Sicherheit in WLANs

Florian Müller

Januar 2003

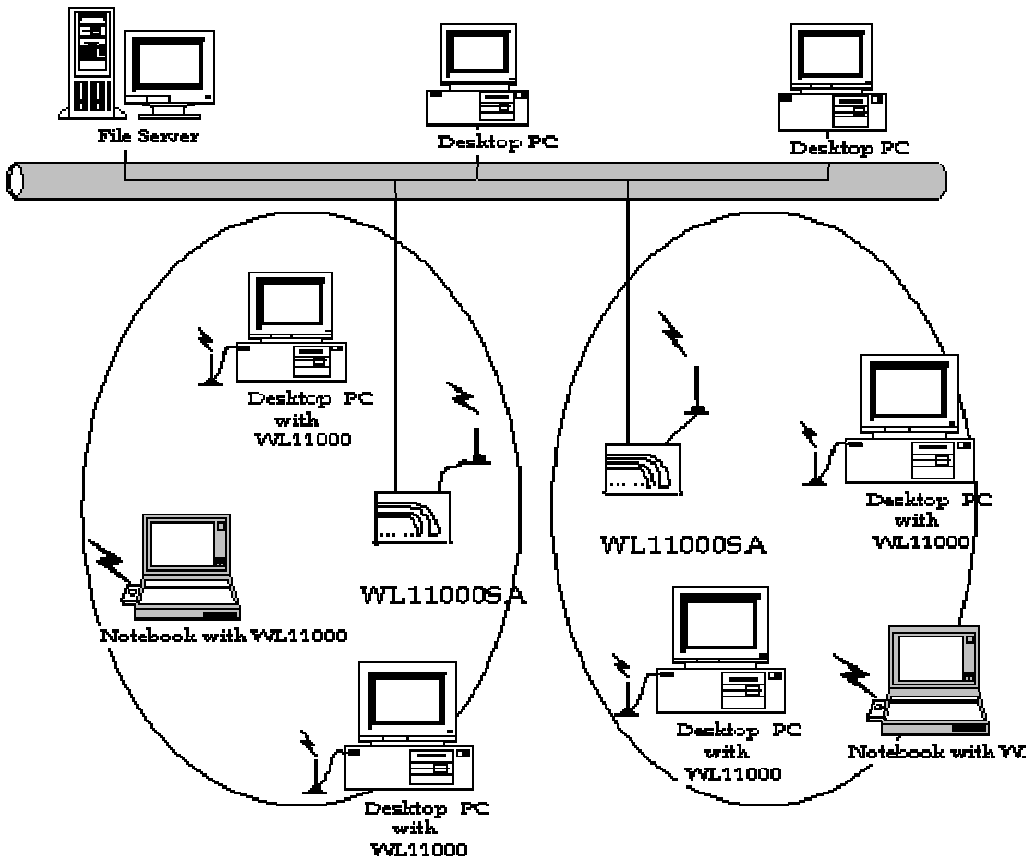
Inhaltsverzeichnis

Einleitung

Dieses Dokument gibt einen Überblick über die Sicherheit der sich mittlerweile schnell verbreitenden Infrastruktur Wireless LANs (Local Area Network). Diese Netzwerke sind sehr beliebt, da sie es erlauben, auch mobile Clients komfortabel in ein LAN zu integrieren.
Es wird zuerst der generelle Aufbau eines Infrastruktur WLANs beschrieben und welche Sicherheitsaspekte für die Absicherung eines solchen Netzwerkes von wesentlicher Bedeutung sind.
Im folgenden dritten Teil schließt sich eine Beschreibung über die Umsetzung der Sicherheitsmechanismen an, welche die geforderten Sicherheitsaspekte umsetzen sollen. In diesem Kapitel werden die einzelnen Mechanismen zur Wahrung der Sicherheit detailliert dargestellt, damit deutlich wird, auf welchem Wege die Sicherheit im WLAN erreicht werden soll.
Der vierte Teil beschäftigt sich mit den Schwachstellen in den Sicherheitsmechanismen und deren Folgen für die Sicherheit in einem Funknetzwerk. Jeder Sicherheitsmechanismus wird separat daraufhin untersucht, ob die angestrebten Sicherheitsaspekte auch wirklich erfüllt werden.
Im letzten Teil werden Möglichkeiten zur Verbesserung der Sicherheit in einem WLAN abgehandelt. Hier sollen die Mechanismen all jene Defizite der Sicherheitsmechanismen des dritten Teils ausgleichen, um so eine sichere Kommunikation in einem Wireless LAN zu gewährleisten.

1. Funktion und Aufbau von (Infrastruktur) Wireless LAN

Ein Infrastruktur Wireless LAN (Local Area Network) besteht aus einem oder mehreren Access Points, über welche die Computer mit ausgestatteten WLAN Adaptern (Clients) miteinander kommunizieren. Hierbei läuft jeglicher Datenverkehr zweier WLAN Adapter über einen Access Point, eine direkte Kommunikation zwischen den WLAN Adaptern findet nicht statt. Die Access Points sind mit sogenannten Radial-Antennen ausgestattet, d.h. sie können in einem bestimmten Radius um sich herum kommunizieren. Dies ist notwendig, damit man sich im WLAN frei bewegen kann, wenn man z.B. einen Laptop mit WLAN Adapter in einem Netzwerk einsetzt.
Durch diesen Aufbau ist es physikalisch einfacher in ein WLAN einzudringen als in ein verkabeltes LAN. Zum Einbruch in ein WLAN muß man sich nur in dem Funkbereich eines Access Points aufhalten, währenddessen man sich bei einem kabelgebundenem Netzwerk an die Verkabelung anschließen muß oder über das Internet mit dem Netzwerk kommuniziert..



2. Sicherheit in Wireless LANs

Für die sichere Kommunikation im Funk-LAN müssen verschiedene Sicherheitsaspekte beachtet werden, damit der Zugriff und die Veränderung von Daten durch nicht berechtigte Personen verhindert wird.

2.1 Integrität von Daten

Unter Integrität von Daten versteht man, daß die Daten während der Übertragung nicht verändert werden dürfen bzw. Daten, die während der Übertragung zum Empfänger geändert wurden, sofort als solche erkannt werden. Hiermit wird verhindert, daß Daten während der Übertragung unbemerkt durch Dritte verändert werden.

2.2 Authentizität von Daten und Nutzer

Authentizität von Daten und Nutzer bedeutet, daß der Absender der Daten, der gegenüber dem Empfänger versichert, ein bestimmtet Absender zu sein, auch wirklich dieser Absender der Daten ist. D.h. es muß verhindert werden, daß irgendein Absender Daten unter dem Vorwand eines bestimmten Absenders an den Empfänger schickt. Hiermit wird u.a. verhindert, daß Dritte in eine bestehende Kommunikation gefälschte Datenpakete einschmuggeln.

2.3 Vertraulichkeit von Daten

Vertraulichkeit ist ein weiterer wichtiger Faktor für die sichere Kommunikation. Unter manchen Umständen muß gewährleistet sein, daß übertragene Daten zwischen Sender und Empfänger nicht abgehört und nur vom Empfänger gelesen werden können.

3. Sicherungsmechanismen in Wireless LANs

In WLAN Komponenten gibt es verschiedene Sicherungsmechanismen, welche in dem Standard IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 ausgearbeitet wurden und die unter Punkt 2 genannten Sicherheitsaspekte umsetzen, um eine sichere Kommunikation über Funk zu gewährleisten.

3.1 „geschlossenes WLAN“ - Verstecken der ESSID

Jedes WLAN hat eine sogenannte ESSID (*Electronic Service Set Identifier*). Hierbei handelt es sich um den Namen des Funknetzwerks, welches aus einem oder mehreren Access Points bestehen kann. Die Clients, welche mit dem Funknetzwerk kommunizieren wollen, müssen diese ESSID kennen und bei der Anmeldung an das Funknetzwerk verwenden. Die Access Points lassen sich so einstellen, daß sie entweder die ESSID via Broadcast im Empfangsradius aussenden oder dies unterlassen. Im Zweiten Fall müssen die Clients die ESSID eines Funknetzwerks genau kennen, um mit ihm kommunizieren zu können, alle anderen Teilnehmer sind von der Kommunikation zu diesem WLAN ausgeschlossen [5].

3.2 MAC-Adressen Zugriffskontrollisten

Mehrere Hersteller haben über den Standard IEEE 802.11 hinaus noch eine weitere Sicherheitsstufe in ihre WLAN Access Points integriert, um so die Sicherheit im WLAN zu verbessern. In den Access Points sind sogenannte Zugriffskontrollisten (*engl.* Access Control Lists) integriert, welche sich bei Bedarf aktivieren lassen. Diese sind dazu da, um nur bestimmte Clients an der Kommunikation zu dem Funknetzwerk teilhaben zu lassen. Nur Clients, welche eine in der Zugriffskontrolliste eingetragene MAC-Adresse (Media Access Control) aufweisen, dürfen mit dem Access Point kommunizieren [3].

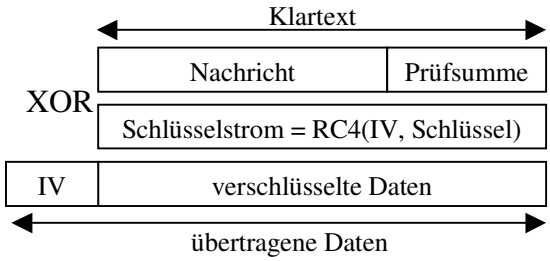
3.3 Wired Equivalent Privacy (WEP) Verschlüsselung

Viele WLAN Komponenten unterstützen zudem noch die WEP (Wired Equivalent Privacy) Verschlüsselung, welche in dem Standard IEEE 802.11 ausgearbeitet wurde und die Vertraulichkeit und Integrität von Daten zusichern soll. Diese Verschlüsselung ist allerdings in dem Standard als optional deklariert, d.h. die Komponenten müssen diese Verschlüsselung nicht zwingend unterstützen [1].
Bei der WEP Verschlüsselung handelt es sich um eine symmetrische Verschlüsselung, d.h. zum Ver- und Entschlüsseln wird ein gemeinsamer geheimer Schlüssel benutzt, den nur Sender und Empfänger kennen dürfen. Als Verschlüsselung wird eine sogenannte Stromverschlüsselung eingesetzt, hierbei werden die Daten bitweise verschlüsselt.
Der WEP Algorithmus setzt eine XOR Verschlüsselung ein, jedes Bit des Datenstroms wird mit dem entsprechenden Bit des Verschlüsselungsstroms über ein Exklusiv-Oder verknüpft.

Hiermit sieht man sofort, daß die zweimalige Hintereinanderausführung den ursprünglichen Inhalt des Datenbits widerspiegelt, dies ist ganz wichtig, da die Daten durch Anwendung der XOR-Verknüpfung verschlüsselt und bei nochmaliger Verknüpfung wieder entschlüsselt werden [2]. Die Verschlüsselung mit der XOR-Verknüpfung wird in der folgenden Tabelle verdeutlicht:

Datenstrom	1	1	0	0	1	0	1	0	0	1
Verschlüsselungsstrom	0	1	1	1	0	0	1	1	0	0
Verschlüsselte Daten	1	0	1	1	1	0	0	1	0	1

Da der Schlüssel für die Daten nicht öffentlich zugänglich sein darf und der Schlüsselstrom genauso groß wie der Datenstrom ist, muß für die Erzeugung des Schlüsselstroms ein Algorithmus angewendet werden, der aus dem geheimen Schlüssel diesen Verschlüsselungsstrom berechnet. Als Basis für die Erzeugung des Schlüsselstroms wird der 1987 von Ron Rivest entwickelte RC4-Algorithmus eingesetzt. Der RC4-Algorithmus berechnet aus dem geheimen Schlüssel und einer weiteren Zahl, dem sogenannten Initialisierungsvektor (IV), welcher bei der WEP-Verschlüsselung 24 Bit umfaßt, den Schlüsselstrom [6, 7]. Bei der Verschlüsselung durch den WEP-Algorithmus wird jedes zu versendende Datenpaket einzeln verschlüsselt.
Zuerst wird von den Nutzdaten eines jeden Datenpakets eine Prüfsumme, welche die Datenintegrität garantieren soll, berechnet und an die Daten angehängt, danach wird der Schlüsselstrom für das Datenpaket erzeugt, wobei für jedes Datenpaket ein neuer Initialisierungsvektor benutzt wird, damit soll gewährleistet sein, daß für die Verschlüsselung verschiedener Datenpakete nicht der gleiche Schlüsselstrom benutzt wird. Danach werden die Nutzdaten inklusive Prüfsumme zur Sicherung der Vertraulichkeit mit dem Schlüsselstrom verschlüsselt und der Initialisierungsvektor den verschlüsselten Daten vorangestellt [2]. Im Folgenden ist die Verschlüsselungsprozedur noch einmal grafisch dargestellt:



3.4 Benutzerauthentifizierung

Für die Authentifizierung von Benutzern gibt es im IEEE Standard 802.11 zwei Authentifizierungs-Mechanismen: *Open System* und *Shared Key*. Die Open System Authentifizierung erlaubt eine Authentifizierung ohne Identifizierung des Benutzers. Die Shared Key Authentifizierung erfolgt mittels des geheimen WEP-Schlüssels. Der zu authentifizierende Client erhält vom Access Point eine zufällig generierte Nachricht, welche er mittels des WEP-Algorithmuses und des WEP-Schlüssels verschlüsseln muß. Daraufhin schickt der Client die Nachricht an den Access Point zurück. Dieser entschlüsselt die Nachricht und überprüft, ob die entschlüsselte Nachricht mit der zuvor an den Client gesendeten Klartextnachricht übereinstimmt. Stimmen die Nachrichten überein, so wird der Client authentifiziert [1].

4. Schwachstellen in den Sicherheitsmechanismen

Eine immer weitere Verbreitung von WLAN Komponenten und eine umfangreiche Analyse hat zu Tage gebracht, daß die in dem Standard IEEE 802.11 entwickelten und von den Herstellern implementierten Sicherheitsmechanismen ihren Zweck nur bedingt erfüllen.

4.1 Abfangen der ESSID

Das Verstecken der ESSID im Funknetzwerk trägt nur wenig zur Sicherheit bei. Angreifer haben zwar keine Möglichkeit über Broadcast den Netzwerknamen in Erfahrung zu bringen, wenn diese Funktion abgeschaltet ist, jedoch muß jeder zugehörige Teilnehmer eines Funknetzwerks sich zuerst gegenüber dem Funknetzwerk authentifizieren, wenn er darüber kommunizieren will. Für die Authentifizierung ist es unumgänglich, daß ein Client die gültige ESSID an einen Access Point des Funknetzwerks übermittelt, da durchaus mehrere verschiedene Funknetzwerke in einem Empfangsradius existieren können. Während der Authentifizierung überträgt ein Client die ESSID allerdings im Klartext zum Access Point, die ein Angreifer abhören kann [3, 5].

4.2 MAC Adressen Zugriffskontrollisten

Die Absicherung eines Funklans über Zugriffskontrollisten ist ebenfalls nicht sicher, zwar lassen sich Teilnehmer mit unbekannten MAC Adressen von der Nutzung des Netzwerks aussperren, doch läßt sich dieser Mechanismus mit einfachen Mitteln überwinden. MAC Adressen müssen während der Kommunikation unverschlüsselt übermittelt werden (auch wenn WEP Verschlüsselung eingesetzt wird), da hierüber eindeutig Sender und Empfänger von Datenpaketen festgelegt werden, somit ist es einfach möglich, gültige MAC Adressen abzuhören. Des Weiteren lassen sich bei fast allen WLAN Karten die MAC Adressen softwaremäßig ändern. Nachdem eine gültige MAC Adresse abgehört wurde, kann ein Angreifer sein WLAN Adapter auf diese MAC konfigurieren und diese benutzen [3].

4.3 Wired Equivalent Privacy (WEP) Verschlüsselung

Die WEP Verschlüsselung ist ebenfalls nicht so sicher, wie sie verspricht. Vielmehr wird dem Anwender eine Sicherheit wie in einem Kabelnetzwerk vorgetäuscht, was zur Folge haben kann, daß Anwender sorglos mit sensiblen Daten umgehen. Es gibt mehrere Techniken trotz WEP Verschlüsselung Zuriff auf Daten zu erlangen und das Netzwerk zu kompromittieren.
Bei längerer Datenübertragung besteht die Möglichkeit, daß für mehrere Datenpakete der gleiche Verschlüsselungsstrom benutzt wird, weil der gemeinsame geheime Schlüssel nur relativ selten gewechselt wird, da alle Teilnehmer im Netzwerk den selben Schlüssel benutzen und der Wechsel des Schlüssels im Funknetzwerk somit administrativ ziemlich aufwendig ist. Wenn man davon ausgeht, daß ein gut ausgelasteter Access Point eine dauerhafte Datentransferrate von 5Mb/s (ca. 436 Datenpakete/s mit je 1500 Bytes) hat und für jedes Paket ein Verschlüsselungsstrom aus dem statischen geheimen Schlüssel und einem zuvor nicht benutzten 24-Bit IV erzeugt wird, trifft man nach ca. 12 Stunden auf ein Datenpaket mit IV eines bereits zuvor verschickten Pakets, da in dieser Zeit über 2^{24} Datenpakete verschickt

wurden. Wird der IV zufällig ausgewählt, läßt sich hier das sogenannte Geburtstagsparadoxon (gibt die Wahrscheinlichkeit an, daß zwei Menschen am gleichen Tag Geburtstag haben bzw. hier, daß zwei Datenpakete den gleichen IV haben) anwenden und bereits nach ca. 5000 Paketen werden mit hoher Wahrscheinlichkeit Pakete mit doppelten IV auftauchen. Hinzu kommt noch, daß der WEP Standard nicht vorschreibt, daß der IV nach jedem Paket gewechselt werden muß, und daß viele PCMCIA Karten jedesmal nach der Initialisierung den IV auf 0 setzen und bei jedem Paket um eins inkrementieren.
Wenn man es jetzt noch erreicht, zu den IV den Schlüsselstrom zu berechnen, lassen sich so alle folgenden Datenpakete mit gleichen IV dekodieren, da diese ebenfalls mit dem gerade berechneten Schlüsselstrom verschlüsselt wurden und die Vertraulichkeit der Daten kann nicht mehr gewährleistet werden.

```
P = bekannter Klartext
C = bekannter verschlüsselter Klartext

C = P xor RC4(v,k)

_____________________________________________

C xor P⇔ (P xor RC4(v,k)) xor P
       ⇔ P xor (RC4(v,k) xor P)
       ⇔ P xor (P xor RC4(v,k))
       ⇔ (P xor P) xor RC4(v,k)
       ⇔ 0 xor RC4(v,k)
       ⇔ RC4(v,k)
```

Die Vorgehensweise ist hier relativ einfach, da viele Felder in den Paketdaten standardmäßig schon vorbelegt sind, z.B. durch TCP/IP Protokollheader. Die einfachste Methode ist, man schickt einfach IP-Pakete an den Rechner, welchen man im WLAN gerade abhört, hierzu muß man allerdings die IP-Adresse des abzuhörenden Rechners kennen. Dies läßt sich je nach Anbindung des Funknetzwerks an das „normale“ Netzwerk mit wenig oder etwas mehr Aufwand betreiben, z.B. mittels ARP-Spoofing bzw. durch gezieltes Schicken von Emails und warten bis der Nutzers diese über das WLAN abruft. In der Email selbst kann man wieder Verknüpfungen mit Bildern oder anderen Dateien, deren Inhalt der Angreifer genau kennt, anbringen, welche dann automatisch heruntergeladen werden. Um Emails zu tarnen, kann man sie einfach als SPAM deklarieren, so daß kein Verdacht aufkommt, wenn diese Nachricht über das WLAN heruntergeladen wird.
Hat man jetzt zu einem verschlüsselten Datenpaket auch deren unverschlüsselten Daten zugeordnet, läßt wie in der obigen Box dargestellt einfach der Verschlüsselungsstrom berechnen. Da die XOR-Verknüpfung kommutativ ist, lassen sich die Parameter beliebig gegeneinander vertauschen, ohne das Ergebnis zu beeinflussen. Führt man jetzt eine XOR-Verknüpfung zwischen dem verschlüsselten Text (C) und dem unverschlüsselten Text (P) durch sieht man nach vertauschen der Parameter, daß sich die Klartexte aus dem verschlüsselten Text und dem zusätzlichen Parameter herauskürzen (P xor P = 0) [2].
Als Ergebnis bleibt dann nur noch der Schlüsselstrom übrig, welcher zur Verschlüsselung des Datenpakets benutz t und nun dem bekannten IV zugeordnet werden kann. Nach weiterer Analyse der übertragenen Daten im WLAN kann man sich als Angreifer eine Datenbank aufbauen, die dem IV den zugehörigen Schlüsselstrom zuordnet. Für 2^{24} Initialisierungsvektoren fallen dafür ca. 24GB an Daten an. Dies gilt aber nur, wenn man

wirklich alle IV analysiert, was eigentlich nicht notwendig ist, da wie oben beschrieben bei vielen häufig eingesetzten PCMCIA WLAN Adaptern wenige IV oftmals wiederverwendet werden [2]. Wer sich diesen Aufwand nicht machen will, kann sich bereits den vorhandenen Programmen „Wepcrack“ oder „Airsnort“ zum knacken der WEP-Verschlüsselung bedienen [5].

Auch die in den Datenpaketen eingesetzten CRC-32-Checksummen für die Datenintegrität lassen sich, da linear, leicht aufschlüsseln und zusammen mit einer veränderten Nachricht neu erstellen, deswegen kann hier auch nicht die Datenintegrität gewährleistet werden [2].

4.4 Shared Key Authentifizierung

Die Shared Key Authentifizierung erlaubt es Angreifern, Schlüsselströme zu IV noch einfacher zu berechnen als unter Punkt 4.3 beschrieben. Die Schwachstelle während der Authentifizierung liegt darin, daß zwischen Client und Access Point nacheinander eine Klartextnachricht und basierend auf einem IV die zugehörige verschlüsselte Nachricht ausgetauscht werden. Ein Angreifer, welcher diesen Prozeß abhört, erhält so ebenfalls beide Nachrichten. Durch die Exklusiv-Oder-Verknüpfung erhält der Angreifer sehr leicht den Schlüsselstrom zu einem bestimmten IV [3].

4.5 Denial of Service (DoS) im WLAN

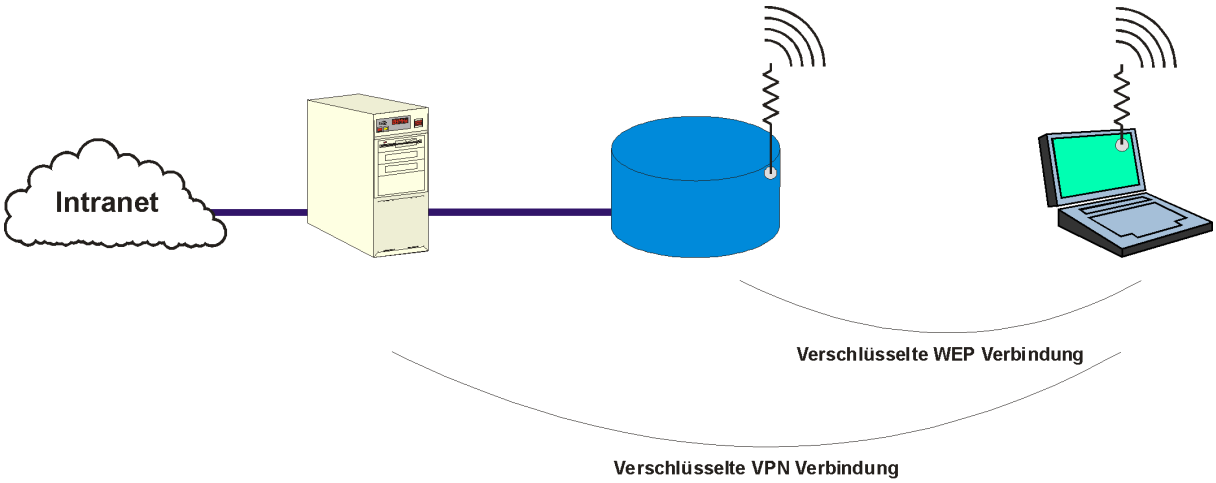
In einem WLAN ist es auf einfachste Weise möglich, ein Netzwerk zur Dienstverweigerung (*engl.* Denial of Service) zu zwingen. Dies liegt nicht an dem WLAN selbst, sondern ist vielmehr ein Problem, das viele Funkübertragungssysteme betreffen kann.
Ein Angreifer kann mit seiner WLAN-Karte so viele unzulässige Datenpakete zum Access Point eines Funknetzwerks schicken, so daß gültige Daten gar nicht oder nur noch schwer den Access Point erreichen. Des Weiteren kann ein Angreifer mit entsprechender technischer Ausstattung das Frequenzband, auf dem Daten im WLAN übertragen werden, stören. Aufgrund dieser Störungen auf den Datenübertragungskanälen wird von den WLAN-Komponenten automatisch die Datenübertragungsrate gedrosselt, um die Daten möglicherweise trotz der Störungen doch noch fehlerfrei übertragen zu können. Ein Angreifer kann aber so starke Störungen auf den Frequenzen verursachen, daß es nicht mehr möglich ist, irgendwelche Daten darüber zu übertragen und die WLAN-Komponenten ihre Kommunikation einstellen müssen [14].
Abhilfe kann man hier nur schaffen, indem die Quelle der Störungen lokalisiert und entfernt wird, was bei mobilen Störquellen aber schon ein aufwendiges Problem darstellen kann.

5. Verbesserung der Sicherheit

Da die z.Zt. zur Verfügung stehenden Mechanismen im Standard IEEE 802.11 Schwächen gegenüber Angriffen von außen aufweisen, müssen zur Gewährleistung einer sicheren Datenübertragung über WLAN weitere Sicherungsmaßnahmen auf höheren Schichten integriert werden. Gegenwärtig wird auch an einer Verbesserung am IEEE-Standard 802.11 gearbeitet, um WLANs in Zukunft sicherer gegenüber Attacken zu machen.

5.1 Verschlüsselung auf höherer Ebene

Für die Verschlüsselung von Daten auf höherer Ebene gibt es mehrere Alternativen, mit dem Vorteil, daß sie schon vielfach getestet sind, da sie bereits bei kabelgebundenen Netzwerken wie z.B. bei VPN (Virtuelles Privates Netzwerk) über das Internet zum Einsatz kommen. Das WLAN läßt sich zusätzlich so absichern, daß über das WLAN nur Daten durch einen VPN-Tunnel übertragen werden, hierzu ist es notwendig, daß die Daten vom Access Point an einen zuständigen VPN-Server geleitet werden.



Durch die Übertragung der Nutzdaten im WLAN durch einen VPN-Tunnel soll verhindert werden, daß ein Angreifer durch abgehörte Datenübertragungen die zugehörigen Schlüsselströme für ein IV berechnen und damit weitere Datenpakete dekodieren kann. Im VPN-Protokoll werden wesentlich komplexere Verschlüsselungsprotokolle eingesetzt, die es nicht erlauben, daß Daten auf so einfache Weise wie bei der WEP-Verschlüsselung unberechtigt dekodiert werden können. Eine einfache Änderung der linearen CRC-32 Prüfsumme wie bei der WEP-Verschlüsselung ist bei VPN getunnelten Daten ebenfalls nicht so einfach möglich, da hier auch Prüfsummen bzw. Signaturen eingesetzt werden, welche z.B. durch sichere Hash-Funktionen berechnet werden. Die Authentifizierung wird im VPN auch besser abgesichert als bei der WEP-Verschlüsselung, da an dieser Stelle durch den Austausch von Zertifikaten und der besseren Verschlüsselungsmechanismen der Authentifizierungsvorgang nicht abgehört werden kann. Der Einsatz von VPN im WLAN ist auf jeden Fall ein Sicherheitsgewinn, da ein Angreifer zusätzliche Sicherheitsmechanismen überwinden muß, um an die Nutzdaten zu gelangen.

Gebräuchliche Protokolle sind PPTP(Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol) und IPSec (Internet Protocol Security), auf die Protokolle PPTP und IPSec wird näher eingegangen und gezeigt, wie mittels einer VPN Verbindung die Sicherheit im WLAN erhöht werden kann [9]. Die wichtigsten Eigenschaften beider Protokolle sind im Folgenden tabellarisch gegenübergestellt:

Eigenschaft	PPTP	IPSec
Protokoll-Ebene	**Schicht 2**	**Schicht 3**
Standard	**Nein**	**Ja**
Paket-Authentifizierung	**Nein**	**Ja**
Benutzer-Authentifizierung	**Ja**	**Ja**
Datenverschlüsselung	**Ja**	**Ja**
Schlüsselmanagement	**Nein**	**Ja**
QoS (Quality of Service)	**Nein**	**Ja**
Andere Protokolle (neben IP) tunnelbar	**Ja**	**z.Zt. noch nicht**
Punkt-zu-Punkt Sicherheit	**Ja**	**Ja**

5.1.1 PPTP (Point-to-Point Tunneling Protocol)

Beim PPTP handelt es sich um ein von Microsoft und Ascend entwickeltes Protokoll, welches als Erweiterung des Point-to-Point Protocols (PPP) erlaubt, PPP-Datenpakete über ein IP-Netzwerk zu tunneln. Das PPTP arbeitet auf Schicht 2 des ISO/OSI (Industrie Standards Organisation / Open System Interconnection) Basisreferenzmodells und bietet Datenverschlüsselung, Benutzer-Authentifizierung und Punkt-zu-Punkt Sicherheit zur sicheren Datenübertragung an und kann neben IP auch noch andere Protokolle tunneln [9]. Zur Benutzer-Authentifizierung stehen beim PPP zwei verschiedene Verfahren zur Zugangskontrolle zur Verfügung, das Password Authentication Protocol (PAP) und das Challenge Handshake Protocol (CHAP). Zur Wahrung der Vertraulichkeit stehen als Verschlüsselungsalgorithmen die bereits oben erwähnte RC4-Verschlüsselung und der Data Encryption Standard (DES) zur Verfügung. Alle Datenpakete der getunnelten Verbindungen werden auf Senderseite in PPP-Pakete verpackt und dann gemultiplext über den Tunnel verschickt, auf der Empfängerseite wieder entmultiplext und aus den PPP-Paketen ausgepackt.
Ob dieses Protokoll für die übertragenen Daten eine hohe Sicherheit garantieren kann ist umstritten, da dieses Protokoll mehrere Sicherheitslücken aufweist, die ein Angreifer im WLAN nach Überwindung der WEP-Verschlüsselung ausnutzen kann. So ist es z.B. möglich, daß ein Angreifer, die Aushandlung des PPP-Protokolls zwischen den Gegenstellen über den Tunnel abzuhören und zu modifizieren. Aus diesen Gründen ist das PPTP für die Absicherung eines WLANs über ein VPN nicht zu empfehlen und statt dessen das im Folgenden beschriebene IPSec (Internet Protocol Security) einzusetzen [13].

5.1.2 IPSec (Internet Protocol Security)

Bei IPSec handelt es sich um ein Schicht 3 Protokoll, d.h. die Daten werden selbst über die IP-Schicht getunnelt, welches sowohl für IPv4 (Internet Protocol Version 4) als auch für IPv6 von der IETF standardisiert wurde. Dieses Protokoll bietet sicherheitstechnisch Benutzerauthentifizierung, Paketauthentifizierung, Datenverschlüsselung, Schlüsselmanagement und Punkt-zu-Punkt Sicherheit. Es sichert die Kommunikation über ungesicherte Netzwerke wie das Internet durch Vertraulichkeit, Authentizität und Integrität der Daten und Nutzer ab [9]. Bei der Entwicklung von IPSec wurde bewußt viel Wert auf die Flexibilität und zukünftige Erweiterung gelegt, so ist es möglich zwischen verschiedenen Verschlüsselungs- und Hash-Algorithmen auszuwählen und neue in dieses Protokoll zu integrieren. IPSec unterstützt zur Zeit gängige Verschlüsselungsalgorithmen wie DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfisch und Hash-Algorithmen zur digitalen Signatur wie MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm 1). Durch die vielfältige Algorithmenauswahl ist es im Falle möglich, falls Schwachstellen in einem Algorithmus bekannt werden, diesen sofort durch einen anderen Algorithmus innerhalb der IPSec-Architektur zu ersetzen [8, 10]. Zur Sicherung von Authentizität, Integrität und Vertraulichkeit beinhaltet IPSec zwei zusätzliche Protokolle, welche auf das Internet Protokoll aufsetzen, zum Einen das AH-Protokoll (Authentication Header) und zum Anderen das ESP-Protokoll (Encapsulating Security Payload) [10].
Das AH-Protokoll kann IP-Pakete lediglich mit einer digitalen Signatur versehen, deswegen ist es für die Sicherung eines WLANs nicht zu empfehlen, da es nur Integrität und Authentizität, aber keine Vertraulichkeit von Daten garantieren kann [11]. Das ESP-Protokoll bietet neben der digitalen Signatur auch eine Verschlüsselung an, um Integrität, Authentizität und Vertraulichkeit von Daten und Nutzer zu garantieren [12].

5.2 Verbesserungen am Standard IEEE 802.11

Nach bekanntwerden diverser Sicherheitsschwächen in der WEP-Verschlüsselung, hat es sich das IEEE zur Aufgabe gemacht, durch Ausarbeitung eines neuen Sicherheitsstandards die Sicherheit im WLAN zu verbessern. Im Moment wird das Temporary Key Integrity Protocol (TKIP) entwickelt. Nach der Entwicklung von TKIP steht als nächster Schritt die Entwicklung eines komplett neuen Sicherheitsstandards IEEE 802.11i an, wobei als Ausgangsbasis das Sicherheitssystem aus IEEE 802.1x, welches ursprünglich für drahtgebundene Ethernet-Netzwerke definiert wurde, dient. Gegenüber dem bisherigen Ansatz gibt es in dem neuen Standard eine Vielfalt von Authentifizierungsmechanismen, dabei können die Computer aushandeln, welcher Mechanismus eingesetzt werden soll. Die Authentifizierung erfolgt entweder über Benutzername und Paßwort oder aber auch über den Austausch von Zertifikaten. Ebenso kann die Authentifizierung über eine SIM-Karte (Subscriber Identification Module) erfolgen, wie sie schon im Bereich des Mobilfunks eingesetzt wird [5].

5.2.1 Temporary Key Integrity Protocol (TKIP)

TKIP stellt im Großen und Ganzen eine Erweiterung des WEP-Standards dar, es soll den WEP-Algorithmus in entscheidenden Punkten verbessern: Verlängerung des Schlüssels,

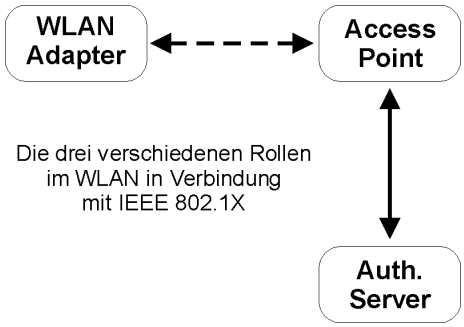
zusätzliche Sicherheitsmerkmale auf Paketebene und Neudefinierung des Algorithmus zugunsten eines regelmäßigen Schlüsselwechsels, da bei WEP ein gleichbleibender Schlüssel verwendet wird. Die Spezifizierung von TKIP ist seit Ende Januar 2002 abgeschlossen und wird zukünftiger Bestandteil des Standards IEEE 802.11i sein [5].

5.2.2 Advanced Encryption Standard (AES)

In die Entwicklung des neuen Standards IEEE 802.11i soll auch der bereits verfügbare Verschlüsselungsalgorithmus AES mit einfließen [5]. Der Verschlüsselungsalgorithmus AES soll mit Schlüssellängen von 128, 192 und 256 Bit als Nachfolger den DES Verschlüsselungsalgorithmus ablösen, welcher lediglich Schlüssellängen von 56 Bit unterstützt. Mit AES soll die Sicherheit in der Verschlüsselung um ein Vielfaches erhöht werden und so leichte Angriffe unmöglich machen [4].

5.2.3 IEEE 802.1X

Der IEEE Standard 802.1X soll eine weitere Basis sein, um WLANs in Zukunft sicherer gegen Angreifer zu machen. Dieser Standard beabsichtigt eine sichere Authentifizierung, Zugriffskontrolle und Schlüsselmanagement bereitzustellen. Die Authentifizierung soll dabei von einem zentralen Server durchgeführt werden. Dieser soll die Skalierbarkeit und Sicherheit von verteilten Access Points in einem Netzwerk erhöhen, da so die Administration eines jeden einzelnen Access Points auf ein Minimum reduziert wird.



Der WLAN-Adapter authentifiziert sich gegenüber dem Access Point, dieser führt die Authentifizierung nicht selbst durch, sondern schickt die Informationen an den Authentifizierungsserver weiter. Der Authentifizierungsserver entscheidet daraufhin, ob die Authentifizierung erfolgreich ist. Genauso wird auch mit jedem Datenpaket vom WLAN-Adapter zum Access Point verfahren, der Authentifizierungsserver muß vor der Datenverarbeitung erst die Authentizität und Integrität des Datenpakets überprüfen.
Der Einsatz des Standards IEEE 802.1X in Verbindung mit einem WLAN eröffnet erneut Sicherheitslücken. So ist es z.B. möglich, daß ein Client einer „Man-In-Middle“-Attacke ausgesetzt wird, da er sich nur gegenüber dem Access Point, der Access Point aber nicht gegenüber dem Client authentifizieren muß. Der Angreifer gibt sich gegenüber dem ahnungslosen Client als Access Point und dem echten Access Point als Client aus und übernimmt die Kommunikation zwischen beiden [15].

Fazit

Die in dem Standard IEEE 802.11 integrierten Sicherheitsmechanismen (WEP-Verschlüsselung und Verstecken der ESSID) können die Anforderungen an die Sicherheit im WLAN aufgrund mehrerer Sicherheitsmängel nicht erfüllen. Auch die von manchen Herstellern zusätzliche Sicherheitsüberprüfung der MAC-Adressen trägt nicht zur Erhöhung der Sicherheit in einem WALN bei. Aus diesem Grunde ist es sehr wichtig, die Funkverbindungen durch zusätzliche Sicherungsmaßnahmen vor unberechtigten Zugriffen durch Dritte zu schützen. Da die Entwicklung des Standards IEEE 802.11i (TKIP und AES) noch nicht vollständig abgeschlossen ist und der Standard IEEE 208.1X in Verbindung mit einem WLAN auch Sicherheitslücken aufweist, ist die Absicherung eines WLANs damit auch nicht möglich. Deshalb bleibt z.Zt. nur die Möglichkeit, die Funkverbindungen durch ein VPN zu tunneln, um die Sicherheit (Authentizität, Integrität und Vertraulichkeit) zu gewährleisten. Da allerdings das PPTP ebenfalls Sicherheitslücken aufweist, ist für die Sicherung von WLAN-Verbindungen durch einen VPN-Tunnel nur der Einsatz von IPSec zu empfehlen, da mit diesem Protokoll alle bekannten Sicherheitslücken ausgeschlossen werden.

Literaturverzeichnis

[1] *IEEE:* ANSI/IEEE Standard 802.11, 1999 Edition
[2] *Nikita Borisov, Ian Goldberg, David Wagner:* Intercepting Mobile Communications: The Insecurity of 802.11
[3] *William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan:* Your 802.11 Wireless Network has No Clothes
[4] *Reinhard Wobst:* AES unter Beschuß, c't 21/2002
[5] *LANline:* LANline - Magazin für Netze Daten und Telekommunikation, Ausgabe 11, November 2002
[6] *Rüdiger Weis:* Der RC4 Stromchiffrierer, http://www.informatik.uni-mannheim.de/~rweis/rgp/rc4/
[7] *Oliver Müller:* Einführung in die Kryptologie – Der RC4 Algorithmus, http://www.linux-magazin.de/Artikel/ausgabe/1997/11/Krypto/krypto5.html
[8] *Lessing & Partner:* Virtual Private Networks auf IPSec-Basis, http://www.lessing.de
[9] *Gerhard Glaser:* VPN (Virtual Private Networks) mit IPSec
[10] *IETF:* RFC 2401, Security Architecture for the Internet Protocol
[11] *IETF:* RFC 2402, IP Authentication Header
[12] *IETF:* RFC 2406, IP Encapsulating Security Payload (ESP)
[13] *IETF:* RFC 2637, Point-to-Point Tunneling Protocol (PPTP)
[14] *Christopher Klaus:* Wireless Security FAQ, http://www.iss.net/wireless/WLAN_FAQ.php
[15] *William A. Arbaugh, Arunesh Mishra:* An Initial Security Analysis of the IEEE 802.1X Standard