Sicherheit drahtloser Netze – Luftangriffe abwehren

Marc Ruef <maru@scip.ch>

Drahtlose Netze erfreuen sich zunehmends grosser Beliebtheit. Die neue Freiheit, ungebunden und von überall Daten transferieren zu können, wurde mit offenen Armen empfangen. Die Technik ist zwar nicht wirklich neu, noch nicht mal ausgereift – Der Boom wurde in erster Linie durch die Erschwinglichkeit angetrieben. Die Goldgräberstimmung bei Herstellern und die Euphorie bei den Benutzern wurde jedoch schnell wieder getrübt: Die mangelhafte oder gar fehlende Sicherheit drahltoser Systeme ist eine Spielwiese für Hacker und Cracker.

Wireless LANs galten lange Zeit als relativ sicher: Die Möglichkeit der Verschlüsselung zum Schutz vor unerlaubtem Abhören war gegeben. Durch Wired Equivalent Privacy (WEP) lassen sich WLANs mit kryptographischen Mitteln schützen. Die Hacker-Sezene interessierte sich nur mässig für die neue Technologie. Angriffsmethoden oder spezielle Tools, wie zum Beispiel Wireless-Sniffer, gab es keine [Dobkowitz 2002]. Es war jedoch nur eine Frage der Zeit, bis sich das Blatt wenden würde.

In diesem Artikel wollen wir uns mit den grundlegenden Aspekten der Sicherheit drahtloser Netzwerke befassen. Wir werden sehen, welche Fehler bei der Erstellung der Standards gemacht wurden, wie sich diese ausnützen lassen und was man dagegen tun kann.

Schwache Verschlüsselung

WEP stellt ein Verfahren zur Verschlüsselung vom Kommunikationen dar und ist im Standard IEEE 802.11 als optionales Feature spezifiziert. Je nachdem, mit welcher Schlüssellänge gearbeitet wird, spricht man von WEP64 oder WEP128. Im Grunde ist nur WEP64 im Standard definiert. WEP128 stellt einen erweiterten Industrie-Standard dar. Die Schlüssellängen entsprechen sodann 64 oder 128 Bit, wobei davon jeweils 24 Bit den Initialisierungsvektor (abk. IV) darstellen. Dies ist ein zufällig gewählter Wert, der von Datenpaket zu Datenpaket verändert wird [Schneier 1996]. Der Rest, die 40 bzw. 104 Bit, können vom Anwender frei definiert werden. Die Verschlüsselung von Datenpaketen mittels WEP findet in drei Schritten statt [Zacchendu 2002]:

1. Zu Beginn wird die Nachricht M nach einem CRC-32 Verfahren berechnet. Dies ist der sogenannte Integrity Check Value (ICV). Die mit der Checksumme verknüpfte Nachricht bildet den Klartext.

2. Im zweiten Schritt wird wird aus dem WEP-Schlüssel k und einem möglichst zufällig gewählten Initialisierungsvektor v, bestehend aus 28 Bit, mit der Hilfe des altbekannten RC4-Algorithmus ein Schlüsselstrom (engl. keystream) erzeugt [Schneier 1996].

3. Im dritten und letzten Schritt wird der Klartext und der Schlüsselstrom mittels der mathematischen Operation XOR (eXclusive-OR) verknüpft. Dies erstellt den Ciphertext C, der verschickt werden kann.

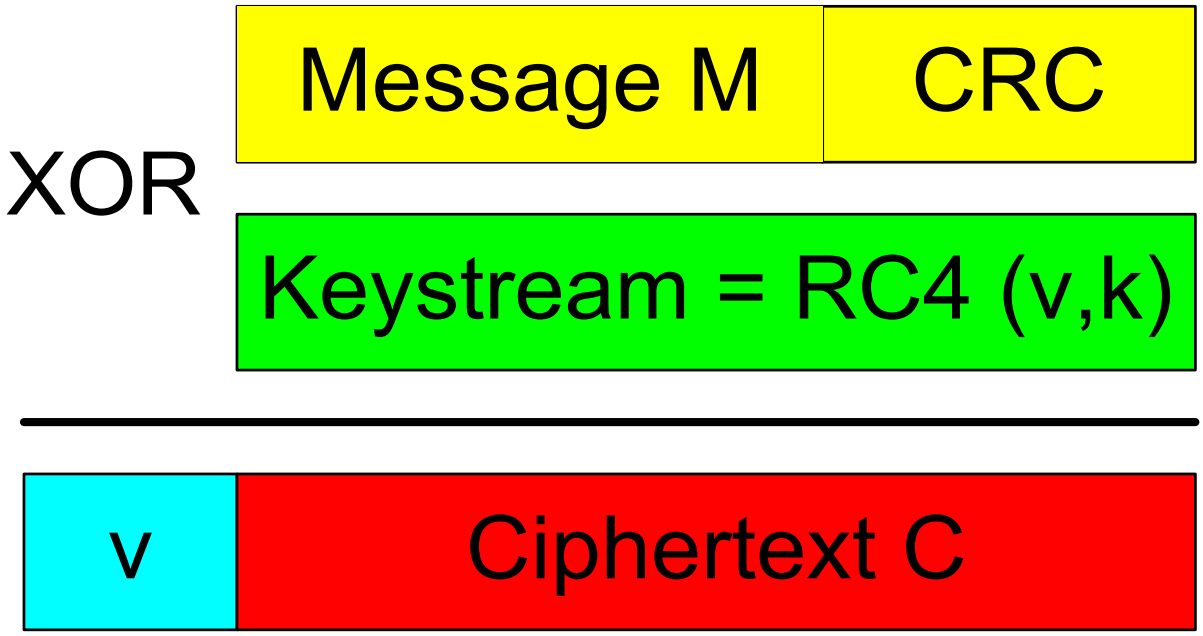


Abbildung 1: WEP-Verschlüsselung

Eine Kommunikation zwischen den jeweiligen Wireless-Elementen (z.B. Client und Access Point) kann sodann nur stattfinden, wenn auf beiden Seiten der gleiche Schlüssel hinterlegt wurde. Sind die Schlüssel nicht identisch, kann keine Verbindung hergestellt werden. Einige Access Points lassen sich jedoch so konfigurieren, dass sie auch unverschlüsselte Kommunikationen zulassen. Dies ist ein nettes Feature für Administratoren, die sich nicht durch den Konfigurations-Dschungel von WEP kämpfen wollen. Grundsätzlich bedeutet diese Freizügigkeit jedoch auch, dass a) nur ein Teil der Kommunikationen verschlüsselt ist und b) sich jeder, auch ohne den richtigen WEP-Schlüssel ins Funk-Netzwerk einwählen kann.

Wie Studenten der Rice Universität zusammen mit Angestellten von AT&T Ende Juli 2001 festgestellt haben, ist die Umsetzung von WEP misslungen [Ioannidis et al. 2001]. Zuerst wurde angenommen, dass sich die Schwachstelle allein in der Implementierung des RC4-Algorithmus findet. Dies ist jedoch nicht ganz richtig, denn der Fehler ist auch dadurch gegeben, dass WEP einen schwachen Initialisierungsvektor generiert. Er ist zu klein. Dadurch kann er seiner Aufgabe, dem Verhindern von Schlüsselwiederholungen, nicht gerecht werden. So kann es vorkommen, dass nach wenigen Stunden eine WLAN-Karte alle möglichen 2^24 Initialisierungsvektoren durch hat und diese zum wiederholten Male zum Einsatz kommen. Einige Karten erreichen diesen Punkt schneller, bei anderen dauert es etwas länger.

Kennt ein Angreifer zwei verschlüsselte Nachrichten mit dem gleichen IV, kann er diese mit XOR verknüpfen. Durch diese XOR-Verknüpfung erhält er die Klartexte der beiden verschlüsselten Nachrichten. Die Schwachstellen im WEP-Mechanismus können durch Tools wie WEPCrack (http://wepcrack.sourceforge.net/) und Airsnort (http://airsnort.shmoo.com/) ausgenutzt werden, um unberechtigten Zugriff zum WEP-Schlüssel zu erhalten. Ist dies einem Angreifer gelungen, kann er wieder nach Herzenslust Daten mitlesen oder sich selber in das WLAN einklinken.

In meinem Buch „Hacking Intern“ habe ich das Horror-Szenario um WEP jedoch ein bisschen relativiert [Ruef et al. 2002, 2003]: „Auch wenn direkte Mängel in WEP nachgewiesen werden können, darf nicht die ganze Schuld darauf abgeladen werden. WEP erfüllt

schlussendlich den Zweck, zu dem es entwickelt wurde. Es gewährt dem Benutzer die Sicherheit, die er auch auf einem Kabel erwarten kann.“

Agere Systems hat das Problem erkannt und WEPplus ins Leben gerufen. Dies ist eine verbesserte Version von WEP, die auf der Basis der ORiNOCO-Technik entwickelt wurde.

Gesprächige SSID

Jeder Access Point (AP) sendet in einem bestimmten Intervall Beacon Frames, die die SSID (Service Set Identification) beinhaltet. Diese ebenfalls in IEEE 802.11 definierte Zeichenkette dient der Zuweisung von Systemen zu einem bestimmen WLAN. Dadurch soll verhindert werden, dass jemand versehentlich in ein falsches Netz gerät, oder dass sich zwei paralell laufende WLANs stören. Was beim Internet Protocol (IP) die Subnetzmasken sind, sind bei WLANs die SSIDs. Alexander Hagenah schreibt in seiner Dokumentation „Catching the Air Stuff“ (Kapitel 2), dass eine SSID mit einem Passwort vergleichbar ist [Hagenah 2002]. Denn nur wer sich im Besitz der richtigen SSID befindet, darf mit dem entsprechenden Access Point kommunizieren.

Das Problem besteht nun jedoch darin, dass Angreifer mittels einem Wireless-Sniffer die Beacon Frames auffangen und die mitgeschickte SSID – in unserem Beispiel lautet diese „WirelessLAN4“ - extrahieren können. Sodann ist der erste Grundstein gelegt, um in das drahtlose Netzwerk einzubrechen. Ist keinerlei Verschlüsselung und Authentisierung vorhanden, muss der Angreifer nur noch seinen Rechner richtig konfiurieren, um sich im Netzwerk frei zu bewegen.

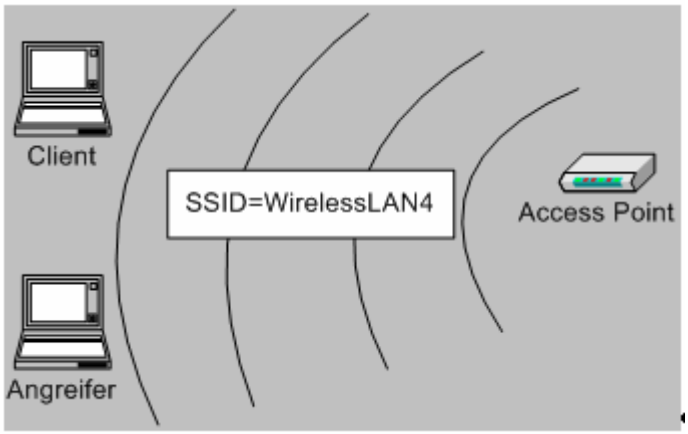


Abbildung 2: SSID Broadcast

Die Hersteller von Access Points haben dieses Problem erkannt und bietet in ihren modernen Geräten die Möglichkeit an, auf das Broadcasting der SSID zu verzichten. Von dieser Funktion gilt es bestmöglich Gebrauch zu machen, denn die meisten Angreifer lassen sich durch diese simple Massnahme an einem erfolgreichen Einbruch hindern. Um auch weiterhin das Funktionieren des WLANs gewährleisten zu können, muss man die SSID manuell auf den jeweiligen Geräten eintragen und speichern.

Max Moser, der Entwickler des Wireless-Sniffers „Wellenreiter“ (http://www.remote-exploit.org) berichtete mir Ende letzten Jahres von einer weiteren Möglichkeit, sich die

Gegebenheiten von SSIDs zum Schutz des eigenen WLANs zunutze zu machen [Ruef et al. 2002]. Fehlerhafte Übertragungen im Funkbereich sind üblich. Viele der Wireless-Sniffer, wie zum Beispiel der populäre Kismet (http://www.kismetwireless.net), versuchen fehlerhaft übertragene SSIDs zu ignorieren. Die Filterung findet anhand dessen statt, dass selten gebräuchliche Zeichen auf eine fehlerhafte Übertragung hindeuten. Eine SSID von „WirelessLAN4“ wird von Kismet fehlerfrei als richtig erkannt. Setzen wir die SSID jedoch auf „WL4*+$“, dann vermutet der Wireless-Sniffer eine Falschübertragung und verwirft die eigentlich richtige Information.

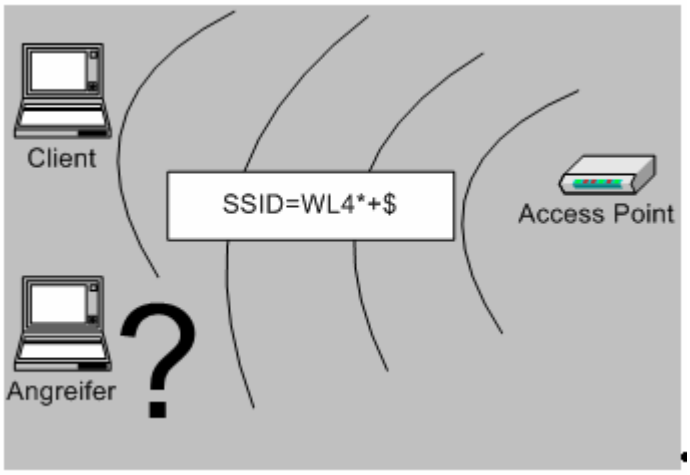


Abbildung 3: Sonderbare SSID

Versuchen Sie deshalb Sonderzeichen in Ihren SSIDs einzusetzen. So kann eine Vielzahl der Wireless-Sniffer ausgetrickst werden. Zwar lassen sich diese exotischen SSIDs nicht gerade einfacher merken. In Anbetracht dessen, dass man die SSID jedoch nur selten manuell eingeben muss, ist dieser Nachteil gerne in Kauf zu nehmen.

Schutz durch MAC-Filter

Viele moderne Access Points erlauben es, nur gewisse Netzwerkkarten aufgrund der denen zugeteilten MAC-Adresse zuzulassen. Auf dem AP werden in einer lokalen Tabelle sämtliche zugelassenen MAC-Adressen gespeichert. Möchte sich ein System verbinden, das nicht in dieser Liste vermerkt ist, wird es abgewiesen. Dabei spielt es keine Rolle, ob die anderen Informationen, wie Frequenz, SSID oder WEP-Schlüssel korrekt waren. Diese Technik wird als MAC-Filter oder ACL (Access Control List) bezeichnet.

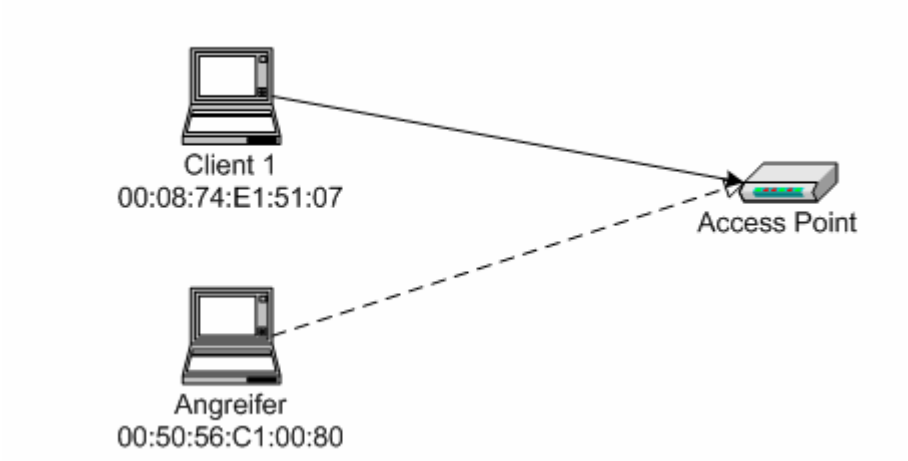


Abbildung 4: MAC-Authentisierung

Alexander Hagenah schreibt in seiner Dokumentation jedoch ganz richtig, dass es sich hierbei um eine trügerische Sicherheit handelt [Hagenah 2002]. Grundsätzlich werden in jedem Falle, auch bei aktivierter WEP-Verschlüsselung, die MAC-Adressen per Funk übertragen. Ein Angreifer kann mittels Wireless-Sniffer diese Information auslesen und so zugelassene MAC-Adressen identifizieren.

Zudem erlauben die meisten Betriebssysteme das Überschreiben der MAC-Adresse der jeweiligen Schnittstellen. Ist ein Angreifer im Besitz des Wissens zugelassener MAC-Adressen, kann er sich selber eine solche vergeben und dadurch die MAC-Authentisierung überlisten.

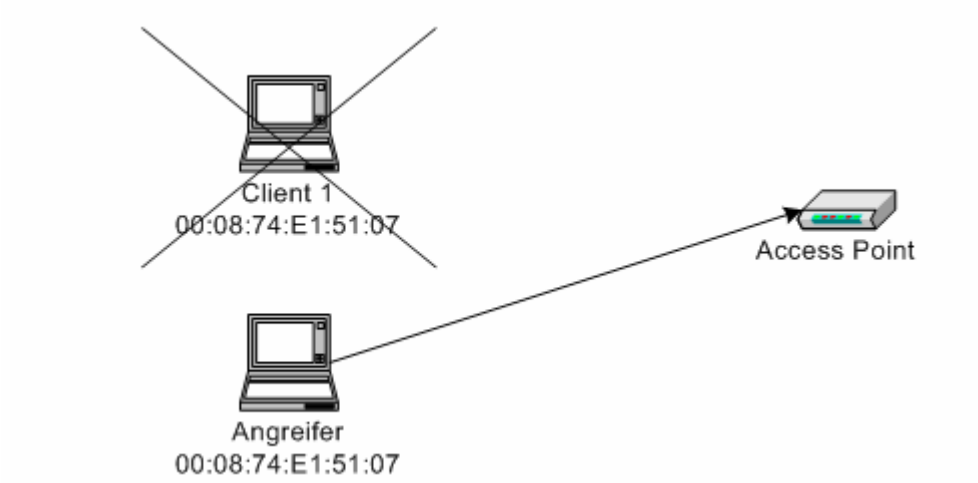


Abbildung 5: MAC-Authentisierung umgehen

Das Anpassen der eigenen MAC-Adresse ist nicht wirklich schwierig. So gibt es zum Beispiel für Windows das Tool smac (http://home.attbi.com/~rbourret/download/smac_1.1.zip), das einem dies komfortabel durchführen lässt. Bei einem Red Hat Linux ab der Version 7.0 kann in der Datei /etc/sysconfig/network-scripts/ifcfg-eth0 die Variable MACADDR angepasst werden:

```
[...]
```

```
IPADDR="192.168.0.1"
MACADDR="00:08:74:E1:51:07"
PROMISC="promisc"
[...]
```

Aber auch die Anpassung mit dem Befehl ifconfig ist möglich. Nachteil dieser Lösung ist, dass die Ethernet-Adresse der Schnittstelle nach einem Neustart des Systems wieder auf den Standard zurückgesetzt wird. Findige Angreifer werden sich dieser Einschränkung bewusst sein und die paar ifconfig-Kommandos in einem Startup-Skript unterbringen:

```
mruef@linux~$ ifconfig wlan0 down
mruef@linux~$ ifconfig wlan0 hw ether 00:08:74:E1:51:07
mruef@linux~$ ifconfig wlan0 up
```

Wardriving – Ein neuer Volkssport

Wir haben gesehen, dass das Angreifern von WLANs sehr einfach sein kann. Es war sodann nur eine Frage der Zeit, bis gelangweilte Gemüter das Einbrechen von Funk-Netzwerken zu ihrem Hobby erkoren würden. Mit einem Laptop und einer Funknetzwerk-Karte bewaffnet machen sich kleine Gruppen von Crackern auf die Suche nach offenen Netzen. Mit dem Auto werden so die interessanten Bezirke der Grossstädte abgeklappert – Deshalb wird dies auch Wardriving genannt. Ottonormalverbraucher wäre erstaunt, wieviele offene Funk-Netzwerke sich beispielsweise im Banken-Viertel von Zürich finden.

Die folgende Karte zeigt einen kleinen Teil der durch www.wardriving.ch gefundenen Access Points im Raum Zürich. Die Informationen werden teilweise gleich mittels GPS-Hardware in den Wardriving-Karten eingesezeichnet. Die meisten Wireless-Scanner bieten heutzutage eine solche Funktionalität. Die blauen Markierungen zeigen Access Points ohne WEP-Verschlüsselung. Das Mitlesen und Einspeisen von Daten ist dort also ein Kinderspiel. Solche Karten existieren für die meisten grösseren Städte. Manchmal sind die Karten nicht öffentlich zugänglich und nur einem kleinen Kreis vorbehalten.

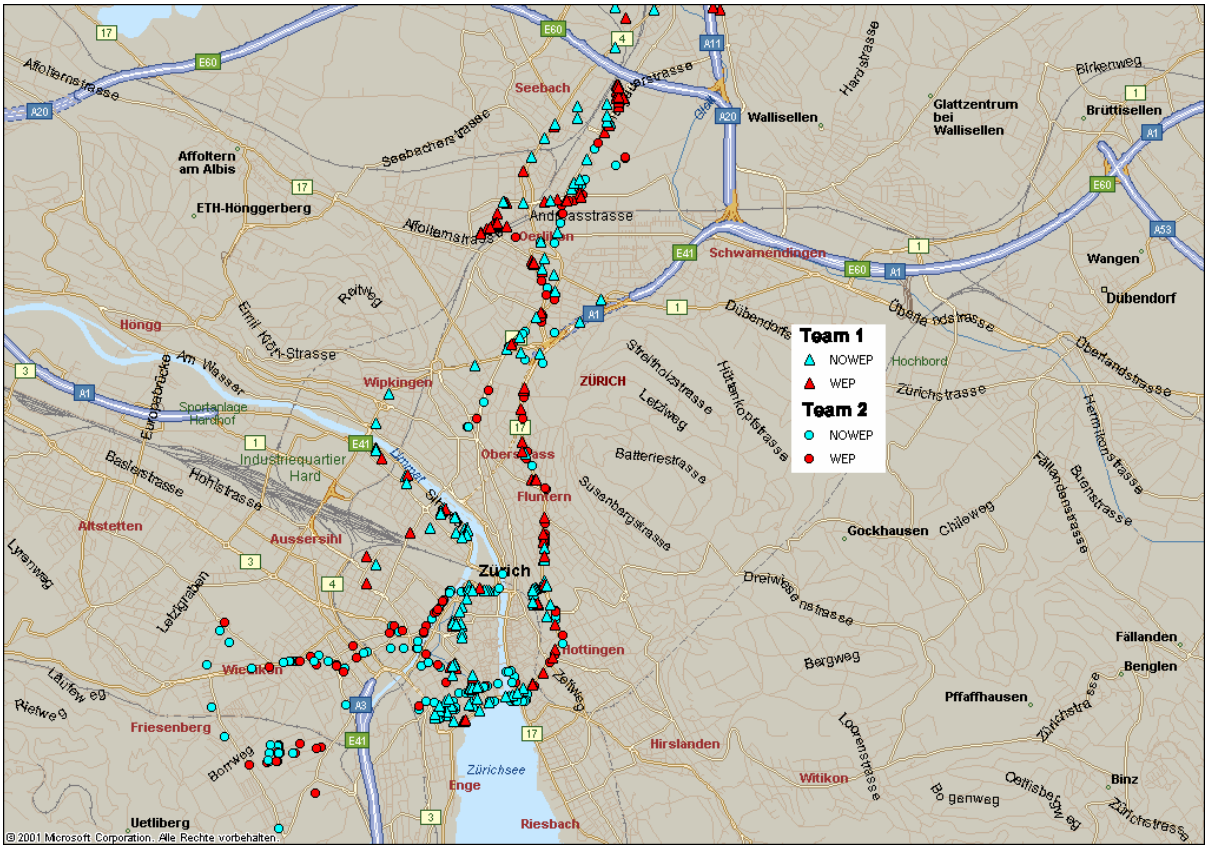


Abbildung 6: Wardriving-Karte von Zürich

Fazit

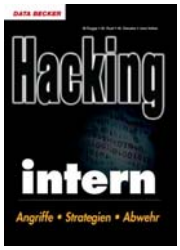
Die Technologie der Funknetzwerke steckt noch in den Kinderschuhen. Dies merkt man vor allem an den sehr schwachen Umsetzungen der Bemühungen zur Wahrung der Sicherheit. Grundlegende Fehler bei der Entwicklung der Standards und der Administration entsprechender Funk-Netzwerke öffnen Angreifern Tor und Angel. Um seine sensitiven und vertraulichen nicht jedem Eindringling auf dem Präsentierteller zu servieren, sollten grundlegende Sicherheitsmassnahmen umgesetzt werden.

Dies schliesst den Einsatz von WEP-Verschlüsselung nicht aus. Aber zusätzlich sollten auf anderen Ebenen die sensitiven Informationen zusätzlich verschlüsselt werden. Altbekannte Mechanismen wie IPsec, SSH (Secure Shell) oder PGP (Pretty Good Privacy) bieten sich da an. Nur so können die Schwächen bei der Entwicklung und Umsetzung von WEP ausbegügelt werden. Desweiteren sollte man auf den Einsatz schwer zu erratender SSIDs setzen und das Broadcasting von diesen Daten verzichten. Dies macht die Administration, vor allem grösserer Funk-Netzwerke, nicht gerade einfacher. Dafür kann man ein bisschen ruhiger schlafen. Als letzte aber nicht zu unterschätzende Möglichkeit sollte man die Filterung der Clients anhand ihrer MAC-Adressen einsetzen. Dadurch können ungebetene Gäste fergehalten werden.

Zwar lassen sich die meisten Sicherheitsmassnahmen mit genügend Zeit und Aufwand umgehen. Aber die meisten Angreifer wollen sich lieber in einem Netz vergnügen, das keine allzu schweren Hürden aufweist.

Über den Autoren

Marc Ruef arbeitet als Security Consultant bei der Firma scip AG (www.scip.ch) in Zürich. Neben dem Umsetzen von Vulnerability Assessments ist er dort unter anderem auch für das Durchführen von Schulungen zum Thema Computersicherheit zuständig. Im September letzten Jahres ist sein Buch mit dem Titel „Hacking Intern“ im Data Becker Verlag erschienen (ISBN 381582284X).



Literaturverzeichnis

Dobkowitz, März 2002, Sicherheit in Wireless LANs, ARtem, http://www.computec.ch/dokumente/wireless/sicherheit_in_wireless_lans/sicherheit_in_wireless_lans.pdf

Diese Publikation der Firma ARtem beschäftigt sich mit der grundlegenden Sicherheitsproblematik von Funk-Netzwerken. Es werden die wichtigsten Elemente dieser Technologie unter die Lupe genommen. Ein guter Einstieg für jederman, der sich noch nicht mit der Materie beschäftigen konnte..

Hagenah, Alexander (aka. Xaitax), 2002, Catching the Air Stuff, http://www.computec.ch/dokumente/wireless/catching_the_air_stuff/catching_the_air_stuff.txt

Diese sehr gelungene Dokumentation berichtet über die Möglichkeiten und Schwachstellen des 802.11-Standards. Sehr gut für den Einstieg geeignet. Eine ältere Version dieses Dokuments kann hier gefunden werden.

Ioannidis, John, Rubin, Aviel D., Stubblefield, Adam, 6. August 2001, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, http://www.cs.rice.edu/~astubble/wep_attack.pdf

Diese Abhandlung beschreibt, wie die durch WEP gegebene Verschlüsselung geknackt werden kann. Das Dokument erregt damals wie heute die Gemüter, denn es beweist Eindrücklich, dass bei der Erstellung des Standards offensichtliche Fehler begangen worden sind. Diese hätten durch open-source, die Einsicht durch die Öffentlichkeit frühzeitig erkannt und behoben werden können.

Ruef, Marc, Gagliardi, Rocco, Zumstein, Simon, 20. April 2002, scip monthly Security Summary – Ausgabe April 2002, http://www.scip.ch

I monatlich erscheinenden E-Magazin der Firma scip AG werden die wichtigsten und interessantesten Security-Themen der letztetn Wochen behandelt. Unter anderem findet sich auch ein Kapitel, das sich dem Beantworten von Fragen widmet. In dieser Ausgabe wird das Thema der Unsicherheit von WLANs behandelt.

Ruef, Marc, Gieseke, Wolfram, Rogge, Marko, Velten, Uwe, September 2002, Hacking Intern, Data Becker, Düsseldorf, ISBN 381582284X, http://www.amazon.de/exec/obidos/ASIN/381582284X/

Dieses Buch führt den Leser in die Welt der Computersicherheit ein. So werden klassische Themen wie Mapping, Scanning, Auswertung und Angriffe beschreiben. Aber auch Computerviren, Trojanische Pferde sowie Firewall- und Intrusion Detection-Systeme werden erläutert.

Schneier, Bruce, Januar 1996, Applied Cryptography – Protocols, Algorithms, and Source Code in C, John Wiley, Chichester, ISBN 0471117099, zweite Auflage, http://www.amazon.de/exec/obidos/ASIN/381582284X/, deutsche Ausgabe, Angewandte Kryptographie – Protokolle, Algorithmen und Sourcecode in C, Addison-Wesley, 15. Mai 1996, ISBN 3893198547, http://www.amazon.de/exec/obidos/ASIN/3893198547/, fünfte Auflage

> Eine schier alles umfassende Enzyklopädie, die in Fachkreisen als das Buch schlechthin gehandelt wird. Die einzelnen kryptographischen Methoden und Algorithmen sind Inhalt des monumentalen Werks, kompakt und kompetent erklärt. Wer sich intensiv mit der Wissenschaft der Geheimschriften auseinandersetzt, der kommt auf seinem Weg früher oder später an diesem Buch vorbei.

Zachhendu, Sebastian, 2002, Sicherheit bei WLANs, http://web.informatik.uni-bonn.de/IV/martini/Lehre/Veranstaltungen/WS0102/Sem_Rechnernetze/Vortraege/Sebastian_Zaccheddu.pdf

> Diese Semesterarbeit führt sehr gut in die Grundlagen der Technik und Sicherheit von WLANs ein. Der Autor erklärt die Grundlagen der Funk-Netzwerke sowie die bekannten Sicherheitsmängel. Gut geeignet, um sich einen Überblick zum Thema zu verschaffen.

Weiterführende Links

Computec – Computer, Technik und Security
http://www.computec.ch/dokumente/wireless/
Deutschsprachige Dokumente über Sicherheit in drahtlosen Netzwerken

scip AG – Security, Consulting, Information, Process
http://www.scip.ch
Beratung bei und Durchführung von Security Assessments

Remote-Exploit.org – Home of Wellenreiter
http://www.remote-exploit.org
Die Webseite von Max Moser beschäftigt sich in erster Linie mit der Sicherheit drahtloser Netze. Hier kann auch sein Wireless-Sniffer namens Wellenreiter gefunden werden.

Kismet
http://www.kismetwireless.net
Die offizielle Webseite des Wireless-Sniffers Kismet

Tools

Windows:

Aerosol, http://www.sec33.com/sniph/aerosol.php
AiroPeek, http://www.wildpackets.com/products/airopeek
ApSniff, http://www.bretmounet.com/ApSniff
ISS Wireless Scanner, http://www.iss.net
Netstumbler, http://www.netstumbler.com
Wlan-expert, http://www.vector.kharkov.ua/download/WLAN/wlanexpert.zip

UNIX/Linux:

AirTools, http://www.dachb0den.com/projects/bsd-airtools.html
AirTraf, http://airtraf.sourceforge.net
Gwireless, http://gwifiapplet.sourceforge.net
Kismet, http://www.kismetwireless.net
PrismStumbler, http://prismstumbler.sourceforge.net
WaveMon, http://www.jm-music.de/projects.html
Wellenreiter, http://www.remote-exploit.org

Macintosh:

Airport, http://homepage.mac.com/macstumbler/airport.tar.gz
AP Scanner, http://homepage.mac.com/typexi/Personal1.html
MacStumbler, http://www.macstumbler.com
KisMAC, http://kismac.binaervarianz.de

Abbildungsverzeichnis