Wireless LAN

Genuss ohne Reue?

Rainer W. Gerling, München*

Ein Wireless LAN (WLAN)[1] oder auch Funk-LAN auf Basis des Standards 802.11b wird massiv mit dem Argument beworben, dass keine Kabel gezogen werden müssen. Dies ist sicherlich in Altbauten ein wichtiges Argument. Aber auch in Konferenz- oder Besprechungsräumen kann auf diese Art schnell und unproblematisch ein Notebook ins Netz gebracht werden. So bequem das auch ist, so bleibt doch die Frage, was bedeutet dies im Hinblick auf die Sicherheit des Firmennetzes. Die Funkwellen machen nicht an der Gebäudewand halt, und der Netzzugriff ist prinzipiell auch vom Firmenparkplatz möglich. Auch in den heute üblichen Technologieparks, wo in einem Gebäude viele Firmen untergebracht sind, ist ein firmenübergreifender Netzzugriff problemlos machbar.

1 Sicherheit im WLAN

Bei der prinzipiellen Art des WLAN sollte man annehmen dürfen, dass es ausgefeilte Sicherheitsfeatures gibt. Auch wird häufig mit 128-Bit WEP-Verschlüsselung geworben. Der eingesetzte RC4-Algorithmus gilt darüber hinaus als sicher. Also gibt es keine Probleme? Leider ist es mal wieder gelungen, aus guten Zutaten eine schlechte Suppe zu kochen.

Ein typisches Wireless LAN besteht aus einem oder mehreren Access-Points und aus Desktop oder Notebook-Rechnern mit entsprechenden Funk-Karten. Die Funkkarten werden von verschiedenen Herstellern angeboten und kosten mittlerweile häufig schon unter 400 DM. Es gibt über-

Abbildung 1: Eine PCMCIA Funk-LAN Karte von SMC. Wenn die Karte in das Notebook gesteckt wird, ragt die Antenne heraus (unten links).

wiegend PCMCIA Karten (Abbildung 1). PCI-Karten bestehen aus einem PCMCIA Adapter für den PCI-Bus und einer PCMCIA Karte. Selbst in die Access-Points (Abbildung 2) wird in der Regel eine PCMCIA Karte für den Funkverkehr eingebaut. An einige PCMCIA Karten lässt sich, um

Abbildung 2: Access-Points der Hersteller Siemens (hinten) und SMC (vorn). Bei dem hinteren Access-Point von Siemens ist deutlich die eingesteckte PCMCIA Karte zu erkennen.

die Reichweite zu erhöhen, eine externe Antenne anschließen. Das Prinzip der Antenne sorgt dafür, dass eine solche Funkkarte immer aus dem Rechner herausragt.

2 Grundlagen des WLAN

Grundsätzlich gibt es zwei Betriebsmodi im Funk-LAN: den AdHock-Modus und den Infrastructure-Modus.

Der AdHoc-Modus wird benutzt, wenn zwei oder mehr Rechner mit einer Funk-Karte direkt miteinander kommunizieren wollen. Es wird spontan ein Netzwerkverbund aufgebaut. Typische Anwendung ist der schnelle Datenaustausch zwischen einigen wenigen Notebooks. Es handelt sich um ein Peer-to-Peer Netzwerk.

Im Infrastructure-Modus verwenden die Klienten einen Access Point um darüber auf das restliche Netzwerk zuzugreifen (Abb. 3). Dabei funktioniert der Access Point quasi als Bridge, die das Funk-Protokoll in das drahtgebundene Protokoll umsetzt. Im Weiteren beschränken wir uns auf den Infrastructure-Modus.

Wenn sich ein Teilnehmer (Klient PC) am Funk-LAN anmelden will, sendet er einen entsprechenden Request. In der einfachsten Form wird eine Open System Authentisierung durchgeführt. Im Wesentlichen wird dabei jeder Klient zum Netzverkehr zugelas-

INHALT:

* Dr. Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft

[1] http://www.wirelessethernet.org

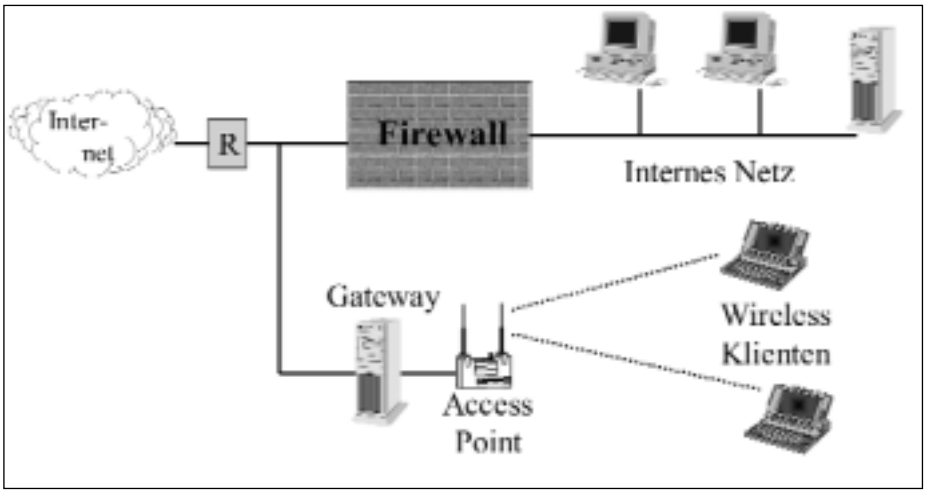

Abbildung 3: Netzstruktur eines Netzes mit einem Access-Point für ein Wireless LAN. Für die Funktion des Gateway siehe Text.

sen. Eine echte Authentisierung findet nicht statt.

Die nächste Stufe der Authentisierung ist die Shared Key Authentisierung. Hierbei wird eine WEP basierte Verschlüsselung eingesetzt. Das bedeutet aber, dass dieses Verfahren nur eingesetzt werden kann, wenn auch ein WEP Schlüssel definiert ist. Im Wesentlichen wird bei diesem Challenge Response Protokoll vom Access Point ein 128 Byte langer Zufallstext an den Klienten geschickt, den dieser mit einem auf beiden Seiten bekannten Schlüssel (=Shared Key) verschlüsseln muss. Als Verschlüsselungsverfahren kommt dabei der RC4 Algorithmus zum Tragen (Details siehe Kasten), da es sich bei um eine Vernam-Verschlüsselung handelt, d.h., ein Schlüsselstrom wird mit dem Klartext per XOR verknüpft. Mathematisch heißt dies

```
s = c XOR Z,
```

wobei c der Klartext, Z der Schlüsselstrom und s der verschlüsselte Text ist. Die Operation geschieht byteweise. Aus den Eigenschaften der XOR-Operation ergibt sich direkt die Umkehrbeziehung

```
c = s XOR Z.
```

Da wir beim Belauschen der Challenge Response Protokolls der Anmeldung sowohl die 128 Byte Klartext (Challenge) als auch den verschlüsselten Text (Response) mitlesen können, kann dieser Teil des Schlüsselstroms problemlos berechnet werden. Damit steht einer Replay-Attacke nichts mehr im Wege. Wenn ein anderer Klient versucht sich anzumelden, sind bis auf den anderen Challenge und die Prüfsumme alle Daten, die verschlüsselt werden, gleich. Das neue Challenge kann aber, der ja der Schlüsselstrom bekannt ist, problemlos verschlüsselt werden.

Diese Schwächen des Protokolls sind schon länger bekannt und publiziert[2].

Bei der WEP Verschlüsselung wird eine auf dem CRC-32 basierende Prüfsumme an die Daten angehängt und mitverschlüsselt. Wegen der Linearität der Prüfsumme kann diese in der verschlüsselten Version ohne Kenntnis des Schlüssels korrigiert werden.

Außerdem wird der Initialvektor dem Datenpaket unverschlüsselt vorangestellt. Auch der Header bleibt unverschlüsselt (Abbildung 4).

Da der WEP-Schlüssel statisch ist, würden alle Datenpakete immer mit dem gleichen RC4-Schlüsselstrom verschlüsselt werden. Dies würde aber die Sicherheit der Verschlüsselung gefährden (Vernam-Verschlüsselungen sind nur sicher, wenn der Schlüsselstrom nie mehrfach benutzt wird). Der Ausweg ist hier die Einführung eines 24-Bit Initialvektors (siehe Kasten). Da es beim WEB-Protokoll keine erzwungenen Regeln für den Initialvektor gibt, kann der Absender ihn frei festlegen. Dies öffnet Replay Attacken Tür und Tor, da der Angreifer einfach bestimmte Initialvektoren mehrfach verwenden kann. Der Initialvektor ist mit seinen 24 Bit auch zu kurz. Bei einem stark genutzten Access-Point mit 11 Mbit Datenrate

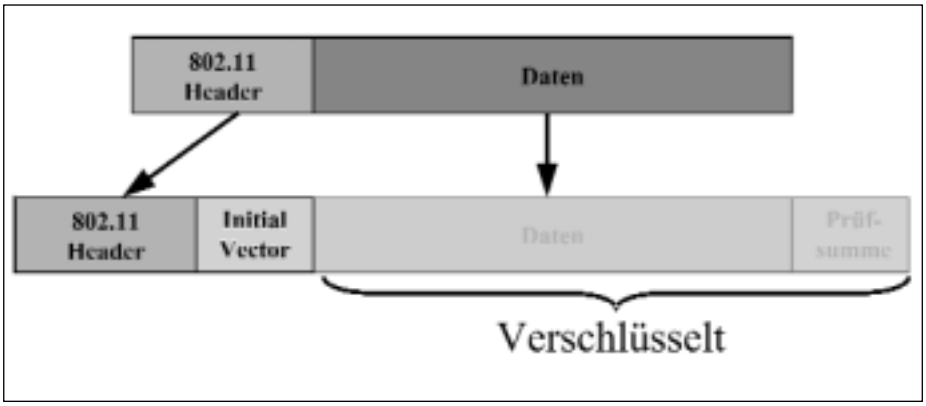

Abbildung 4: Verschlüsselung eines WEP-Paketes. Zur Bedeutung des Initialvektors siehe Text.

dauert es nur wenige Stunden, bis Initialvektoren erneut verwendet werden müssen. Und spätestens dann wird der alte Schlüsselstrom erneut verwendet.

Abbildung 5 zeigt einen typischen Konfigurationsdialog für eine PCMCIA Funk-LAN Karte. Die WEP-Schlüssel sollten immer als HEX-

[2] siehe Links unter http://www.cs.umd.edu/~waa/wireless.html

RC4 oder ARCFour

Der RC4-Algorithmus wurde 1987 von Ron Rivest (RC steht dabei offensichtlich für Rivest Cipher oder Ron's Code) für RSA Data Security Inc. entwickelt. Der Algorithmus war geheim, und man erhielt Informationen über den Algorithmus nur nach Unterschrift eines Nondisclosure Vertrages. Im Herbst 1994 schickte jemand anonym einen Quellcode an die Cypherpunk Mailingliste*. Dank der Kommunikationsstrukturen des Internet breitete sich der Quellcode sehr schnell um die Welt aus. Alle Informationen, die heute über den RC4 Algorithmus bekannt sind, basieren auf diesem Quellcode. Der RC4 Algorithmus mit einer Schlüssellänge von 40 Bit hatte einen speziellen Export-Status in den USA und wurde deshalb in vielen kommerziellen Produkten für die Verschlüsselung benutzt.

Der RC4 Algorithmus ist eine Stromverschlüsselung, d.h., der Zustand der Verschlüsselung hängt von der bisherigen Verschlüsselung ab. Die Struktur des Algorithmus ist sehr einfach und verwendet nur Byte-Variablen. Er besteht aus drei Teilen.

Ein Routine bereitet aus dem Schlüssel die internen Felder vor. Diese Routine muss einmalig vor Beginn der Verschlüsselungsoperationen aufgerufen werden. Ein Feld S mit 256 Elementen wird mit natürlichen Zahlen gefüllt: S[0]=0, S[1]=1, ... S[255]=255. Ein weiteres Feld K mit 256 Elementen wird mit dem Schlüssel gefüllt. K[0]= erstes Byte des Schlüssels, K[2]= zweites Byte des Schlüssels usw. Ist der Schlüssel kürzer als 256 Byte (40 Bit Schlüssel sind 5 Byte und 128 Bit Schlüssel sind 16 Byte lang) so wird der Schlüssel so lange wiederholt, bis alle 256 Feldelemente von K gefüllt sind. Dann wird das Feld S gut durchgemischt. Der eingegebene Schlüssel steuert über das Feld K diese Durchmischung.

```
j=0
für i=0 bis 255
     j=(j+S[i]+K[i]) mod 256
     vertausche S[i] und S[j]i=0
j=0
```

Die Variablen i und j werden noch auf Null gesetzt. Damit ist die Schlüsselvorbereitung abgeschlossen.

Der nächste Teil des Algorithmus kann als ein Pseudo-Zufallszahlengenerator interpretiert werden.

```
i=(i+1) mod 256
j=(j+S[i]) mod 256
vertausche S[i] und S[j]
t=(S[i]+S[j]) mod 256
Z=S[t]
```

Das „Zufallsbyte" Z ist ein herausgenommenes Element aus dem Feld S. Gleichzeitig wird S weiter durchgemischt.

Der aktuelle Wert der Variablen i und j und des Feldes S beschreibt den internen Zustand der Zufallszahlengenerierung. Die Zahl ist gewaltig ($256!*256^2$).

Verschlüsselt wird nun, indem das Zufallsbyte mit dem Klartext XOR-verknüpft wird.

```
s = c XOR Z
```

wobei c ein Byte des Klartextes und s ein Byte des Geheimtextes ist.

Die Geschwindigkeit der Verschlüsselung bzw. der Entschlüsselung ist nicht von der Schlüssellänge abhängig.

Die XOR-Verschlüsselung ist eine sogenannte Vernam-Verschlüsselung oder ein One-Time Pad. Diese Verschlüsselung ist beweisbar sicher, wenn die Zufallsfolge Z zufällig ist, und wenn die Zufallsfolge niemals mehrfach verwendet wird. Der RC4 Algorithmus produziert keine echte Zufallsfolge Z, da diese deterministisch aus dem Schlüssel/Passwort berechnet wird.

Ein weiteres Problem ist die Mehrfachverwendung der Zufallsfolge Z. Werden Datenpakete mit einer durchlaufenden Zufallsfolge verschlüsselt, so bricht mit einem verlorenen Datenpaket die Entschlüsselung ab. Deshalb wird in vielen Protokollen jedes Datenpaket mit einer neu aufgesetzten RC4-Verschlüsselung verschlüsselt. Um zu verhindern, dass ein Zufallsfolge doppelt vorkommt, wird ein sogenannter Initialvektor eingeführt. Bei der Schlüsselvorbereitung wird das Feld K immer abwechselnd mit dem Schlüssel und dem Initialvektor gefüllt. Der Initialvektor wird bei jedem Datenpaket geändert. Damit der Empfänger den Initialvektor kennt, wird er im Klartext mitgeschickt. Wenn Schlüssel und Initialvektor lang genug sind, stellt dies auch prinzipiell kein Problem dar.

---

* Die Cypherpunk Mailingliste kann über majordomo@toad.com abonniert werden. Alte Ausgaben können über ftp://ftp.csua.berkeley.edu/pub/cypherpunks abgerufen werden.

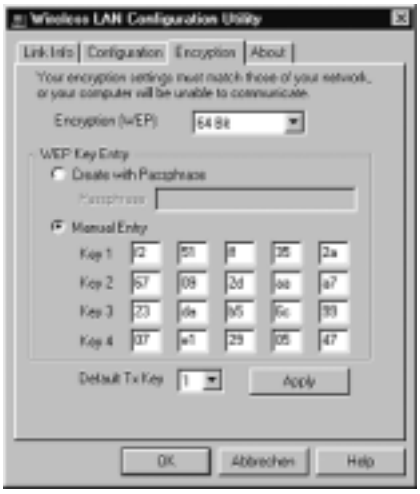

Abbildung 5: Typischer Konfigurationsdialog für WEP. Die Schlüssel sollten in jedem Fall über die HEX-Eingabefelder eingegeben werden, da die Eingabe über Passworte nicht immer zu guten Schlüsseln führt. Bei 64-Bit Verschlüsselung werden 40-Bit Schlüssel eingegeben, bei der 128 Bit-Verschlüsselung ein 104 Bit Schlüssel. Die jeweils fehlenden 24 Bit liefert der Initialvektor. Bei mehreren Schlüsseln muss der Sende-(Tx) Schlüssel angegeben werden.

Schlüssel eingegeben werden. Nur dann ist bei korrekter (d.h. Zufalls-Hex-Zahlen) Eingabe sichergestellt, dass ein zufälliger Schlüssel benutzt wird. Häufig können bis zu vier WEB-Schlüssel eingeben werden. Die Karte kann dann Verbindungen mit allen vier Schlüsseln empfangen, der für das Senden verwendete Schlüssel muss aber explizit ausgewählt werden. Auf Grund des 24-Bit langen Initialvektors werden bei der 64-Bit WEP-Verschlüsselung nur 40 Bit Schlüssel und bei der 128 Bit WEP-Verschlüsselung nur 104-Bit Schlüssel eingegeben.

Da die Schlüssel nur über derartige kryptische Dialoge gewechselt werden können, haben sie eine die Sicherheit gefährdende lange Lebensdauer. Dazu kommt, dass die Schlüssel sich schnell herumsprechen, wenn viele Personen sie benutzen und damit kennen müssen.

Untern Strich ist das WEP-Protokoll eine schönes Lehrbeispiel, was man beim Design eines Krypto-Standards alles falsch machen kann. Derzeit wird am Standard WEP2 gearbeitet. Bis er da ist, muss mit den Sicherheitslücken gelebt werden.

Viele Access Points unterstützen ein Feature, bei dem nur Klienten mit bekannter MAC-Adresse zugreifen dür-

fen. Die MAC-Adresse ist eine Eigenschaft der Netzwerkkarte. Sie ist 6 Byte lang und sie mit einem Netzwerksniffer abgehört werden. Da bei einigen Netzwerkarten die MAC-Adresse per Software geändert werden kann, stellt dies keine absolute Sicherheit dar. Diesen Zugriffschutz sollte man trotzdem aktivieren. Der Pflegeaufwand ist bei häufig wechselnden Notebooks groß, da die MAC-Adressen dann entsprechend oft geändert werden müssen. In statischen Netzen (d.h. wenn immer die gleichen Notebooks das Funk-LAN nutzen) hält sich der Aufwand jedoch in Grenzen.

3 Platzierung des Access Points im Unternehmensnetz

Da Fehler bei der Konfiguration oder bisher unbekannte Sicherheitslücken nie ganz ausgeschlossen werden können, sollten das drahtgebunden und das funkbasierte Firmennetz komplett getrennt werden. Nur so kann sicher gestellt werden, dass Sicherheitslücken im Funknetz sich nicht auf das Firewall-geschützte klassische Netz auswirken.

Die Access-Points sollten wohlüberlegt platziert werden, so dass sich der Aufwand der separaten Verkabelung in Grenzen hält. Bei der heute üblichen strukturierten Verkabelung lässt sich das separate Funknetz durch geeignete Verbindungen am Patchfeld leicht herstellen.

Der Access Point sollte schon die möglichen „Sicherheitsfeatures“ wie Shared Key Authentisierung und MAC-Zugangskontrolle verwenden. Auf eine WEP-Verschlüsselung sollte aber verzichtet werden, um die CPU-Last des Access-Points nicht unnötig in die Höhe zu treiben (siehe weiter unten).

Da die Wireless Klienten vor der Firmenfirewall sind, sind sie aus Sicht der Sicherheitspolicy außerhalb und nicht vertrauenswürdig. Da sie adressmäßig aber zur Firma gehören können Eindringlinge in das Funk-LAN der Firma sehr wohl Schaden zufügen. Wird der Zugang zum Internet über ein PPTP oder IPsec Gateway blockiert, so können die besseren Sicherheitsfeatures dieser Protokolle genutzt werden. Alle anderen Verbindungen werden von diesem Gateway blockiert (siehe Abbildung 3).

Damit kann ein potentieller Angreifer nur diesen Gateway und die anderen Klienten angreifen. Der Gateway kann durch entsprechend sorgfältige Installation (härten) geschützt werden. Die anderen Klienten müssen, soweit möglich, durch Desktop-Firewalls geschützt werden.

4 Verschlüsselte Tunnel

In den Wireless Access-Points werkelt häufig nur ein (gemessen an heutigen Desktop- oder Notebook-CPUs) sehr schwacher Prozessor. Wird WEP benutzt, muss diese CPU die gesamte Ver- und Entschlüsselungsleistung erbringen. Damit wird im Allgemeinen der verschlüsselte Durchsatz von der Leistungsfähigkeit dieser CPU abhängen. Deshalb macht es Sinn, die Verschlüsselung auf ein leistungsfähigeres Krypto-Gateway auszulagern. Hier sind im Prinzip zwei Verfahren denkbar: PPTP[3] oder IPsec[4]. Obwohl PPTP von B. Schneier ziemlich kritisiert wird[5], bietet es mehr Sicherheit als WEP. Aktuell wird die Diskussion über die PPTP Sicherheit durch die Publikation von entsprechenden Angriffstools durch Freiburger Student[6]. Durch 14 Zeichen lange gut gewählte PPTP Passworte (NT-Passworte) kann der beschriebene Angriff erheblich erschwert werden.

PPTP ist für Windows, MAC und Linux/UNIX problemlos verfügbar. Außerdem existieren Hardwarelösungen für PPTP. Die Kompatibilität der Versionen untereinander ist gut. Die deutschen Universitäten setzen in ihren Funk-LAN Installationen häufig PPTP ein[7]. Auf den WWW-Seiten der Uni-Rechenzentren finden sich auch ordentliche Anleitungen zur Installation unter den verschiedenen Betriebssystemen.

IPsec ist wesentlich sicherer, aber auch schwieriger zu installieren und zu konfigurieren. Erste IPsec Angebote kombinieren die LAN-Verschlüsselung mit integrierten Firewall-Lösungen[8].

5 Zusammenfassung

Die Sicherheitsmechanismen des 802.11 Standards sind beim heutigen Stand der Technik nicht ausreichend, da sie gegen fundamentale Regeln der Kryptographie verstoßen. Sie bedürfen dringender Nachbesserung.

Vor diesem Hintergrund ist es erforderlich, beim Einsatz eines Funk-LANs selber für die Sicherheit zu sorgen. Hierzu müssen Protokolle wie PPTP (bei geringen Sicherheitsanforderungen) oder IPsec verwendet werden. Diese erledigen dann auch gleich die Authentisierung.

Die Klienten im Funk-LAN sind durch Desktop-Firewalls vor Angriffen im Funk-LAN selber zu schützen. Der Zugriff vom Funk-LAN auf andere Ressourcen (drahtgebundenes Firmennetz, Internet) ist durch eine Firewall zu schützen.

Trotzdem sollten MAC-basierte Zugangskontrolle und SIID aktiviert werden. □

[3] http://infodeli.3com.com/infodeli/tools/remote/general/pptp/pptp.htm

[4] http://www.vpnc.org/ oder auch http://www.freeswan.org

[5] http://www.counterpane.com/pptp.html

[6] http://mopo.informatik.uni freiburg.de/pptp_mschapv2/

[7] z.B. http://www.lrz-muenchen.de/services/netz/mobil/vpn/ oder http://funk.stud.uni-goettingen.de/

[8] z.B. PGPnet und PGPfire von NAI: Siehe unter www.pgp.com