicherte Verbindung zu einem Radius-Server aufgebaut, der die Identität und Berechtigung des Clients überprüft und bei Erfolg einen verschlüsselten Session-Key an den Client übermittelt.

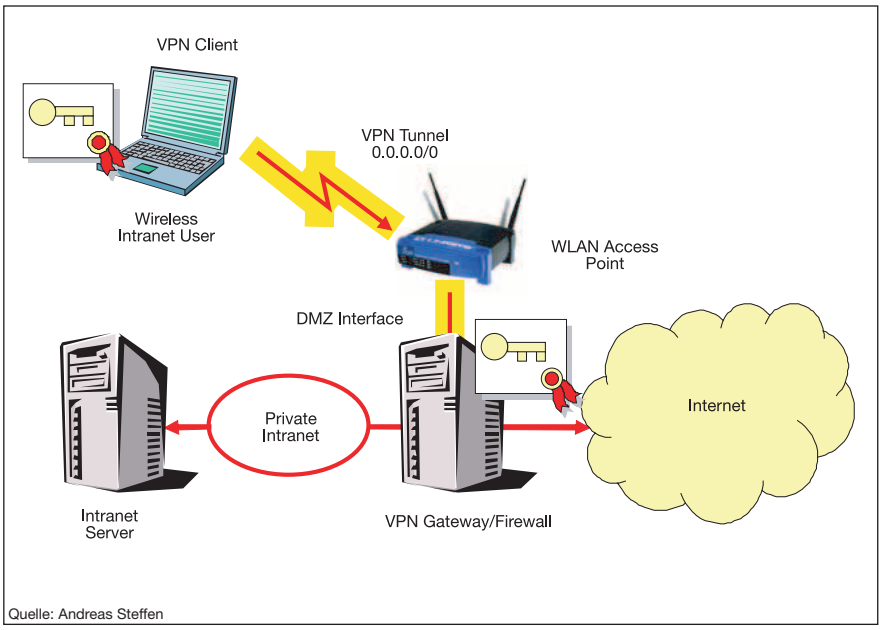


Bild 6 IPsec-basiertes Virtual Private Network (VPN)

Sämtliche über die Luftschnittstelle übertragenen IP-Pakete werden verschlüsselt und gegen Veränderung gesichert zu einem VPN Gateway getunnelt. Nach erfolgreicher Authentisierung des WLAN-Clients, zum Beispiel auf der Basis von X.509-Benutzerzertifikaten, gibt eine Firewall den Weg ins Intranet und oder ins Internet frei.

die Industrie nicht untätig geblieben. Schon seit geraumer Zeit ist eine IEEE-Arbeitsgruppe damit beschäftigt, eine umfassende WLAN-Sicherheitsspezifikation zu definieren, die voraussichtlich 2005 als IEEE-802.11i-Standard verabschiedet werden soll. Die WiFi-Allianz, eine Vereinigung von über 200 Firmen, die sich die Interoperabilität von WLAN-Produkten zum Ziel gesetzt hat, hat als Subset von IEEE 802.11i einen Übergangsstandard unter dem Namen Wi-Fi Protected Access (WPA[4]) definiert, um möglichst schnell sichere Access Points und WLAN-Karten auf den Markt bringen zu können.

Die ersten WPA-fähigen Produkte sind schon erhältlich, und bis Ende 2004 werden die meisten Hersteller nachziehen. WPA besteht aus der Verschlüsselungskomponente Temporal Key Integrity Protocol (TKIP) und dem Authentisierungsstandard IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP)

TKIP arbeitet mit kurzlebigen WEP-Schlüsseln, die zum Beispiel jede Stunde neu generiert werden. Dadurch kann AirSnort nicht genügend schwache Pakete für eine erfolgreiche Attacke sammeln, und selbst wenn mal ein Session-Key geknackt würde, wäre er nur eine begrenzte Zeit nutzbar.

Als zusätzliche Sicherheitsmassnahme wird jedes übermittelte WLAN-Paket mit einer kryptografischen Checksumme versehen, so dass Pakete nicht mutwillig verändert werden können. Weiter wird durch TKIP die Länge des Initialisierungsvektors (IV) von 24 Bit auf 48 Bit erhöht. So kann es nicht mehr vorkommen, dass sich der IV bei starkem WLAN-Verkehr nach 3 bis 4 Stunden wiederholt, was bei einem Stream-Cipher wie RC4 fatale Folgen für die Sicherheit hätte.

IEEE 802.1x Port-Based Network Access Control

Der IEEE-802.1x-Standard führt das Konzept kontrollierter Netzwerkports ein, das nicht nur auf WLAN Access Points angewendet werden kann, sondern allgemein für den Einsatz in Layer 2 Netzwerk-Komponenten (Ethernet Switch, Bridge usw.) gedacht ist. Der Zugriff auf kontrollierte Ports wird nur nach erfolgreicher Authentisierung gewährt. Bild 5 zeigt die prinzipielle Funktionsweise im WLAN-Anwendungsfall:

Ein WLAN-Client meldet sich über den unkontrollierten drahtlosen Port beim Access Point an, der als Authenticator den Zugang ins Intranet kontrolliert. Im sogenannten WPA Enterprise Mode wird als zusätzliche Infrastruktur ein zentraler Radius-Server[5] benötigt, welcher die Benutzerdaten verwaltet. Mittels EAP-TLS (Extended Authentication Protocol – Transport Layer Security) wird eine gesicherte Verbindung vom WLAN-Client zum Radius-Server aufgebaut, und der Client authentisiert sich auf der Basis eines Client-Zertifikats oder Benutzerpasswortes. Der Server muss sich ebenfalls mit einem X.509-Zertifikat ausweisen, damit Man-in-the-Middle-Attacken[6] verunmöglicht werden. Nach erfolgter Authentisierung generiert der Radius-Server einen WEP-Session-Schlüssel, der verschlüsselt via EAP-TLS an den Client und den Access Point übermittelt wird.

Für SOHO-Anwendungen (Small Office / Home Office), wo das Aufsetzen und Betreiben eines Radius-Servers mit zu hohen Umtrieben und Kosten verbunden wäre, hat die Wi-Fi-Allianz den sogenannten WPA Preshared Key Mode vorgesehen. Dabei wird ein geheimes Passwort sowohl auf dem Access Point wie auch auf dem WLAN-Client gespeichert, und von diesem werden dann die kurzlebigen TKIP-Schlüssel abgeleitet. Leider wird es dadurch weiterhin möglich sein, schwache Preshared Keys mittels einer Wörterbuchattacke zu knacken, so dass in dieser Hinsicht dieser WPA-Modus keinen Fortschritt bringen wird.

Schutz durch ein Virtual Private Network (VPN)

Um ein WLAN wirklich sicher zu machen, empfiehlt es sich, ein Virtual Private Network (VPN) auf der Basis des IPsec-Standards aufzusetzen. Damit werden sämtliche IP-Pakete kryptografisch sicher verschlüsselt und authentisiert, so dass WEP oder WPA nicht mehr benötigt werden. Wie Bild 6 zeigt, muss auf jedem WLAN-Rechner eine VPN-Client-Software installiert sein, damit ein IPsec-Tunnel zu einem VPN Gateway aufgebaut werden kann, der sich hinter dem WLAN Access Point befindet. Da IPsec ein OSI-Schicht-3-Protokoll ist, leitet der Access Point als Schicht-2-Gerät die IPsec Pakete unverändert an die Endpunkte weiter, ist also selber nicht an der Sicherung der Verbindung beteiligt.

Der VPN Gateway wird nun mit einer Firewall gekoppelt, die in der Grundeinstellung sämtlichen von der Luftschnittstelle kommenden IP-Verkehr blockiert. Der Access Point und damit das WLAN-Netz befindet sich also in einer Art «demilitarisierten Zone» (DMZ[7]). Nur nach erfolgreicher Authentisierung des VPN Clients wird die Firewall gezielt für – durch den IPsec Tunnel geschleuste – IP-Pakete geöffnet und nach dem Beenden des Tunnels wieder automatisch geschlossen.

Prinzipiell wird der gesamte, über die Luftschnittstelle laufende IP-Verkehr getunnelt, und zwar unabhängig davon, ob auf einen Server im Intranet zugegriffen

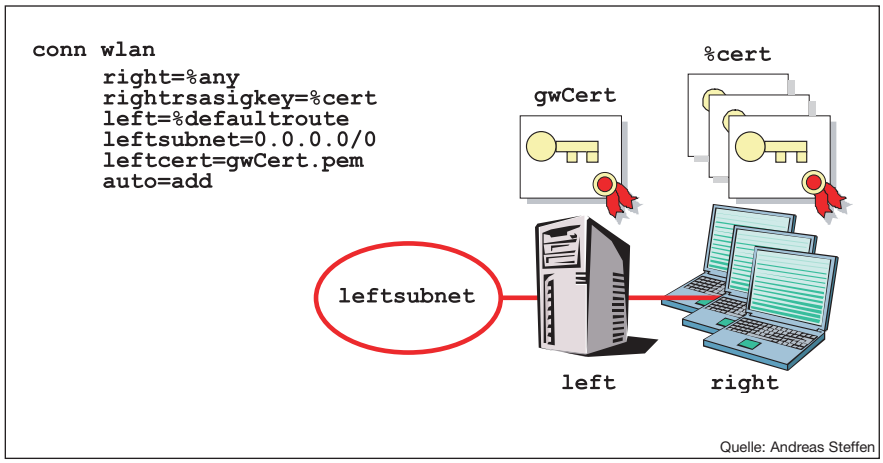


Bild 7 Konfiguration eines Linux strongSwan VPN Gateways

Diese einfache Konfiguration erlaubt einer beliebigen Anzahl von VPN Clients (right=%any), die ein gültiges Zertifikat (rightrsasigkey=%cert) präsentieren, den Zutritt ins Netz (leftsubnet=0.0.0.0/0) hinter dem VPN Gateway, das im WLAN-Fall das gesamte Internet darstellt. Auch der Gateway weist sich mit seinem Zertifikat (leftcert=gwCert.pem) gegenüber den Clients aus.

oder ob im Internet gesurft wird. Im SOHO-Bereich bietet sich als kompakte Lösung ein kombinierter VPN-Gateway-Firewall-Router mit drei Netzwerkschnittstellen für LAN (Intranet), WAN (Internet via ADSL oder Cable TV) und WLAN (DMZ für Access Point) an. Die Firewall schützt auch gleich vor Attacken aus dem Internet, und der VPN Gateway kann auch für den gesicherten Fernzugriff auf das Firmen- oder Campus-Netzwerk verwendet werden. Entsprechende Kombigeräte, die teils auch gleich den Access Point mitintegrieren, sind zunehmend auf dem Markt erhältlich.

Linux VPN Gateway

Als kostengünstige Alternative kann die Open-Source-Software strongSwan [9] auf einem PC – auch älterer Bauart – unter dem Linux-Betriebssystem eingesetzt werden, um einen VPN Gateway inklusive Firewall zu realisieren. Die strongSwan-Distribution wird von der Security Group der Zürcher Hochschule Winterthur (ZHW) gepflegt und ist aus dem Linux-FreeS/WAN-Projekt hervorgegangen, zu dem Informatikstudenten der ZHW im Rahmen von Projekt- und Diplomarbeiten in den letzten drei Jahren viele zusätzliche Leistungsmerkmale wie zum Beispiel die Authentisierung über X.509-Zertifikate, SmartCard-Unterstützung usw. beigetragen haben.

Die genaue Konfiguration eines Linux VPN Gateways ist in [9,10] ausführlich beschrieben. Bild 7 zeigt übersichtsweise, dass nur wenige Konfigurationszeilen notwendig sind, um eine beliebige Anzahl von WLAN-Clients mittels VPN-Tunnel zu schützen. Die Clients und der Gateway authentisieren sich gegenseitig auf der Basis von X.509-Zertifikaten, die ebenfalls im Eigenbau hergestellt werden können [11,12].

Fazit

Es wurde gezeigt, dass eine Wörterbuchattacke auf schwache Passwörter oder eine Attacke basierend auf schwachen Initialisierungsvektoren die WEP-Verschlüsselung völlig unbrauchbar macht. Wirkliche Sicherheit schafft der neue WPA-Standard, allerdings nur im gesicherten Enterprise Mode, oder alternativ der starke End-zu-End-Schutz mittels eines Virtual Private Networks.

Referenzen

[1] *Dominik Blunk und Alain Girardet:* WLAN War Driving, Diplomarbeit, Zürcher Hochschule Winterthur, Oktober 2002, www.zhwin.ch/~sna/DA/Sna6_2002.pdf
[2] *Dominik Blunk und Andreas Steffen:* WLAN-Hacking en Passant, Heise Security Portal, Juni 2003, http://www.heise.de/security/artikel/38099
[3] *Tim Newsham:* Cracking WEP Keys, 2001, www.lava.net/~newsham/wlan/WEP_password_cracker.ppt
[4] WepAttack Download: http://wepattack.sourceforge.net
[5] John the Ripper Download: www.openwall. com/john/
[6] Kismet Download: www.kismetwireless.net/
[7] *Scott Fluhrer, Itsik Mantin, Adi Shamir:* Weaknesses in the Key Scheduling Algorithm of RC4, August 2001: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
[8] AirSnort Download: http://airsnort.shmoo.com
[9] Linux strongSwan: http://www.strongswan.org/
[10] *Jürgen Schmidt:* Der Pförtner zum Netz, Ein IPSec-Gateway im Eigenbau, c't 10/03, Heise Verlag, Hannover, 2003, S. 118 ff.
[11] *Andreas Steffen:* Den Ausweis bitte, sicherer Zugang zum LAN via Virtual Private Network, c't 5/02, Heise Verlag, Hannover, 2002, S. 216 ff. http://www.heise.de/ct/02/05/216/
[12] *Andreas Steffen:* Eigener Schlüsseldienst, VPNs und Zertifikate im Eigenbau, c't 5/02, Heise Verlag, Hannover, 2002, S. 220 ff. http://www.heise.de/ct/02/05/220/

Angaben zum Autor

Dr. ***Andreas Steffen*** ist Professor für Kommunikation und Sicherheit an der Zürcher Hochschule Winterthur (ZHW). Er leitet die ZHW Security Group, die angewandte Forschung und Entwicklung auf dem Gebiet der Netzwerksicherheit betreibt.
Zürcher Hochschule Winterthur, Technikumstrasse 9, 8401 Winterthur, andreas.steffen@zhwin.ch.

[1] Wi-Fi: Wireless-Fidelity-Allianz von rund 200 WLAN-Herstellern.
[2] RC4: Rivest Cipher Nr. 4
[3] RSA: Public-Key-Verschlüsselungssystem von Rivest, Shamir und Adleman
[4] WPA: Wi-Fi Protected Access. WLAN-Sicherheitsspezifikation der Wi-Fi-Allianz. Subset des IEEE-802.11i-Standards, der voraussichtlich 2005 verabschiedet wird.
[5] Radius: Das Remote-Authentication-Dial-In-User-Service-Protokoll (RFC 2865) zentralisiert die Authentisierung, Autorisierung und Verrechnung des Netzwerkzugriffs auf einem sicheren Server, dem Radius-Server.
[6] Man-in-the-Middle-Attacke: Dabei schaltet sich ein Gegner aktiv in eine Kommunikationsverbindung ein und übernimmt zum Beispiel gegenüber einem Client die Rolle des Servers. Der ahnungslose Client sendet nun seine Daten an den falschen Server, wobei dieser sie an den richtigen Server weiterleitet, damit die Attacke nicht bemerkt wird.
[7] DMZ: Demilitarized Zone. Bezeichnung für jenen Teil eines Netzwerks, das weder zum internen Netzwerk noch zum Internet gehört.

Sécurité des Wireless LAN

Attaques et mesures de protection

Les WLAN – Wireless LAN – ouvrent de toutes nouvelles perspectives de liberté dans la communication mobile et flexible des données. Mais la transmission sans fil présente des dangers considérables. L'article décrit deux possibilités, pour les attaquants éventuels, de s'infiltrer dans les réseaux codés. Fort heureusement, il existe des mesures de protection permettant de protéger les WLAN des intrusions indésirables, ceci fiablement et à des frais acceptables.