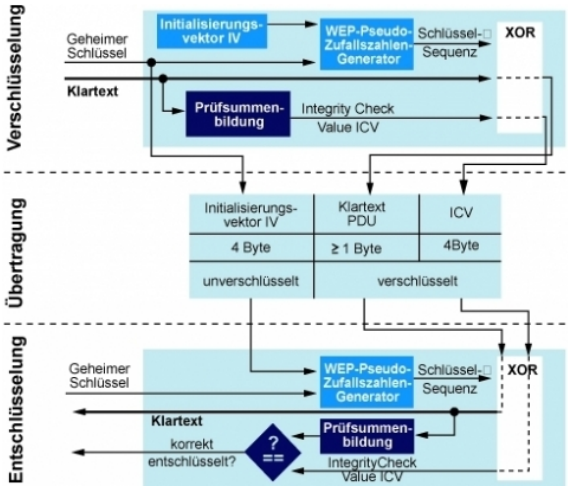
Sicherheitsrisiko WEP

› Die meisten WLAN-Besitzer verschlüsseln ihr drahtloses Netzwerk mittels WEP. Wer allerdings glaubt, dass er damit fremde Zugriffe verhindert, der irrt. Aktuelle Programme knacken den Schutz innerhalb von Minuten.

VON Moritz Jäger (11.08.2005 08:31:00)

WLAN-Sicherheit bedeutet in erster Linie das Verschlüsseln der eigentlichen Datenübertragung. Ohne diese Verschlüsselung sind die Daten während der Übertragung für jeden sicht- und lesbar, ähnlich einer Postkarte. Die beiden bekanntesten Verschlüsselungsverfahren sind Wired Equivalent Privacy (WEP) und Wi-Fi Protected Access (WPA).

WEP ist einen optionalen Bestandteil des IEEE802.11-Standards und muss nicht zwingend implementiert sein. Inzwischen ist ein Schlüssel 128 Bit Länge in den meisten Geräten der Standard. Die Verschlüsselung im Rahmen des IEEE802.11 wird nicht nur zum 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 Netzwerk.



Verschlüsselungsablauf: Das Diagramm zeigt, wie WEP den Datenstrom verschlüsselt.

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

› Angriffsziel Initialisierungsvektor

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. Das Verfahren verschlüsselt Klartext als auch die Prüfsumme und überträgt diese mit dem unverschlüsselten Initialisierungsvektor.

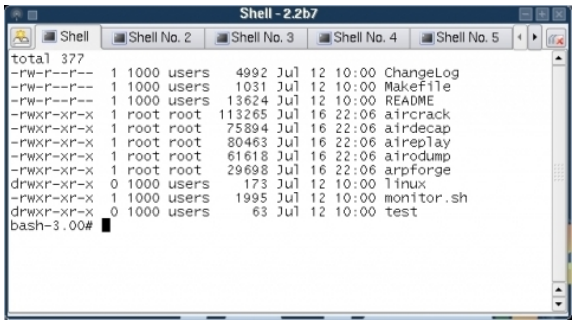
Dieser 24-Bit lange IV wird anhand eines feststehenden Algorithmus mit jedem neuen Paket verändert. Dies bedeutet, dass nach rund 16,7 Millionen Paketen wieder mit der gleichen Abfolge von Initialisierungsvektoren begonnen wird. Entsprechend liegen dann der Verschlüsselung der folgenden Pakete die gleichen Zeichenfolgen zugrunde.

Am 06. August 2004 erstellte ein Hacker namens KoreK einen Eintrag (http://www.netstumbler.org/showthread.php?postid=89036#post89036) im Forum des Windows-Sniffers Netstumbler. In diesem Eintrag stellte er den Quellcode für einen neuen Cracker zur Verfügung, der bald als Chopper bekannt wurde. Die Neuerung in Chopper war, dass er eine statistische Angriffsmethode nutzt. Diese Attacke lieferte schneller Ergebnisse als jede andere. Bislang waren mehrere Millionen IV-Pakete notwendig, dank KoreKs Methode reduzierte sich die Zahl auf etwa 2,5 Millionen Pakete.

› Chopper - Das Ende von WEP

KoreK wies im Netstumbler-Forum (http://www.netstumbler.org/showthread.php?t=11878) Christophe Devine, den Entwickler eines WEP-Crackers namens Aircrack, auf seinen Code hin. Devine war von den Fähigkeiten der Methode beeindruckt und integrierte sie in sein Programm. Er war selbst vom Ergebnis überrascht: Aircrack knackte einen 128-Bit-Schlüssel innerhalb von 5 Minuten und benötigte lediglich 500.000 Initialisierungsvektoren. Sobald eine Million IVs vorhanden waren, wurde der Key nahezu sofort gefunden, andere Forennutzer berichten, dass maximal 2,2 Millionen IV-Pakete nötig waren um jeden WEP-Key innerhalb von Sekunden zu knacken.

Aircrack steht sowohl für das Crack-Programm als auch für eine Sammlung von „Zulieferprogrammen“. Die Whax-Live-CD (http://www.iwhax.net/) enthält die kompletten Satz an Tools, die nötig sind, um die Angriffswege nachzuvollziehen und die Sicherheit der eigenen WLAN-Umgebung zu prüfen. Zu den wichtigsten Programmen gehören Aircrack selbst, Airodump sowie Aireplay.



Alles was nötig ist: Whax enthält sämtliche Tools, um ein WEP-verschlüsseltes WLAN prüfen zu können.

Vorraussetzung ist lediglich ein WLAN-Adapter, deren Chipsatz die Programme unterstützt. Da die Hauptseite des Entwicklers offline ist, ist eine Empfehlung schwierig. Am besten fahren Sie mit einer Wi-Fi-Karte, die einen Prism-2- oder Orinoco-Chipsatz enthält. Sollten Sie eine passende Karte suchen, empfehlen sich die Wardriving-Foren von Netstumbler (http://netstumbler.org/) oder dem Wireless-Forum (http://www.wireless-forum.ch/forum/index.php) .

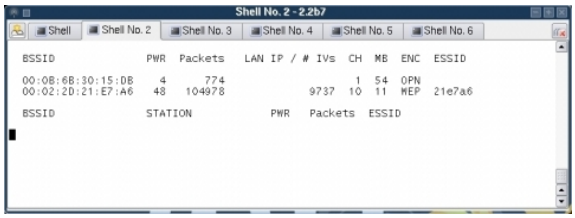
› Airodump - Der Paketsammler

Das wichtigste Programm ist Airodump. Das Programm zeichnet den gesamten Netzwerk-Traffic auf, der auf einem zuvor festgelegten Interface empfangen wird und trägt ihn in eine Datei ein.

Das Programm starten Sie mit: `» airodump <Netzwerk-Interface oder pcap-Datei> <Name der Ausgabedatei> <WLAN-Kanal> [IVs Flag] «`

Beim ersten Start macht es Sinn, keinen Channel anzugeben. Dadurch zeigt das Programm erst einmal sämtliche aktiven WLAN-Kanäle an. Unterbrechen Sie im Anschluss den Betrieb, starten Sie Airodump neu, diesmal mit dem Channel, der überwacht werden soll.

Ein Beispielaufruf für unsere Testumgebung ist: airodump ath0 wepdump 10 1. Damit weisen wir das Programm an, mit der WLAN-Karte ath0 sämtlichen Netzwerkverkehr auf dem Kanal 10 zu überwachen. Sobald dort einzigartige IVs registriert werden, sollen diese in der Datei „wepdump“ abgelegt werden. Das Programm startet und beginnt mit der Aufzeichnung.



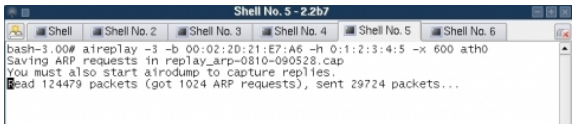
Sammeltrieb: Airodump zeichnet den kompletten Traffic auf, den ein Netzwerkadapter empfängt. Auf Wunsch lassen sich außerdem die IVs automatisch ausfiltern.

Der Schalter IVs Flag legt fest, ob das Programm den kompletten Traffic aufzeichnet und in einer pcap-Datei sichert (0) oder sich auf einzigartige WEP Initialisierungsvektoren beschränkt (1). Diese IVs lassen sich auch aus bereits vorhandenen pcap-Dateien extrahieren. Wie das funktioniert, erfahren Sie, indem Sie Airodump ohne zusätzliche Optionen aufrufen.

› Aireplay - Mehr Pakete, mehr IVs

Theoretisch reicht bereits Airodump um die benötigen Pakete zusammenzukriegen. Allerdings ist ein dazu ein relativ aktives WLAN notwendig, in dem genügend Clients Traffic erzeugen. Ist das nicht der Fall, kommt Aireplay zum Einsatz.

Das Programm meldet sich beim Access Point an und beginnt damit ARP-Anfragen zu senden. Der jeweilige Host wird immer auf diese ARP-Pakete antworten, selbst wenn eine Firewall im Einsatz ist. Genauere Informationen zu ARP finden Sie in dem Artikel „ARP-Grundlagen und Spoofing“ (Webcode: 402460). Jede Antwort ist wieder per WEP verschlüsselt und bringt somit weitere IVs in die Dump-Datei. Voraussetzung ist, dass in dem Netzwerk mindestens ein weiterer Client mit dem Host per WLAN kommuniziert.



Paket-Sturm: Aireplay sendet kontinuierlich ARP-Anfragen. Die Antwortdaten enthalten weitere IVs, die Airodump aufzeichnen kann.

Aireplay bietet 27 Optionen und Schalter. Der Grundaufruf ist mit `» aireplay [Optionen] <Netzwerk-Interface> «` relativ harmlos, muss aber durch diverse Angaben erweitert werden. `» aireplay «` allein zeigt sämtliche Schalter mit einer kurzen Erklärung an.

Zunächst muss Aireplay beim Access Point anmelden und mit ihm assoziieren. Das erreicht der Befehl `» aireplay -1 0 -e [SSID des APs] -a [MAC-Adresse des Access Points] -h [beliebige Quell-MAC-Adresse im Format 0:1:2:3:4:5] ath0 «` . Über den Parameter -h lässt sich beispielsweise eine bereits im Netzwerk vorkommende MAC-Adresse klonen.

Neuanmeldung: Die Option -0 unterbricht sämtliche Client-Verbinungen und zwingt sie zu einer erneuten Authentifizierung.

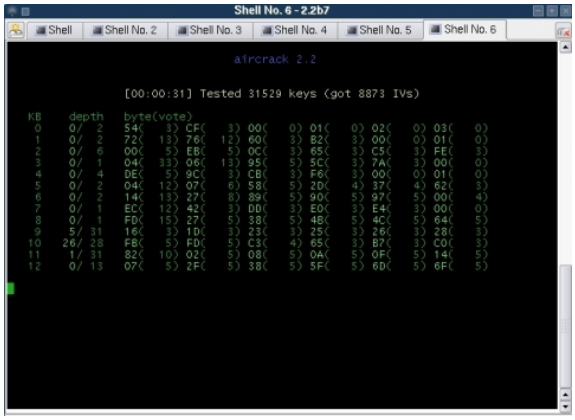
Kommt als Antwort ein Vierzeiler, der die Worte „Authentication successful“ und „Association successful“ enthält, ist Aireplay einsatzbereit. Der Befehl um das Senden der ARP-Anfragen zu beginnen lautet: » `aireplay -3 -b [MAC-Adresse des Access Points] -h [beliebige Quell-MAC-Adresse im Format 0:1:2:3:4:5] -x [Anzahl der Anfragen pro Minute] ath0` «

Ein weiterer interessanter Schalter ist die Option -0. Damit fordert Aireplay jeden angemeldeten Client auf, seine Verbindung zu unterbrechen und sich erneut anzumelden. In Kurzer Zeit lassen entsteht so ein massiver Zuwachs an IVs.

› Aircrack - Knackt jeden WEP-Key

Sobald eine Airodump eine ausreichende Anzahl an IVs gesammelt hat, kommt Aircrack selbst zum Einsatz. Ein guter Wert sind etwa 500.000 IVs. Der Cracker selbst lässt sich einfach starten, die Befehlszeile lautet » `aircrack [Optionen] <.cap-/.ivs-Datei(en)>` « . Eine komplette Übersicht mit alle 14 Schaltern erhalten Sie wie gehabt durch die Eingabe von » `aircrack` « .

Im Anschluss liest der Cracker die aufgezeichneten Dateien aus und versucht die erste gefundene MAC-Adresse zu knacken. Sobald Aircrack mit der statistischen Attacke Erfolg hat, zeigt er den Schlüssel auf dem Bildschirm an.



Entschlüsselnd: Aircrack nutzt die aufgezeichneten IVs um einen Angriff auf den WEP-Key durchzuführen.

Damit ist der Schlüssel zum WLAN in den Händen des Angreifers, einer Anmeldung am Access Point steht nichts mehr im Weg.

› Alternative WPA?

Mit WEP verschlüsselte WLANs halten schon lange keine Angreifer mehr ab. Die notwendigen Tools sind für jedermann erhältlich, die Linux-Distribution Whax bringt sie ebenfalls bereits einsatzbereit mit. Wie lassen sich kabellose Netzwerke trotzdem effektiv schützen? Eine Möglichkeit ist die Verschlüsselung mit Wi-Fi Protected Access (WPA). Die Methode wurde dem zukünftigen WLAN-Standard 802.11i entnommen.

WPA nutzt denselben RC4-Verschlüsselungsalgorithmus wie auch WEP. Allerdings sind die Initialisierungsvektoren länger (48 Bit statt 24 Bit) und zusätzlich wird die Verbindung durch eine Per-Packet-Key-Mixing-Funktion, einen Re-Keying-Mechanismus und einen Message Integrity Check (MIC) geschützt. Derzeit aktuelle WLAN-Geräte verwenden einen Pre-Shared-Key (WPA-PSK). Einen möglichen Angriffspunkt bieten hier allerdings schwache Passwörter. Sobald das Passwort leicht zu erraten ist, stehen dem Angreifer wieder die Tore des WLANs offen.

Ein Angriff auf WPA lässt sich ebenfalls mit Aircrack durchführen, es muss lediglich ein zusätzliches Wörterbuch spezifiziert werden. Wie schnell und einfach eine solche Attacke ist, zeigt ein Flash-Film in der Dokumentation (http://www.cr0.net:8040/code/network/aircrack/#q010) von Aircrack.

› Fazit

Zum Absichern eines WLANs ist WPA-PSK definitiv die bessere Wahl, solange ein starkes Passwort zum Einsatz kommt. WEP bietet inzwischen keinen ausreichenden Schutz mehr, selbst Laien können den Schutz aushebeln.

WLANs sind zwar extrem angenehm, bieten aber dennoch ein nicht zu unterschätzendes Risiko in Firmen. Besonders wenn mehrere Clients auf das Netz zugreifen, sind die benötigten IV-Pakete schnell zusammen.

Richtige Sicherheit wird wohl erst WPA2 geben. Das Protokoll ist komplett dem 802.11i-Standard entnommen und basiert auf der Verschlüsselungstechnologie AES. Die notwendige Rechenpower macht WPA2 teilweise inkompatibel mit älteren Geräten. Ist die CPU-Kapazität ausreichend, reicht ein einfaches Update der Firmware. Die Wi-Fi Alliance (http://www.wi-fi.org/) hat auf ihrer Homepage bereits die ersten Geräte und Firmware-Versionen freigegeben (http://certifications.wi-fi.org/wbcs_certified_products.php) . (mja)