WAR DRIVING UND SICHERHEIT IN KABELLOSEN NETZEN

von

Sascha Lange

Seminar Mobile Computing
FB Mathematik/Informatik
Universität Osnabrück
im SS 2003

Ausarbeitung

Osnabrück, den 30.7.2003

ABSTRACT

In „Wireless LANs“ nach IEEE 802.3 ist es ein leichtes, Zugang zum Übertragungsmedium – Luft – zu bekommen. Ohne aufwendige Verkabelung ist es möglich, schnell Zugang zu wechselnden Netzen zu erlangen. Dies kann im Falle sich im Firmennetzwerk an- und abmeldender Mitarbeiter erwünscht sein, bietet aber auch Möglichkeiten für potentielle Angreifer, deren Zugang zum Übetragungsmedium nicht verhindert und nur schlecht überwacht werden kann.

Das War Driving oder auch Net Stumbling befasst sich nun genau mit der Aufspürung von Funknetzwerken, die für eigene Zwecke (egal ob mit oder ohne Zustimmung der Betreiber) verwendet werden können. Gefundene offene Netze (so genannte Hot Spots) werden mittels spezieller Kreidezeichen für andere kenntlich gemacht.

Nicht nur offene Netze können so zweckentfremdet werden. Es gibt auch einige Mängel in den Sicherheitsvorkehrungen des IEEE 802.11 Standards, die selbst die Nutzung „geschützter“ Funknetze möglich machen und fast gleichzeitig von zwei verschiedenen Gruppen im Jahr 2001 entdeckt und veröffentlicht wurden.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AP	Access Point
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
GPS	Global Positioning System
IEEE	Institute of Electrical an Electronics Engineers
IP	Internet Protocol
IV	Initialization Vector
KS	Key Stream
PDA	Personal Digital Assistant
SSID	Service Set Identifier
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WLAN	Wireless Local Area Network

1 Einleitung

Funknetze wie Wireless LAN (WLAN) nach dem weit verbreiteten IEEE 802.11 Standard ermöglichen den Aufbau von Computernetzwerken über das Übertragungsmedium „Luft“. Der Zugang ist damit nicht mehr nur stationär über kabelgebundene Geräte möglich, sondern auch mittels mobiler Klienten, die sich in dem Empfangsbereich eines Zugangspunktes („Access Point“, AP) befinden. Einerseits zeichnen sich Funknetze damit durch eine größere Flexibilität und auch oftmals durch eine reale Kostenersparnis (keine Verkabelung von Gebäuden nötig) aus, geben dabei aber auch die alleinige Kontrolle über das Übertragungsmedium preis. Nicht nur die Klienten, denen vom Betreiber ein physikalischer Zugang zum Netzwerk in Form eines Anschlusses an das Übertragungsmedium gewährt wurde, sondern alle Klienten, die in den Empfangsbereich eines AP gelangen, können Daten in das Netz einspeisen und mithören. Das Übertragungsmedium kann nunmehr sogar von mehreren, unabhängigen Netzwerken gleichzeitig verwendet werden.

1.1 Überblick

Im folgenden zweiten Teil wird eine „Community“ beleuchtet, die sich diesen Kontrollverlust über das Übertragungsmedium und die breite Verfügbarkeit von Netzzugangspunkten zunutze gemacht hat.

Während sich diese Gemeinde in der Regel auf das Aufspüren und die Nutzung von „offenen“ Netzen beschränkt, werden im dritten Teil ernste Mängel in den Sicherheitsmechanismen des relevanten Industriestandard beschrieben, die für alle Betreiber von Funknetzwerken von Bedeutung sind. Selbst die Verwendung aller vorgesehenen Sicherheits- und Zugangskontrollmechanismen bietet in „geschlossenen“ Netzwerken keinen wirksamen Schutz vor üblichen Angriffen.

Im vierten und letzten Teil erfolgt dann eine kurze Zusammenfassung.

Wenn im Folgenden von „Funknetzen“ oder „WLAN“ die Rede ist, sind immer die in dieser Arbeit ausschließlich betrachteten Funknetze nach IEEE 802.11b, die bereits ausführlich von Ba Kien Tran (2003) im Rahmen dieses Seminars behandelt wurden, gemeint. Sollten andere Netze gemeint sein, wird darauf ausdrücklich hingewiesen.

2 Net Stumbling

Im Zuge der kommerziellen Verbreitung von WLAN fähigen Endgeräten wird gerade in Industrie- und Ballungszentren eine beachtliche Abdeckung mit Funknetzen erreicht. Zumeist sind diese Netze auch direkt an das Internet angeschlossen. Damit böte sich unter Mitarbeit der Netzbetreiber die Möglichkeit, einen schnellen, unabhängigen, dezentralen und kostengünstigen Internetzugang für Nutzer mobiler Endgeräte bereitzustellen, der in direkter Konkurrenz zu anderen Zugangsarten wie z.B. dem Zugang über das Mobiltelefon stünde.

Diese Idealvorstellung, aber auch der persönliche Vorteil und die technische Neugier haben wohl den Antrieb zu der Entstehung einer breiten Gemeinde von Funknetz-Freaks, die sich gerne selber als „Stumbler“ oder „War Driver“ bezeichnen, geliefert.

Der weit verbreitete Begriff „War Driving“ ist eine Abwandlung des Begriffs „War Dialing“ und hat seinen Ursprung in dem Kultfilm der Szene „War Games“ von 1983. In dem etwas abstrusen Film wählt Matthew Broderick mittels eines Modems wahllos Telefonnummer an, um schlecht geschützte Einwahlstellen in Firmennetzwerke zu finden. Dies gelingt ihm letztendlich auch; nur entpuppt sich das auf der Gegenseite vermutete Spiel als ein Computer zur Steuerung strategischer Atomwaffen. Der dritte Weltkrieg kann aber glücklicherweise noch kurz vor Ende des Films verhindert werden.

Prinzipiell verfolgen die War Driver die gleiche Idee: Sie begeben sich mit einem mobilen Empfangsgerät (ein Laptop oder PDA) wahllos auf die Suche nach aktiven Funknetzwerken. Das Augenmerk liegt auch hier auf offenen (oder extrem schlecht geschützten) AP, die für den

Zugang zum Internet oder andere Zwecke verwendet werden können. Im Gegensatz zu Matthew Broderick können die War Driver diese Suche nicht von zu Hause aus erledigen, sondern müssen sich dazu vor Ort, in den Empfangsbereich der Netze begeben. Dies kann natürlich zu Fuß (War Walking) oder per Auto (daher der Begriff War Driving) geschehen.

2.1 „offene" Netze

Nicht immer verfolgen die War Driver dabei kriminelle Ziele: Einige Funknetzbetreiber erlauben fremden Personen z.B. aus ideellen Gründen die Nutzung der eigenen, nicht ausgeschöpften Kapazitäten. Und auch immer mehr Gaststätten möchten Ihren Kunden einen kostenlosen Zugang zum Internet anbieten. Hinzu kommt noch, dass es fraglich ist, ob die Verwendung eines ungeschützten Funknetzes überhaupt strafbar ist, selbst wenn der Eigentümer nicht mit einer Nutzung einverstanden wäre. Sind keinerlei Vorkehrungen zur Zugangsbeschränkung unternommen worden, kann bezweifelt werden, dass sich der „Eindringling" der Zustimmung des Betreibers nicht gewiss sein konnte. Aber natürlich gibt es auch kriminelle Interessen, in Funknetze einzudringen. So soll zum Beispiel die Wirtschaftsspionage ein so lukratives Geschäft sein, dass auch größere Anstrengungen zur Umgehung der Sicherheitsmaßnahmen wirtschaftlich attraktiv werden.

Generell ist also zwischen der Aufspürung und Nutzbarmachung „offener" („legal") und „geschlossener" Netze (illegal) zu unterscheiden. Ein offenes Netz ist hierbei ein Access Point mit Netzanbindung, bei dem keinerlei spezielle Maßnahmen zur Zugangsbeschränkung oder Zugangskontrolle und keinerlei Anstrengungen zur Verschlüsselung des Datenverkehrs unternommen wurden. Ein solches Netz kann, wie schon oben argumentiert, als öffentlich bezeichnet werden.

Die Vielzahl verfügbarer offener Netze in Ballungszentren begründet sich zum einen in der absichtlichen, ideellen Bereitstellung der eigenen Kapazitäten, zum anderen aber auch in Defiziten bei den Einstellungen der Geräte. So sehen die Standardeinstellungen verbreiteter AP wie der

AP von Linksys keinerlei Zugangsbeschränkungen vor. Da die Standardeinstellungen weithin bekannt sind, sind solche Netze zudem extrem leicht aufzuspüren. Viele Betreiber wissen oftmals schlichtweg gar nicht um die Gefahren, denen sie durch den Anschluss eines AP an ihr bestehendes Netz ausgesetzt sind.

An dieser Stelle sei stellvertretend für die Vielzahl von Non-Profit Organisationen, die Netze flächendeckend bereitstellen, das Personal Telco Project genannt, das sich zum Ziel gesteckt hat, mit Hilfe von Spenden und Privatpersonen einen kostenlosen Internetzugang für die gesamte Innenstadt von Portland bereitzustellen (vgl. Personal Telco Project 2003).

2.2 Funknetze Kennzeichnen: „War Chalking“

Um einmal gefundene, nützliche Funknetze kenntlich zu machen, so dass sie für nachfolgende Benutzer mobiler Endgeräte leichter aufzuspüren sind, hat die Gemeinde eigens eine Serie von Zeichen entwickelt,

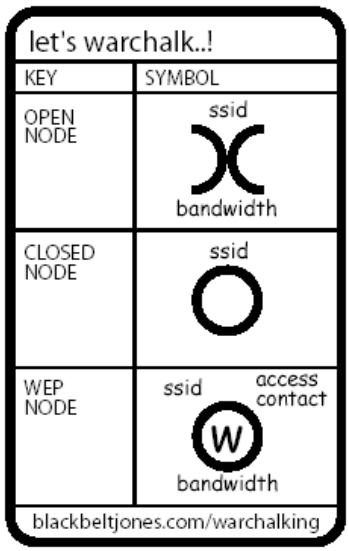


Abbildung 1: Offizielle War Chalking Symbole. (Abbildung von Warchalking.Org 2002)

die mit Kreide oder Sprühfarbe gut sichtbar im Empfangsbereich der AP des Funknetzes angebracht werden. Die Zeichen können Informationen über Zugangskontrolle, Netzwerkname, Bandbreite und Übertragungskanal des AP enthalten. Um der wachsenden Zahl der Schutzmechanismen Rechnung zu tragen, gab es zwischenzeitlich eine Vielzahl von entsprechenden Symbolen in der Diskussion. Letztendlich ist man aber zu dem Schluss gekommen, dass für andere nur nutzbare Netze von Interesse sind, und sich die Kenntlichmachung des genauen Sicherheitsmechanismus, der einen Zugang unmöglich macht, nicht lohnt. Es sollen also im Wesentlichen offene oder schlecht geschützte Knoten mit den nötigen Informationen „gechalkt" werden. Dafür haben sich drei „offizielle" Symbole durchgesetzt (vgl. Abbildung 1).

Da die Tools zum Aufspüren der Netze inzwischen so ausgereift und einfach zu bedienen sind, dass sie eigentlich jeder interessierte Endbenutzer ohne Probleme einsetzen kann, stellt sich die Frage, ob die visuelle Kennzeichnung überhaupt noch Sinn macht. Bis man ein solches Zeichen entdeckt hat, befindet man sich vermutlich längst im Empfangsbereich des AP, der also bereits mit einem entsprechenden Tool aufgespürt worden sein könnte. Das War Chalking scheint daher inzwischen zum Selbstzweck der Gemeinde geworden zu sein, ähnlich wie das von „Sprayern" und „Skatern" bekannte „Tagging" seines Namenskürzels.

Abbildung 2: Zwei Symbole, die Hauswände in einer italienischen Großstadt zieren. Links sind gut die Bandbreit (11 Mbps), der Netzwerkname (ZANNI.ORG) und der Netzwerktyp (B für 802.11b) zu erkennen.

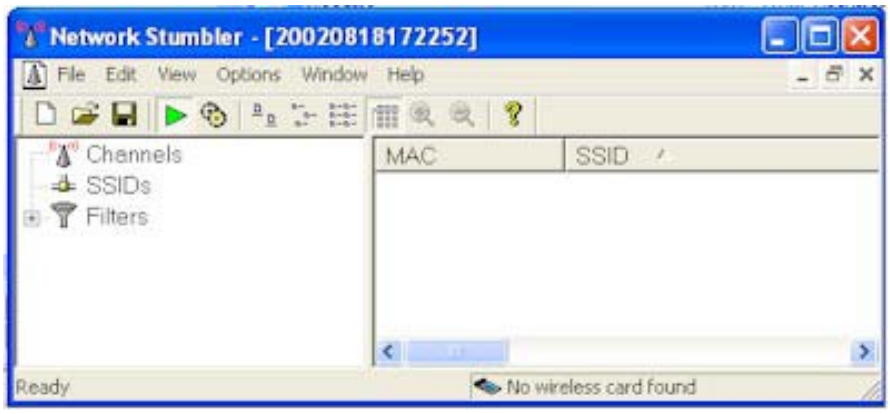
In Abbildung 2 sind einige Symbole aus der „freien Wildbahn“ zu sehen.

2.3 Werkzeuge zum Aufspüren von Funknetzen

War das Aufspüren von Funknetzen anfangs nur Eingeweihten möglich, gibt es inzwischen eine Vielzahl von frei verfügbaren Tools, die die Suche nach Hot Spots zum Kinderspiel werden lassen. Der Anwender kann dabei je nach seinem Betriebssystem (DOS, Linux, Windows 98/2000/XP und sogar Windows CE werden unterstützt) und dem auf der WLAN Empfangseinheit verwendeten Chipsatz aus einer größeren oder kleineren Auswahl von Programmen wählen.

Im Folgenden werden dreieinhalb Tools kurz exemplarisch vorgestellt.

2.3.1 NetStumbler für Windows 98/2000/XP



Der NetStumbler ist ein einfach zu bedienendes und weit verbreitetes Tool. Es sucht ununterbrochen nach AP im Empfangsbereich. Dazu werden so genannte Beacons ausgesendet und detektiert. Sendet ein Access Point diese Beacons nicht (kann bei einigen Herstellen entgegen dem Standard abgestellt werden), bzw. reagiert nicht auf diese Signale von ihm unbekannter Karten, kann er vom NetStumbler auch nicht aufgespürt werden.

Detektierte Access Points werden je nach Zugangsbeschränkungen und Verschlüsselungsmaßnahmen (WEP Encryption, WEP Authentication, offen) eingeordnet. Der Netzwerkname wird, soweit übermittelt, angezeigt.

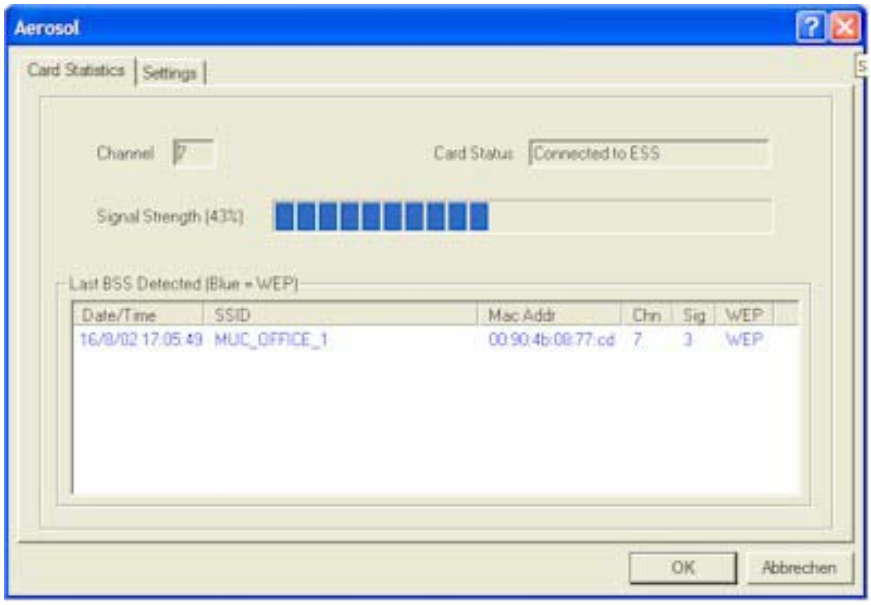
In einer weiteren Ansicht kann die Empfangsstärke in kurzen Zeitabständen gemessen und grafisch dargestellt werden. Dies hilft bei der Ortung des Standortes der Antenne.

Interessant ist auch die Anbindungsmöglichkeit eines an die serielle Schnittstelle angeschlossenen GPS Empfängers. Mit seiner Hilfe kann der NetStumbler ein automatisches Protokoll erstellen, in dem alle georteten Netze mit exakten Weltkoordinaten zur späteren Auswertung oder Übermittlung an ein Netzverzeichnis aufgeführt werden.

2.3.2 *MiniStumbler für Windows CE*

Der MiniStumbler ist die Version des NetStumblers für Windows CE. Er bietet die gleichen Such- und Protokollfunktionen und ermöglicht ebenfalls die Verwendung eines GPS Empfängers zur Erstellung eines Protokolls. In Hinblick auf Komfort und Darstellung müssen aber ein paar gerätebedingte Einschränkungen hingenommen werden.

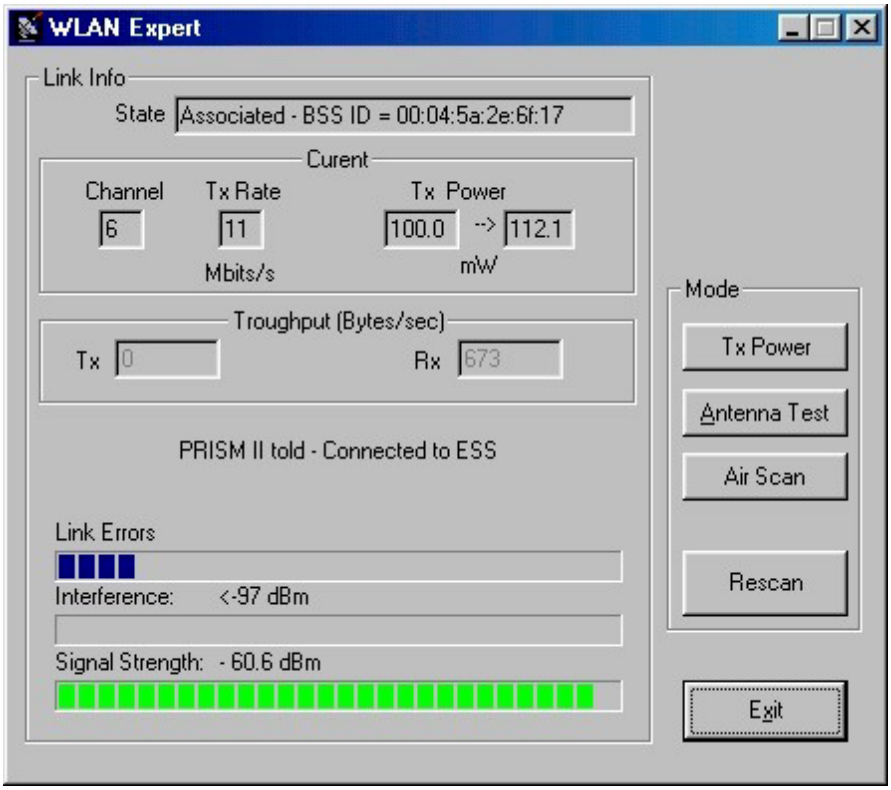
2.3.3 *Aerosol*



Aerosol kommt noch minimalistischer daher: Es gibt lediglich zwei Dialoge: Einen, um ein paar Einstellungen vorzunehmen und einen, in dem alle Informationen angezeigt werden. Die Informationen beinhalten eine Balkenanzeige der Empfangsstärke und eine Liste der zuletzt gesehenen Netze mit zum NetStumbler vergleichbaren Informationen.

Interessant wird Aerosol durch die für das nächste Release geplante Erweiterung um eine Funktion zur WEP Decryption. Sollte sich diese Funktion nahtlos in das einfache, intuitive Bedienungskonzept einfügen, sind WEP geschützte Netze wohl in Zukunft nicht einmal mehr vor Einblicken unversierter „normaler" Endbenutzer sicher.

2.3.4 WLAN Expert



Der WLAN Expert ist eigentlich nicht als Tool zum Stumbling gedacht. Er sollte vielmehr als Testwerkzeug für Administratoren von Funknetzen dienen. So zeigt er die üblichen Daten des verbundenen AP an, bietet aber auch Daten zu der Sende- und Empfangsstärke in mW und verfügt über einen ausgefeilten Antennentest, mit der die Funktion bzw. die Güte einer verwendeten Antenne gemessen werden kann. Damit

Abbildung 3: Selbstgebastelte Richtantenne aus einer Chipsdose. Links: Die ausgerichtete und an eine PCMCIA WLAN Karte angeschlossene Antenne. Rechts: Einblick in die Röhre, in die ein „Empfangsstift“ ragt.

eignet er sich auch hervorragend zur Bewertung und Optimierung selbstgebauter Antennen und ist somit auch für War Driver ein nützliches Werkzeug.

2.4 Antennen

Neben dem Endgerät und der Software spielen die verwendeten Antennen bei der Suche nach Funknetzen eine entscheidende Rolle. Haben die Netze nach der Spezifikation gerade in bebauten Gebieten nur eine sehr kleine effektive Reichweite (praktisch immer unter 100m), kann die Reichweite der eigenen Einheit durch spezielle Antennen beträchtlich gesteigert und die Suche damit entscheidend vereinfacht werden. Das Angebot verfügbarer Antennen für den 2.4 GHz Bereich reicht von bequemen, aber in ihrer Reichweite beschränkten omnidirektionalen Antennen bis hin zu Richtantennen, mit denen Verbindungen oftmals noch über mehrere Kilometer aufgebaut werden können, sofern sie genau auf die Gegenstelle ausgerichtet werden. Einen guten Überblick über das bestehende Angebot erhält man zum Beispiel auf den Seiten des Anbieters FAB Corp (2003).

Ein richtiger Enthusiast greift aber nicht auf diese kommerziellen Angebote zurück, sondern verlässt sich nur auf seine Antenne Marke Ei-

genbau. Wie man z.B. mit geringem finanziellen Aufwand eine Antenne aus einer Verpackung von bekannten Kartoffelchips bastelt, wird im Internet ausführlich beschrieben (vgl. Flickenger 2001, siehe Abbildung 3).

Ein weiterer Schritt ist es dann, die Antennen fest in Fahrzeugen zu montieren. Es hat sich eine der Bassröhrenfraktion ähnliche Fangemeinde solcher Modifikationen gebildet, die selbst nicht davor zurückschreckt, das Display ihres Navigationssystems als Bildschirm für ihre WLAN Endgeräte zu zweckentfremden (leider wurde die entsprechende Seite http://home.attbi.com/~digitalmatrix/wardriving/ inzwischen gelöscht).

2.5 Listen von Hot Spots

Inzwischen gibt es mehrere Datenbanken, in denen die Standorte und Daten von AP verzeichnet sind. Zum Teil wurden sie von den Betreibern selber, aber auch von War Drivern gefüllt. Ein weltweites Verzeichnis ist z.B. die NodeDB (2003). Leider sind dort kaum europäische Funknetze verzeichnet. Highspeed-Hotspots.de (2003) und Mobileaccess.de (2003) bieten gerade über Deutschland mehr Informationen.

3 Sicherheitsmaßnahmen in Funknetzen

Da das Übertragungsmedium öffentlich und einfach zugänglich ist, besteht ein verständlicher Bedarf nach zusätzlichem Schutz gegenüber kabelgebundenen Netzen. Der Standard sieht daher einige Maßnahmen noch auf Ebene des Link Layers vor, die zudem von einigen Herstellern noch um proprietäre Schutzmaßnahmen erweitert werden. Die Maßnahmen lassen sich in drei Kategorien einordnen:

1. Zugangskontrolle
Unautorisierte Klienten sollen an der Anmeldung und am Einspeisen von Daten gehindert werden.

2. Schutz vor Lauschern
Das Abhören der übertragenen Daten soll verhindert, bzw. die enthaltene Information verschleiert werden.

3. Schutz vor Veränderungen
Legitim eingespeiste Daten müssen vor Veränderungen durch unautorisierte Klienten geschützt werden, um deren Integrität sicherstellen zu können.

Im Folgenden werden die verschiedenen Sicherheitsmaßnahmen kurz dargestellt und im Falle der WEP (Wired Equivalent Privacy) Verschlüsselung ausführlicher auf Ihre Wirksamkeit hin untersucht. Leider wird sich zeigen, dass die Maßnahmen im Einzelnen teilweise ungenügend sind und in ihrer Gesamtheit dem Ziel, sichere Datenübertragung zu gewährleisten, nicht gerecht werden.

3.1 Maßnahmen zur Zugangskontrolle

Der IEEE 802.11b Standard schreibt keine Zugangskontrolle vor. Es gibt lediglich eine optionale Zugangskontrolle unter Verwendung des WEP Schlüssels. Daher bieten einige Hersteller ihren Kunden eigene, proprietäre Maßnahmen zur Zugangskontrolle an.

3.1.1 „geheimer" Service Set Identifer (SSID)

Jedes Netzwerk besitzt einen eigenen Namen, den Service Set Identifer (SSID). Ein Klient, der sich an dem Netz anmelden will, muss diesen Namen kennen. Allerdings wird dieser Name in einem so genannten Beacon-Signal von den meisten AP regelmäßig mit kurzen Zeitabständen versendet. Nachdem einige Hersteller Karten und Treiber auf den Markt gebracht haben, bei denen man einstellen kann, dass sie sich bei „irgendeinem" Netz anmelden sollen, ohne dass der Benutzer den Namen zuvor eingegeben hätte, war diese ehedem dünne Sicherheitsschicht unwirksam. Einige Hersteller von AP bieten daher inzwischen die Möglichkeit an, das Aussenden des SSID abzustellen. Aber selbst dann bietet der SSID als Passwort nur einen geringen Schutz: Jeder Klient muss das (gleiche) Passwort kennen, um sich an das Netz anmel-

den zu können. Eine Kontrolle über die Weitergabe des Passwortes ist damit nur schwer möglich. Zudem belassen es viele Betreiber auch einfach bei dem bei der Auslieferung eingestellten Namen. In der Statistik der am häufigsten verwendeten Netzwerknamen, nehmen die Standardeinstellungen tatsächlich die vorderen Plätze ein.

3.1.2 Positivliste autorisierter MAC Adressen

Eine weitere Schutzmaßnahme, die von verschiedenen AP angeboten wird, ist eine Positivliste erlaubter MAC Adressen. Dabei muss der Administrator im AP alle MAC Adressen der WLAN Karten eintragen, die sich bei ihm anmelden dürfen. Pakete von Karten mit anderen MAC Adressen werden einfach ignoriert. Da die MAC Adressen weltweit eindeutig vergeben werden, sollte dieser Mechanismus eine sichere Zugangskontrolle bieten, wäre es nicht möglich, treiberseitig eine andere, beliebige MAC Adresse vorzuspiegeln (MAC address spoofing). Hierfür gibt es für Windows modifizierte Treiber, während es unter Linux sogar ein Standardfeature ist.

Außerdem gestaltet sich die Verwaltung dieser Listen in großen Netzwerken aufwendig. Da es keine sichere Übertragung und keine passenden Werkzeuge gibt, müssen diese Daten in jeden AP einzeln eingegeben und auf dem aktuellen Stand gehalten werden. Zudem reicht es bei einem Angriff aus, eine einzige gültige MAC Adresse aus den versendeten Paketen zu erlauschen, schon ist das ganze System wertlos.

3.1.3 Statische IP Adressen anstelle dynamischer Vergabe

Ein ähnlicher Ansatz setzt eine Schicht höher an. Anstatt sich anmeldenden Klienten automatisch eine IP Adresse zuzuweisen, kann man bei einigen Geräten eine „geheime“ Liste statischer IP einstellen. Ein Klient muss dann auf eine dieser IP eingestellt sein, um Pakete senden zu dürfen. Andernfalls werden seine Daten ignoriert.

Neben dem geringeren Komfort gegenüber einer Adressvergabe z.B. mittels DHCP, hat das Verfahren die gleichen Vor- und Nachteile und Probleme wie die MAC-Adresslisten.

3.1.4 Keine Sicherheit bei der Zugangskontrolle

All diesen zum Teil herstellerspezifischen Maßnahmen ist eines gemein: Sie erschweren den unerlaubten Zugang zum Funknetzwerk, verhindern ihn aber nicht. Während unbedarfte Normalbenutzer durch diese Maßnahmen durchaus wirksam vom Missbrauch abgehalten werden können, bieten die Maßnahmen keine unüberwindbare Hürde und können von motivierten und versierten Angreifern mit Leichtigkeit genommen werden. Von einer sicheren Zugangskontrolle bei einem durch diese Maßnahmen geschützten Netz zu sprechen, wäre also fahrlässig.

3.2 WEP

Um den Benutzern von Funknetzen dennoch eine mit kabelgebundenen Netzen vergleichbare Privatsphäre zu bieten, beinhaltet der IEEE 802.11 Standard ein optionales Sicherheitsprotokoll auf Ebene des Link Layers: Die Wired Equivalent Privacy, kurz WEP.

WEP soll durch Verschlüsselung die Geheimhaltung übertragener Daten gewährleisten. Neben diesem Primärziel ist aber auch die Zugangskontrolle, bzw. die Authentifizierung der Klienten genau wie die Datenintegrität ein Ziel.

3.2.1 Datenintegrität und Datensicherheit

Das WEP Protokoll verwendet einen „Stream cipher“ zur Verschlüsselung der zu übertragenden Daten. Ein Stream cipher ist ein Algorithmus, der aus einem endlichen Schlüssel (engl: key) einen unendlichen Strom von Pseudozufallszahlen erzeugt. Der gleiche Schlüssel erzeugt dabei bei jedem Durchlauf exakt den gleichen „Schlüsselstrom“ KS (engl: key stream). Die zu sendenden Daten werden dann mit dem Schlüsselstrom bitweise per XOR verknüpft. Bei einem idealen Schlüsselstrom sind die so verschlüsselten Daten nicht mehr von Zufallsrauschen zu unterscheiden. Das WEP Protokoll verwendet den RC4 Algorithmus zur Erzeugung der KS.

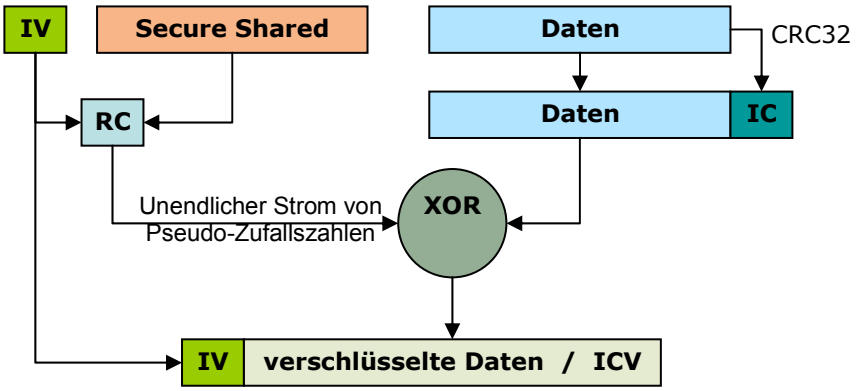


Abbildung 4: Verschlüsselungen von Daten im WEP Protokoll. Die mit einer CRC32 Checksumme versehenen Daten werden mit einem vom RC4 Algorithmus erzeugten Strom von Pseudozufallszahlen logisch XOR verknüpft. Der RC4 Algorithmus wird dabei mit einem Initialisierungsvektor IV und einem geheimen Schlüssel k gestartet. (Abbildung von Ba Kien Tran 2003)

Das WEP Protokoll sieht in der Originalfassung einen geheimen Schlüssel k von 40 Bit Länge vor, der beiden Kommunikationspartnern bekannt sein muss. Zusätzlich enthält jedes gesendete Paket im Klartext einen beliebigen Initialisierungsvektor IV (engl.: initialization vector) von 24 Bit. Die Auswahl des Initialisierungsvektors ist nicht näher spezifiziert und kann von jedem Endgerät nach einer beliebigen Strategie vorgenommen werden (auch die Verwendung des immer gleichen IV ist damit erlaubt).

Auf Seiten des Empfängers wird an die eigentliche Nachricht M nun zuerst eine Checksumme, die helfen soll, Übertragungsfehler festzustellen, angehängt. Hierzu wird das weithin bekannte CRC32 Verfahren verwendet. Der zu übertragende Klartext P setzt sich also aus der Nachricht M und deren CRC32 Checksumme c(M) zusammen:

$$P = \langle M, c(M) \rangle$$

Dieser Klartext wird dann, wie in Abbildung 4 dargestellt, mit dem vom Streamcipher erzeugten KS XOR verknüpft. Der RC4 Algorithmus wird dabei mit dem IV und dem geheimen Schlüssel k initialisiert. Praktisch wird der IV einfach vor den Schlüssel k gehängt, so dass der RC4 Algorithmus mit einer 64 Bit langen Sequenz initialisiert wird.

$$C = P \oplus RC4(\langle IV, k \rangle)$$

Der so erhaltene Ciphertext wird nun zusammen mit dem unverschlüsselten IV am Paketanfang übertragen. Der Empfänger kann nun mit dem übertragenen IV und dem ihm ebenfalls bekannten k das Paket entschlüsseln, indem er es mit dem vom RC4 Algorithmus erzeugten KS wieder bitweise mittels XOR verknüpft. Die XOR Operation hat ja die Eigenschaft, dass

$$X = X \oplus Y \oplus Y$$

gilt.

Dem Initialisierungsvektor kommt bei diesem Verfahren eine besondere Bedeutung zu. Eine einzelne Nachricht, die mit einem Streamcipher verschlüsselt wurde sollte nicht zu entschlüsseln sein. Kommt jemand aber in den Besitz mehrerer, mit dem gleichen KS verschlüsselter Nachrichten, so ergeben sich mehrere Probleme. Gelingt es diesem Empfänger eine einzige Nachricht zu entschlüsseln oder zu erraten, erhält er wegen der Eigenschaften von XOR den verwendeten KS. Damit könnte er natürlich alle anderen Nachrichten entschlüsseln, die mit diesem KS verschlüsselt wurden, ohne den geheimen Schlüssel k kennen zu müssen. Außerdem bieten sich statistische Angriffsmöglichkeiten. Sind mehrere mit dem gleichen KS verschlüsselte Ciphertexte bekannt, kann man über statistische Buchstaben- oder Worthäufigkeiten Rückschlüsse auf Teile des KS ziehen (vgl. Borisov, Goldberg und Wagner 2001). Je mehr solcher Ciphertexte abgehört werden, desto wahrscheinlicher wird der Erfolg einer solchen Attacke.

Aus diesem Grund soll mittels des wechselnden IV verhindert werden, dass Pakete mit dem gleichen KS verschlüsselt werden.

Da generell Schlüsseln von 40 Bit Länge als nicht sicher gegenüber Brute-Force Angriffen gelten, hat sich inzwischen anstelle des 64 Bit Schlüssels (24 Bit IV + 40 Bit k = 64 Bit) ein 128 Bit Schlüssel durchgesetzt. Die Ursprüngliche 64 Bit Definition war in den Ausfuhrbestimmungen der USA bezüglich kryptographischer Produkte begründet.

Durch die Berechnung, Verschlüsselung und Sendung der CRC32 Checksumme des Paketes soll zudem die Integrität der übertragenen Daten sichergestellt werden. Sollte ein Bit geändert worden sein, so würde die Checksumme bei der Kontrolle auf Empfängerseite nicht mehr stimmen und das Paket würde verworfen werden.

3.2.2 Zugangskontrolle mittels WEP

Während das WEP Protokoll hauptsächlich zum Schutz der übertragenen Informationen geschaffen wurde, sieht der Standard auch ein optionales, auf dem geheimen, geteilten Schlüssel k basierendes Verfahren vor.

Einem Klienten wird dabei eine unverschlüsselte Nachricht M (die so genannte „Challenge“) zugesendet, die der Klient zum Beweis seiner Zugriffsberechtigung zu verschlüsseln und zurückzusenden hat. Der AP entschlüsselt die Antwort des Klienten dann und kontrolliert, ob die erhaltene Nachricht mit der Challenge übereinstimmt. Ist dies der Fall, ist sichergestellt, dass der Klient Kenntnis vom geheimen Schlüssel k hat und sich damit am AP anmelden darf.

3.3 Angriffe auf WEP

Leider hat sich das WEP Protokoll als völlig unsicher erwiesen. Es ist gleich von mehreren Seiten aus angreifbar. Tatsächlich ist fast jeder Punkt der Definition des Protokolls fehlerhaft, bzw. greift zu kurz. Die Entwicklung dieses Protokolls bei der IEEE wird daher von der kryptographischen Gemeinde – teilweise mit hämischem Spott – als Nega-

tivbeispiel gegen das „Design by Comittee“ zu Felde geführt und kann wohl zu Recht als Fiasko bezeichnet werden. Die Kritik richtet sich gegen den Ausschluss von Kryptographieexperten beim Protokolldesign (dort waren hauptsächlich Vertreter der diversen Hersteller beteiligt) und die Verwendung von schlecht untersuchten Verfahren anstelle von erwiesenermaßen sicheren und verbreiteten Standardverfahren. Das WEP Protokoll wird gerne als typisches Ergebnis, das herauskommt, wenn Laien sich mit Kryptographie beschäftigen, bezeichnet.

Generell können die bisher bekannten Angriffe auf das WEP Protokoll in zwei Klassen eingeordnet werden. Die eine Klasse von Angriffen versucht den geheimen Schlüssel selber anzugreifen bzw. aufzudecken, während die andere Klasse von Angriffen den vom Streamcipher erzeugten Keystream angreift und ohne Rückschlüsse auf den geheimen Schlüssel auskommt.

3.3.1 „Direkte“ Angriffe auf den Streamcipher

Der RC4 Algorithmus wurde 1987 von Ron Rivest entwickelt aber nicht veröffentlicht und patentrechtlich geschützt. 1994 wurde er allerdings decompiliert und auf einer Mailingliste veröffentlicht. Wegen der anfänglichen Geheimhaltung und seiner eher untergeordneten Rolle war er bis zu seinem Einsatz im WEP Protokoll eher schlecht auf seine kryptographischen Eigenschaften untersucht.

Es ist daher nicht verwunderlich, dass seine Schwachstellen erst im Jahre 2001 von Fluhrer, Mantin und Shamir (2001) entdeckt und veröffentlicht wurden. Die entdeckten Schwachstellen im RC4 Algorithmus ermöglichen eine Aufdeckung des geheimen Schlüssels. Fluhrer, Mantin und Shamir beschrieben außerdem einen möglichen Angriff auf WEP verschlüsselte Daten, der von Stubblefield, Ioannideis und Rubin (2001) noch im selben Jahr in der Praxis vorgeführt wurde.

Ohne an dieser Stelle auf die Details einzugehen, gründet sich die Attacke auf die Existenz von einigen „schwachen Schlüsseln“. So gibt es eine relativ große Klasse von Schlüssel, bei denen eine hohe Anzahl von

Bits im Anfang des Keystreams von nur wenigen Bits des geheimen Schlüssels abhängen. Diese schwachen Schlüssel werden durch die sich ändernden IV irgendwann verwendet. Sind erstmal einige Bits dieser schwachen Schlüssel anhand der Keystreamanfänge erschlossen, werden auch Rückschlüsse auf die restlichen Bits des geheimen Teils des verwendeten Schlüssels leichter. So lässt sich in relativ kurzer Zeit auch der geheime Teil des Schlüssels aufdecken.

Der von Stubblefield, Ioannidis und Rubin durchgeführte und zum Beispiel im Tool aeroSnort implementierte Angriff benötigt dazu ungefähr 5-10 Millionen abgehörte Pakete und berechnet anschließend quasi per Knopfdruck in weniger als einer Sekunde den geheimen Schlüssel.

Inzwischen ist dieser Angriff die Attacke „der Wahl", da sie mit relativ wenigen Paketen auskommt und völlig passiv ist. Der Fehler, einen schlecht untersuchten Algorithmus verwendet zu haben, ist aber in Hinblick auf die anderen Angriffe ein noch vergleichsweise kleiner Fehler, den sich das Designkomitee vorwerfen lassen muss.

3.3.2 „Indirekte" Angriffe auf den Keystream

Abgesehen von der grundsätzlichen Schwäche des RC4 Algorithmus, für den die IEEE keine Verantwortung trägt, wurden einige tragische Designfehler gemacht, wegen denen das WEP Protokoll selbst unter Verwendung eines sicheren Ciphers angreifbar wäre. Borisov, Goldberg und Wagner (2001) haben diese Schwächen fast zur gleichen Zeit, zu der Fluhrer, Mantin und Shamir die Unsicherheit von RC4 belegt haben, bekannt gemacht.

3.3.2.1 Bildung eines Wörterbuches

Das Hauptproblem des WEP Protokolls ist, dass es keinerlei Regeln für die Wiederverwendung von IV gibt und diese generell zu kurz sind. Bei nur 24 Bits Länge gibt es nur 2^{24} verschiedene IV. Das sind ca. 16 Millionen. Im ersten Moment hört sich das nach viel an. Ein AP, der mit einer durchschnittlichen Datendurchsatzrate von 5Mbps und einer Paketlänge von 1500 Bytes (bei vielen Netzen die Standardeinstellung)

sendet, sind in weniger als 12 Stunden alle IV verbraucht und werden sich spätestens dann zwangsläufig wiederholen.

Da keinerlei verbindliche Regeln für das „Scheduling“ der Schlüssel existieren, werden sie sich in der Praxis schon sehr viel früher wiederholen. Die meisten Geräte verwenden die IV nämlich inkrementell und fangen nach einem Neustart häufig bei Null an. Wurden also zwei Geräte zu einem ähnlichen Zeitpunkt neu gestartet[1] oder kann der Angreifer sogar einen Neustart herbeiführen, verringert sich die nötige Wartezeit beträchtlich. Aber selbst ohne diese Möglichkeit ist ein passiver Angriff durchaus praktikabel.

Mit Hilfe der Kollisionen kann der Keystream aus den Ciphertexten entfernt werden:

$$\begin{aligned}&\left(P \oplus RC4\langle IV,k\rangle\right) \oplus \left(P' \oplus RC4\langle IV,k\rangle\right)\\ &= P \oplus P' \oplus RC4\langle IV,k\rangle \oplus RC4\langle IV,k\rangle\\ &= P \oplus P'\end{aligned}$$

Der String $P \oplus P'$ ist nun nur noch von den ursprünglichen Nachrichten abhängig und kann mit statistischen Verfahren untersucht werden. Diese Untersuchung wird einfacher, je mehr Ciphertexte mit kollidierten IV zur Verfügung stehen.

Mit der Entschlüsselung eines Klartextes gelangt man natürlich auch in den Besitz des Keystreams, mit dem er verschlüsselt wurde. So lässt sich mit der Zeit ein Wörterbuch bilden, in dem zu jedem IV der zugehörige KS abgespeichert wird. Ein vollständiges Wörterbuch für alle 16 Millionen IV benötigt bei einer Paketlänge von 1500 Bytes nur ca. 24 GB. Die Zahl tatsächlich benötigter entschlüsselter Keystreams kann sich durch

[1] Das passiert in der Praxis relativ häufig. So machen in einem Funknetz oft gerade Laptops einen Großteil der Klienten aus. Diese wechseln aus Energiespargründen aber oftmals schon nach kurzer Zeit in den Standbymodus, nach dessen Beendigung die PCMCIA Karten neu gestartet werden.

die oben beschriebene Lücke in den Vorschriften zur Wiederverwendung der IV in der Praxis noch reduzieren.

3.3.2.2 Pakete modifizieren

Ein Sekundärziel ist die Kontrolle der Datenintegrität. Mittels der Checksumme sollen Veränderungen an den Daten festgestellt werden. Da aber der CRC32 Algorithmus und der RC4 Algorithmus beide linear sind, sind bitweise Änderungen in den Paketen und korrekte Anpassung der Checksumme auch „blind", d.h. ohne Kenntnis der verwendeten Schlüssel oder des Keystreams, möglich.

So gilt für den CRC32 wegen der Linearität folgendes:

$$c(M) \oplus c(\Delta) = c(M \oplus \Delta)$$

Möchte man also an einer bestehenden Nachricht M eine Änderung Δ vornehmen, so lässt sich die Checksumme der geänderten Nachricht auch aus den für M und Δ getrennt berechneten Checksummen errechnen. Damit kann man nun blind beliebige Bits in dem Ciphertext umdrehen, die Checksumme nur für diese Änderungen berechnen, und diese an der richtigen Stelle (Paketende) mit dem Ciphertext verknüpfen. Die resultierende Nachricht ist danach wieder gültig:

$$\begin{aligned} C' &= RC4(v,k) \oplus \langle M', c(M') \rangle \\ &= RC4(v,k) \oplus \langle M', c(M \oplus \Delta) \rangle \\ &= RC4(v,k) \oplus \langle M \oplus \Delta, c(M) \oplus c(\Delta) \rangle \\ &= RC4(v,k) \oplus \langle M, c(M) \rangle \oplus \langle \Delta, c(\Delta) \rangle \\ &= C \oplus \langle \Delta, c(\Delta) \rangle \end{aligned}$$

Diese Attacke hat durchaus praktische Relevanz! Zum Beispiel kann sie bei der Bildung eines Wörterbuches helfen. Kennt man z.B. die Zieladressen einiger Pakete, kann man sie auf Adressen eigener Server verän-

dern. Freundlicherweise übernimmt der AP die Dekodierung der mittels WEP verschlüsselten Pakete und leitet sie im Klartext an den eigenen Rechner weiter. Mit dem Klartext erhält man auch Kenntnis vom verwendeten KS.

3.3.2.3 Keystream Reuse bei Authentifizierung mittels WEP

So gut gemeint das Authentifizierungsverfahren mittels WEP auch gemeint ist, so unnütz ist es leider auch. Da der AP die Challenge im Klartext an den Clienten sendet, den dieser verschlüsselt zurückzusenden hat, ist jemand, der einen solchen, erfolgreichen Vorgang belauscht, anschließend im Besitz eines Klartextes samt zugehörigen Ciphertextes. Per logischem XOR erhält er einen gültigen Keystream zu dem „gesehenen" IV. Da der Client bei der Auswahl des IV zur Verschlüsselung der Challenge freie Hand hat, kann der Lauscher sich bei dem AP nun unter Verwendung des gleichen IV und zugehörigen Keystream erfolgreich authentifizieren. Leider ist dadurch nicht nur der Authentifizierungsmechanismus selber unwirksam. Da der Lauscher im Besitz eines Keystreams ist, den er beliebig oft verwenden darf, kann er in der Folge ungehindert gültige Pakete in das Netz einspeisen. Dass er die Antworten des AP nicht entschlüsseln kann, ist da nur ein kleiner Trost.

Die meisten Anbieter raten daher ihren Kunden konsequent die Authentifizierung abzustellen, da das Netz ohne diese Sicherheitsmaßnahme paradoxerweise sicherer ist.

3.3.2.4 Aktive Maßnahmen zur Beschleunigung der Wörterbuch Bildung

In Kombination dieser Schwächen lässt sich eine Reihe von aktiven Angriffen finden, die die Bildung eines Wörterbuches erheblich beschleunigen und so schnell den gesamten Verkehr offen legen können. Eine Möglichkeit wurde bereits in Abschnitt 3.3.2.2 erläutert.

Sind die am AP angemeldeten Endgeräte zum Beispiel direkt an das Internet angebunden und kennt oder errät man einige Netzwerkadressen, kann man diesen Computern direkt eigene Pakete mit bekanntem Klartext und bekannter Größe zusenden, um den zugehörigen Cipher-

text zu belauschen. Kennt man die Netzwerkadresse nicht, helfen eventuell Emails weiter. Oder man verfügt über die Kontrolle einer Internetseite, die von den Klienten häufig besucht werden…

3.4 Lehren aus dem WEP Fiasko

Obwohl die RC4 Attacke die effektivere (weil völlig passiv, weniger Pakete benötigt) ist, können aus den indirekten Angriffen ebenfalls nützliche Lehren gezogen werden. So scheint einiger kryptographischer Sachverstand nötig zu sein, um ein tatsächlich abhörsicheres Protokoll zu definieren.

Der Standard wurde daher noch einmal überarbeitet. Noch in diesem Jahr sollen die ersten Geräte mit dem (hoffentlich) sicheren WPA Verfahren auf den Markt kommen. Bis sich dieses Protokoll durchgesetzt hat, muss man für einen sicheren Datenverkehr auf übliche Verschlüsselungsmethoden auf höheren Schichten des OSI-Referenzmodells zurückgreifen.

4 Zusammenfassung

Es wurde gezeigt, dass schon allein wegen der recht gut organisierten Suche nach offenen Netzen und deren Zweckentfremdung berechtigter Bedarf an Schutzmaßnahmen besteht. WEP suggeriert diesen Schutz zwar mit seinem Namen, schlägt aber gleich aus mehreren Gründen völlig fehl, die gesteckten Ziele wirksam zu erreichen. Einen Ausweg soll das kurz vor der Markteinführung stehende WPA Verfahren bringen.

LITERATURVERZEICHNIS

Borisov, N., Goldberg, I., Wagner, D. 2001. Intercepting Mobile Communications: The insecurity of 802.11. *MOBICOM 2001,* Italy

Borisov, N., Goldberg, I., Wagner, D. 2001b. *Security of the WEP Algorithm*. http://www.isaac.-cs.berkeley.edu/isaac/wep-faq.html Letzter Besuch: 27.7.2003

FAB Corp 2003. http://www.fab-corp.com USA. Letzter Besuch: 27.7.2003

Flickenger, R. 2001. *Antenna on the Cheap (er, Chip).* http://www.oreillynet.com/cs/weblog/view/wlg/448/ Letzter Besuch: 27.7.2003

Fluhrer, Mantin, Shamir 2001. Weaknesses in the Key Scheduling Algorithm of RC4. *Eigth Annual Workshop on Selected Areas in Crypthography*, Canada

Highspeed-Hotspots.de 2003. *WLAN-Hotspots in Deutschland*. http://www.highspeed-hotspots.de/ Letzter Besuch: 27.7.2003

NodeDB 2003. *The Wireless Node Database Project*. http://www.nodedb.com Letzter Besuch: 27.7.2003

Mobileaccess.de 2003. *Wireless LAN HotSpots*. http://mobileaccess.de/wlan/ Letzter Besuch: 27.7.2003

Personal Telco Project 2003. http://www.personaltelco.net/static/ Letzter Besuch: 27.7.2003

Stubblefield, A., Ioannidis, J., Rubin, A. D. 2001. Using the Fluhrer, Mantin and Shamir Attack to Break WEP. *ATT Labs Technical Report, TD4ZCPZZ, Revision 2.*

Tran, B. K. 2003. Wireless LAN. *Mobile Computing Seminar SS 2003*. http://www-lehre.inf.uos.de/mc/ (Vorabexemplar)

Warchalking.Org 2002. The original (v.0.9) symbols. http://www.warchalking.org/story/2002/8/20/17730/3808. Letzter Besuch: 27.7.2003

Wölfer, T. 2002. Einbruch in WiFi Netze verhindern. *PC Magazin Sonderheft „PC-Netze“*, Deutschland