Whitepaper
Wireless LAN Security

Rel. : draft / r2

René Nitzinger

International Product Manager, ELSA

Rene.Nitzinger@elsa.de

März 2002

Whitepaper Wireless LAN Security

Inhalt

ELSA AG ● Sonnenweg 11 ● 52070 Aachen ● Germany
Infoline: +49-(0)241-606-5112 ● E-Mail: PreSales@elsa.de ● Internet: www.elsa.com

Whitepaper Wireless LAN Security

1 Einleitung

Der Wireless LAN-Markt boomt. Seit der Einführung des IEEE 802.11b[1]-Standards für Wireless LANs und der Gründung der WECA[2] (Wireless Ethernet Compatibility Alliance) im Jahre 1999 wächst der Markt für lokale Funknetze mit Wachstumsraten von bis zu 100% pro Jahr. Waren es Ende 2001 bereits über 12 Mio. Wireless LAN-Geräte weltweit im Einsatz, so schätzt Gartner-Dataquest, dass ab 2005 über 50 Mio. Wireless LAN Chipsets jährlich verkauft werden.

Mit fallenden Gerätepreisen sind Wireless LANs heute nicht mehr nur professionellen Anwendungen und Firmen vorbehalten, sondern eignen sich auch optimal für den drahtlosen Internet-Zugang zu Hause oder an öffentlichen Plätzen (Public Access an Hot Spots). Alle führenden PC- und Notebook-Hersteller bieten heute bereits Geräte mit eingebautem Wireless LAN-Adapter oder als Nachrüstoption an.

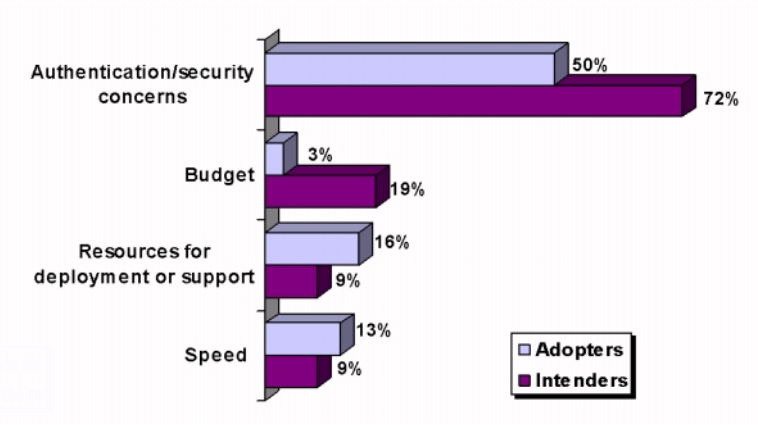

Abbildung 1) Barrieren für die Implementierung von WLANs

Die offensichtlichen Vorteile der Drahtlos-Technologie, Mobilität und Flexibilität, sind in vielen Unternehmen und bei Privatleuten anerkannt oder sogar selbstverständlich. Auch die Installation eines Wireless LANs stellt keine schwere Aufgabe dar, sondern ist auch ohne IT-Fachmann leicht zu bewerkstelligen.

Dennoch gibt es gerade in Firmen Vorbehalte gegen die WLAN-Technologie. Nämlich dann, wenn nach der Sicherheit der Netze gefragt wird. Aktuelle Untersuchungen [1] belegen eindeutig, dass insbesondere für Unternehmen das Thema Sicherheit in Funknetzen die grösste Barriere gegen den Einsatz in geschäftskritischen Bereichen darstellt. Die folgenden Ausführungen sollen dazu beitragen, die potentiellen Gefahren und geeignete Schutzmöglichkeiten besser kennen zu lernen. Denn nur so können mögliche Vorbehalte und Sorgen um den Datenschutz bewertet und individuelle Sicherheitskonzepte erstellt werden.

---

[1] IEEE 802.11b – Standard des Institute of Electrical and Electronics Engineers (englische Ausprache „Eye-triple-E“) für Wireless LANs mit Übertragungsraten bis zu 11 Mbit/s. Links: http://grouper.ieee.org/groups/802/11/

[2] WECA – Die Wireless Ethernet Compatibility Alliance führte 1999 die Wi-Fi-Zertifizierung für Wireless LANs nach IEEE 802.11b ein. Das Wi-Fi-Logo garantiert die Interoperabilität der Geräte verschiedener Hersteller untereinander. Links: http://www.wi-fi.org

2 Bedrohungen für die Sicherheit in Wireless LANs

Wie man sich mit etwas Phantasie denken kann, sind Netzwerke und insbesondere die Daten, die über diese Netze transportiert werden anfällig, für eine ganze Reihe von ungewünschten Zugriffen. Als erstes zu nennen ist sicherlich die Gefahr, dass übertragenen Daten missbräuchlich abgehört oder abgefangen und analysiert werden, d.h. die ***Vertraulichkeit*** bedroht ist. Weiterhin besteht die Möglichkeit, dass Daten bewusst manipuliert werden, um z.B. Sender oder Empfänger zu täuschen. Solche Angriffe bezeichnet man auch als Verletzung der ***Datenintegrität***.

Da heutzutage immer noch viele Netzwerke ohne spezielle Verschlüsselung oder Überprüfung von Teilnehmern arbeiten, reicht es Hackern manchmal, sich ***unerlaubten Zugang*** zum Netz zu verschaffen, um auf Netzwerk-Ressourcen, wie Server oder Drucker zugreifen zu können. Wenn dies nicht gelingt, so kommt es in der Praxis auch zu rein destruktiven ***Denial-Of-Service***-Attacken. Hierbei werden gezielt Datenpakete an zentrale Komponenten eines Netzes gesendet mit der Absicht diese physikalisch ausser Gefecht zu setzen. Direkte Sabotage an Routern, Access Points oder Switches darf natürlich ebenfalls nicht vernachlässigt werden.

Um die potentiellen Bedrohungen und den notwendigen Schutzbedarf eines Firmennetzes festzustellen, ist eine Sicherheitsanalyse notwendig. Bei der Konzepterstellung spielen neben technischen Gegebenheiten und Anwenderwünschen manchmal auch gesetzliche Vorschriften eine Rolle. Ein wunder Punkt, der dabei vielfach vergessen wird ist die Tatsache, dass Bedrohungen auf das Netz und die Firma nicht immer nur von aussen kommen, sondern auch interne Ursachen haben können.

3 Security-Mechanismen in Wireless LANs

Im folgenden Abschnitt werden die wichtigsten Sicherheits-Mechanismen für Wireless LANs erläutert. Einige der beschriebenen Funktionen sind bereits im IEEE-Standard enthalten, andere erfordern Erweiterungen in den Basis-Stationen (Access Points) oder im Backbone-Netzwerk. Die Erläuterungen beschränken sich dabei auf eine Darstellung der wesentlichen Funktionsprinzipien und deren Einsatz in drahtlosen LANs. Für tiefergreifende technische Informationen wird auf entsprechende Referenzen in Abschnitt 6 verwiesen.

3.1 WEP

WEP steht für Wired Equivelent Privacy, einem Verfahren zur Datenverschlüsselung und Authentifizierung in Wireless LANs. Wie der Name bereits sagt, soll das Verfahren eine vergleichbare Vertraulichkeit erzielen, wie in einem drahtgebundenen LAN. Die physikalische Sicherheit in einem Kabel-Ethernet ist prinzipiell höher, da die Kabel i.d.R. innerhalb eines Gebäudes verlegt sind, und der Zugang für Fremde geschützt ist. Bei einem drahtlosen LAN reicht es u.U. aus, sich in der Nähe des Netzes aufzuhalten, um Daten aus der Luft zu empfangen. Im Gegensatz zum Ethernet, wo die Datenübertragung meist unverschlüsselt erfolgt, ist WEP ein fester Bestandteil des IEEE 802.11b Protokoll-Stacks. Auch die WECA testet im Rahmen der Wi-Fi-Zertifizierung alle WLAN-Geräte auf Konformität zum WEP-Standard (bis 40 bit Schlüssellänge). Dennoch ist WEP alleine nicht mit einer Ende-zu-Ende-Sicherheitslösung zu verwechseln, die alle in Abschnitt 2 aufgeführten und erläuterten Sicherheitsanforderungen erfüllt.

WEP verwendet den 1987 entwickelten RC4-Algorithmus von RSA Security Inc, der in sehr vielen kryptographischen Implementationen, wie z.B. SSL (Secure Socket Layer) für sichere Internet-Transaktionen, verwendet wird. Aktuelle WLAN-Produkte mit WEP nutzen RC4 mit einer Schlüssellänge von 40 oder 104 bit zuzüglich einem Initialisierungsvektor (IV) von 24 bit. In der Praxis spricht man daher von den Varianten WEP64 (40 + 24 bit) und WEP128 (104 + 24 bit).

WEP-Verschlüsselung funktioniert wie in Abbildung 2 skizziert: Ein vorgegebener Schlüssel (40 oder 104 bit Länge) wird zunächst mit einem berechneten Initialisierungsvektor kombiniert. Beides zusammen bildet den Input für einen Pseudo-Noise-Generator (dem RC4-Algorithmus). Für die zu übertragenen Daten (Plaintext) wird ein Integritäts-Check (ICV) berechnet, und beides mit dem Ergebnis des RC4-Algorithmus XOR-verknüpft. Der erhaltene Code kann nun gesendet werden. Damit der Empfänger die Nachricht mit dem selben WEP-Schlüssel decodieren kann, wird der IV zusätzlich im Klartext übermittelt. Natürlich wird der IV für jede Nachricht neu berechnet.

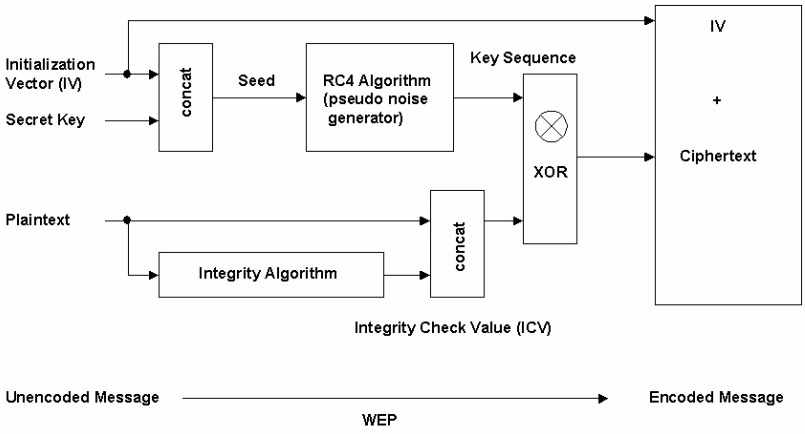

Abbildung 2) WEP-Algorithmus

Derselbe WEP-Schlüssel kann neben der reinen Datenverschlüsselung auch zur Authentifizierung verwendet werden. WEP definiert dazu zwei Verfahren, die Open System Authentication (OSA) und die Shared Key Authentication (SKA). Open System Authentication ist genaugenommen keine Authentifizierung. Jede Station kann sich mit einem Access Point assoziieren und unverschlüsselte Daten empfangen. Bei der Shared Key Authentication prüft der Access Point während der Assoziierung

einer Funkstation im Challenge-Response-Verfahren, ob ein gültiger WEP-Schlüssel vorhanden ist. Erst nach erfolgreicher Prüfung können angemeldete Stationen Daten übertragen.

WEP definiert keine weiteren Verfahren zum Schlüsselmanagement. Die Schlüssel müssen auf allen Stationen und Access Points lokal vorhanden sein. I.d.R. können allerdings vier verschiedene WEP-Schlüssel bei Sender und Empfänger eingetragen werden, was den Schlüsselwechsel erleichtert, weil zu einer Zeit mehr als ein gültiger Schlüssel zur Decodierung vorhanden sein kann. Der Sendeschlüssel wird jedoch an jeder Station fest vorgegeben.

Im Markt gibt es bereits eine Reihe von Erweiterungen zu WEP. Dabei handelt es sich sowohl um standardkonforme als auch um proprietäre Ergänzungen. Ein Beispiel für eine konforme Verbesserung ist **WEPplus**, eine modifizierte Implementation von WEP, die eine bekannte Schwäche (weak keys, siehe Abschnitt 4) des Verfahrens bei der Generierung von IVs beseitigt. Andere Vorschläge, wie „Rapid Re-Keying“ von RSA sollen die Sicherheit von WEP weiter steigern, sind aber nicht kompatibel zum heutigen 802.11b- oder Wi-Fi-Standard.

3.2 Access Control

In WLANs mit Basis-Stationen, sogenannten Infrastrukturnetzen, können die Access Points eine Zugangskontrolle auf Basis von Hardware-Adressen gewährleisten, da jegliche Kommunikation im WLAN über die Basis-Stationen abgewickelt wird. Mittels einfachen Access-Control-Listen (ACL) werden registrierte MAC-Adressen entweder zur Kommunikation zugelassen oder abgewiesen. Einige Basis-Stationen können den Datenverkehr auch nach speziellen Protokollen filtern .

ACLs mit den MAC-Adressen der Client-Stationen müssen auf jedem Access Point vorhanden sein. Dazu werden entweder alle Adressen fest im internen Speicher des Access Points abgelegt oder per RADIUS[1]-Protokoll nach Bedarf von einem zentralen Server abgefragt. Eine zentrale Ablage erleichtert dabei vor allem das Management in einem grossen Netzwerk mit vielen Teilnehmern.

3.3 Closed Network

Eine wichtige Funktion in Wireless LANs nimmt der Netzwerkname ein, der in technischen Dokumenten auch als ESS-ID bezeichnet wird. Über den Namen eines Funknetzes können verschiedene WLANs getrennt werden. An jeder Client-Station muss zur Auswahl des WLANs der passende Netzwerkname eingetragen werden. Allerdings besteht auch die Möglichkeit, die ESS-ID „ANY“ zu verwenden, um sich an beliebigen Wireless LAN Access Points in der Nähe anzumelden. Einige WLAN-Adapter und -Treiber unterstützen dazu auch eine Scan-Funktion, mit der sich eine Liste aller Funk-Netzwerke in Reichweite auf Knopfdruck ermitteln lässt.

Scan und ANY-Anmeldung funktionieren nicht bei eingeschalteter Closed Network-Funktion. Für Clients sind solche geschlossenen Netze unsichtbar. Nur wenn der Name explizit bekannt ist, kann eine Assoziierung mit einer Basis-Station mit aktivierter Closed-Network-Funktion erfolgen.

3.4 IEEE 802.1x/EAP

802.1x ist ein Standard des IEEE für lokale Netze, der im Juni 2001 veröffentlicht wurde, und insbesondere bei Wireless LANs Furore macht. Denn 802.1x erweitert WLANs um die Funktion „Port Based Network Access Control“, d.h. im Klartext einer Authentifizierungs-Möglichkeit für Benutzer und Stationen. EAP (Extensible Authentication Protocol) übernimmt dabei die Auswahl des Authentifizierungs-Mechanismus zwischen den Client- und Basis-Stationen.

Im IEEE-Jargon besteht das Szenario einer 802.1x-Anmeldung aus folgenden Komponenten (siehe Abbildung 3). Der „Supplicant“ ist im allgemeinen ein Client-PC, Notebook oder PDA ausgestattet mit einem Netzwerkadapter. Der PC-Treiber für die Karte muss den 802.1x-Standard unterstützen und eine

[1] RADIUS – Remote Dial-In User Authentication Service, ein Verfahren zur zentralen Authentifizierung von Benutzern oder Stationen. RADIUS ermöglicht zusätzlich die Übermittlung von Abrechnungsdaten.

Client-Software zur Konfiguration muss vorhanden sein. Windows XP enthält bereits alles Notwendige für 802.1x, wenn die Funknetzwerkkarte vom Betriebssystem erkannt wird (WHQL tested). Der „Authenticator“ ist das Gegenstück zum Supplicant, in einem WLAN also der Access Point. Authenticator und Supplicant tauschen per EAP (genauer: EAP-over-LAN) die Authentifizierungs-Daten aus. Die tatsächliche Überprüfung der Benutzerdaten vom Supplicant geschieht allerdings durch den „Authentication Server“. Die Kommunikation zwischen Authenticator und Authentication Server findet per RADIUS-Protokoll statt. Auch der RADIUS-Server muss die EAP-Erweiterungen unterstützen.

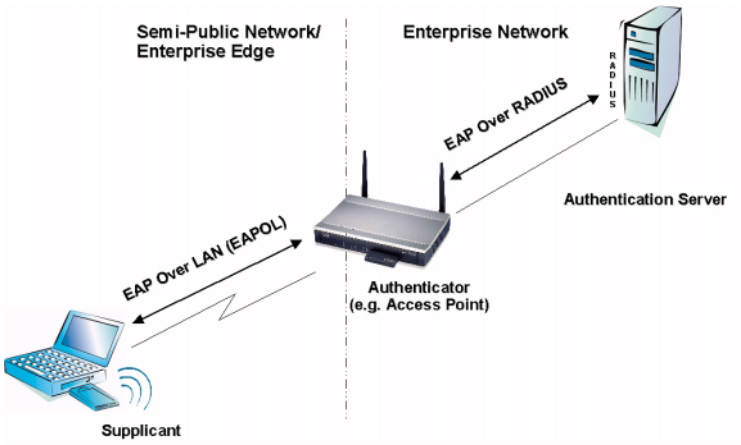

Abbildung 3) IEEE 802.1x-Topologie

EAP und IEEE 802.1x stellen also das Rahmenwerk zur Authentifizierung dar. Wie die Identität von Benutzern und Stationen tatsächlich überprüft wird, bestimmt die EAP-Methode. Die wichtigsten Methoden nutzen dazu entweder digitale Zertifikate[1] oder Passwörter, wie die folgende Tabelle beschreibt.

EAP-Methode	Supplicant	Authenticator	Authentication Server
EAP-TLS	Zertifikat	Zertifikat	Schnittstelle zu Certification Authority
EAP-TTLS	Passwort	Zertifikat	Schnittstelle zu Certification Authority, Benutzerdatenbank
EAP-MD5	Passwort	-	Benutzerdatenbank

Tabelle 1) EAP-Authentifizierungs-Methoden

Der wesentliche Gewinn für die Sicherheit in Wireless LANs durch 802.1x entsteht durch die Kombination des Authentifizierungs-Verfahrens mit der WEP-Verschlüsselung. Denn nachdem Client und Netzwerk gegenseitig ihre Echtheit überprüft haben, ist es möglich, den WEP-Schlüssel automatisch zu generieren oder vom Authentication Server zuweisen zu lassen. Auch ein regelmäßiger Schlüsselwechsel (Key-Roll-Over, Re-Keying) und eine Re-Authentifizierung nach einer festgelegten Zeit sind möglich. Passive Attacken auf WEP, wie in Abschnitt 4 beschrieben, werden damit erschwert bzw. unmöglich gemacht. Der Zeitraum zwischen zwei Überprüfungen und Schlüsselwechseln muss dafür hinreichend klein gewählt werden.

3.5 VPN

VPN-Technologien sind weitverbreitet und eignen sich hervorragend für den Aufbau von sicheren Verbindungen über unsichere Netzwerke. Ein sogenanntes Virtual Private Network kann zwischen Clients, zwischen Client und Gateways oder auch als sicherer Tunnel zwischen zwei Netzwerk-Gateways aufgebaut werden. Die geläufigsten VPN-Protokolle sind IPSec, PPTP und L2TP.

[1] Digitale Zertifikate sind elektronische Dokumente, welche die Echtheit und Integrität von Personendaten oder Institutionen bestätigen. Zertifikate, auch digitale Signaturen genannt, können bei sogenannten Trust-Centern, wie z.B. Verisign, DTAG oder Entrust, bezogen oder für interne Zwecke selbst erzeugt werden. Ein Zertifikat enthält insb. folgende Informationen: Versionsnummer, Seriennummer, Signatur-Algorithmus, Aussteller, Gültigkeitsdatum, öffentlicher Schlüssel.

In WLANs können VPN-Clients als Bestandteil einer firmeninternen Sicherheits-Lösung eingesetzt werden. Ein typisches WLAN-VPN-Szenario ist in Abbildung 4) dargestellt. Alle WLAN Access Points befinden sich hierbei in einem „unsicheren" Netz (z.B. VLAN[1] oder DMZ[2]) und sind weitgehend transparent für alle Wireless-Clients. Das Firmennetzwerk wird durch VPN-Gateways oder Firewalls am Rand des Netzes abgesichert.

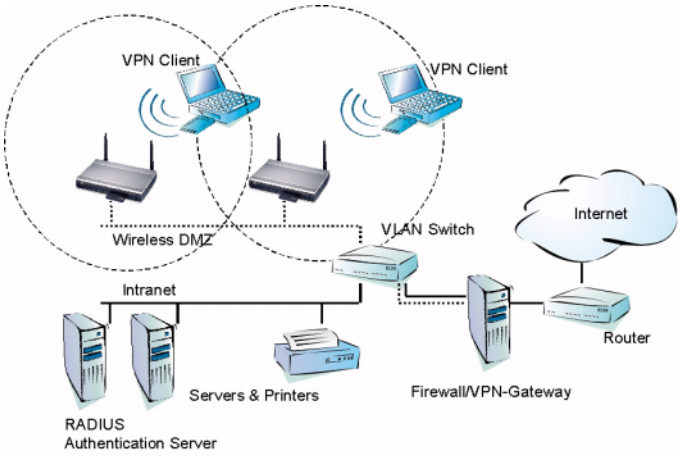

Abbildung 4) Wireless DMZ

Zur Authentifizierung und zur Datenverschlüsselung müssen auf den PCs, Notebooks o.ä. VPN-Clients installiert sein. Damit kann eine sichere Verbindung (ein Tunnel) zum Gateway oder zur Firewall aufgebaut werden. Erst nach der Anmeldung über den VPN-Client kann ein Datenaustausch in das Zielnetz erfolgen. Die Vorteile von VPNs liegen vor allem in der Unabhängigkeit von der Infrastruktur des Netzes. Insbesondere in Firmen, in denen VPN bereits für Remote-Access-Zwecke zum Einsatz kommt, bietet sich die gleichzeitige Verwendung für eine internes WLAN geradezu an. Die zusätzliche Sicherheit durch VPN-Technologien erkauft man sich dabei i.d.R. durch höheren Overhead, zusätzlichen Management-Aufwand, sowie ggf. einen gewissen Verzicht auf Komfort in der Bedienung.

3.6 OUA

Open User Authentication™ (OUA) ist die Bezeichnung für einen Authentifizierungs-Mechanismus, der von ELSA speziell für öffentliche WLANs entwickelt wurde. Denn insbesondere für drahtlose Internet-Dienste werden über den physikalischen Netzzugang hinaus Möglichkeiten zur Authentifizierung und Abrechnung von Benutzern zwingend benötigt.

Das ELSA OUA-Verfahren löst die Anforderung über ein Web-basiertes Login-Verfahren zum Anwender und einer Backend-Authorisierung über RADIUS. Für den Benutzer bedeutet dies, dass er vor Zugriff auf Internet-basierte Dienste zunächst seinen Internet-Browser starten und sich per Benutzername und Passwort anmelden muss. Im Hintergrund prüft das OUA-Gateway (WLAN Access Point oder Router) die Gültigkeit per RADIUS an einem zentralen Benutzerserver und übermittelt Abrechnungsinformation für die Online-Sitzung.

Die *Open User Authentication* ist Bestandteil der *LANCOM Public Spot-Option* für *ELSA LANCOM*-Router und Access Points.

3.7 Traffic Lock

Wie in jedem Ethernet üblich, können auch in einem Wireless LAN alle Client-Stationen untereinander kommunizieren. In einigen Anwendungen ist dies aus Sicherheitsgründen jedoch nicht erwünscht. Z.B.

---

[1] VLAN – Ein „virtuelles LAN" verhält sich wie ein verkabeltes LAN ist aber lediglich eine logische Gruppierung von Netzwerk-Stationen auf einem physikalischen Netz. Da VLANs per Software konfiguriert werden, kann die Gruppierung flexibel geschehen.

[2] Eine de-militarisierte Zone (DMZ) ist ein halb-öffentlicher Bereich eines Netzes, der durch Firewall-Mechanismen vom Firmennetz getrennt ist.

an Public Spots[1] (Hot Spots) können zwar alle mobilen Benutzer auf Internetdienste zugreifen, untereinander sollen die verschiedenen Teilnehmer jedoch getrennt sein, um Missbrauch zu vermeiden.

Die Trennung von Stationen auf dem Link-Layer (OSI-Ebene 2) erledigt die Traffic-Lock-Funktion in den Access Points der ELSA LANCOM-Serie. Die Benutzertrennung gilt dabei nicht nur für Stationen, die an einem Access Point angemeldet sind, sondern für alle Stationen, die sich in einem Wireless LAN (Extended Service Set) bewegen. Denn via IAPP, dem Inter Access Point Protokoll, tauschen die LANCOM Access Points den Anmeldezustand der Stationen untereinander aus; auch wenn Stationen zwischen verschiedenen Funkzellen wechseln (Roaming).

3.8 IEEE 802.11i

Neben diversen Zusatz-Tools einiger Hersteller, die auf Applikations- oder Netzwerkebene die Sicherheit erhöhen können, gibt es auch in den Standardisierungsgremien Arbeitsgruppen, die an einer Verbesserung der aktuellen Verfahren und der Normierung von neuen Standards arbeiten. Zu nennen ist hier insbesondere die Task-Group 802.11i des IEEE [3]. Die bisherigen Entwürfe (Drafts) beinhalten auch den oben beschriebenen 802.1x-Mechanismus zusammen mit einem geregelten Schlüsselaustausch für WEP, dem sogenannten TKIP (Temporal Key Integrity Protocol). Ausserdem soll der RC4-Algorithmus in WEP um das modernere Verfahren „AES“ ergänzt werden.

Die geplanten Neuerungen sind heute noch nicht final als Standard veröffentlicht. Einige der geplanten Verbesserungen sind jedoch schon in aktuellen WLAN-Produkten umgesetzt (z.B. 802.1x). Während andere Punkte wahrscheinlich eine Veränderung an der Hardware erfordern werden und deshalb nicht 100% kompatibel zu „alten“ Adaptern sein können.

[1] Public Spot – oder auch Hot Spot – ist ein Zugangspunkt für ein öffentliches oder halb-öffentliches WLAN. Beispiele: Flughafen, Café, Hotel, Bahnhof, ...

4 Bekannte Attacken gegen Wireless LANs

Für ein gutes Verständnis der genannten Sicherheitsfunktionen werden in diesem Whitepaper nicht nur die Arbeitsweisen und Vorteile der Verfahren beschrieben, sondern auch bekannte Schwächen und potentielle Angriffspunkte genannt. Nur so ist eine objektive Bewertung der Sicherheit möglich. Die genannten Fälle sind keinesfalls als Anleitung zum Missbrauch zu verstehen!

Im Laufe des Jahres 2001 sind verschieden Schwächen von aktuellen WEP-Implementationen aufgedeckt worden. Im Januar stellte man an der University of California (Berkley) [4] fest, dass WEP anfällig ist für bestimmte passive Attacken basierend auf „known Plaintext" und „Dictionaries". Klartext- und Wörterbuch-Attacken arbeiten nach folgendem Prinzip:

Klartext- und Wörterbuch-Attacken
Zur Verschlüsselung verwendet WEP einen Strom von Pseudozufallszahlen, der mit den zu übertragenen Daten mittels XOR verknüpft wird. Die Zufallszahlen werden durch den Algorithmus RC4 aus einem geheimen Schlüssel k berechnet. Aus einem Klartext P wird der verschlüsselte Text C = P ^{XOR} RC4(k) berechnet. Für feste k gilt jedoch C1 ^{XOR} C 2 = P 1 ^{XOR} P 2 , d.h., man kann mit einem bekannten Paar (P 1 , C 1) auch P 2 = (C 1 ^{XOR} C 2) ^{XOR} P 1 berechnen und somit sämtliche Kommunikation entschlüsseln, ohne k zu kennen.
Um diesen Effekt zu verhindern, sieht WEP zusätzlich den Initialisierungsvektor (IV) vor, der sich bei jedem Datenpaket ändern muss: C = P ^{XOR} RC4 (IV, k). Damit die Gegenseite das Paket wieder entschlüsseln kann, wird der IV dem übertragenen Datenpaket als Klartext hinzugefügt. Der IV ist aber nur 24 Bit groß. Somit ist spätestens nach ein paar Tagen durchschnittlicher Netzlast dieser Zahlenraum erschöpft. Hat man sich in dieser Zeit eine Tabelle (oder ein „Wörterbuch") aller IVs mit zugehörigen Codes und bekannten Klartextpassagen angelegt, so ist man in der Lage, weitere Pakete mit sich wiederholenden IVs zu entschlüsseln.

Schwache Schlüssel
Im August 2001 deckten Fluhrer, Mantin, Shamir [5] weiter Schwachpunkte bei der Verwendung von RC4 in WEP fest. Hauptvorwurf gegen typische WEP-Implementationen ist das Vorhandensein einer grossen Menge von schwachen Schlüsseln (weak keys). Die Ursache dafür liegt vor allem in der unzureichenden Länge des Initialisierungsvektors (IV) und einer Eigenschaft des RC4-Verfahrens, bestimmte Muster in den Codes zu erzeugen. Bei einer Kryptoanalyse reduzieren solche Muster die Anzahl der zu untersuchenden Schlüssel deutlich. Verschiedene Cracking-Tools wie z.B. Airsnort [6] und WEPcrack [7] nutzen diese Ergebnisse von Fluhrer, Mantin, Shamir und behaupten von sich, WEP-Schlüssel innerhalb weniger Stunden herauszufinden.

Problem IV und Lösung WEPplus
Wie weiter oben beschrieben wird der 24 bit lange Initialisierungsvektor für jedes Datenpaket berechnet, zusammen mit dem WEP-Schlüssel codiert und zusätzlich im Klartext übertragen. Die Generierung dieses IV ist (wie in den obigen Attacken zu sehen) ein kritischer Punkt. Tatsächlich war und ist z.T. immer noch die Implementierung des IV-Generators in vielen WLAN-Produkten nachlässig. Dabei werden IVs z.T. mit statischen Anfangswerten (Null) gestartet, inkrementell erhöht oder erzeugen oben genannte weak keys. Genau diesen Missstand beseitigt WEPplus, eine Implementation von WEP, die vom Chip-Hersteller Agere Systems eingeführt wurde. IVs werden hierbei „intelligent" erzeugt, so dass Tools wie Airsnort oder Wepcrack keinen Ansatzpunkt mehr haben. Ein Versuch, WEPplus-Schlüssel zu knacken, wird daher eher zur Brute-Force-Attacke – bei 2^{64} bzw. 2^{128} möglichen Permutationen (möglichen Schlüsseln) kein Erfolg versprechender Ansatz.

Authentifizierung und Key-Management
Das in WEP definierte Authentifizierungs-Verfahren Shared Key Authentication (SKA) wird in der Praxis selten genutzt. Tatsächlich bringt es wenig Sicherheit und ist z.B. anfällig für Man-In-The-Middle-Attacken. Mit SKA ist der Schutz des WEP-Schlüssels geringer als ohne Authentifizierung (OSA). Das vermutlich schwerwiegendste Problem in vielen, insbesondere grossen WLAN-Installationen ist die Schlüsselverteilung oder das Key-Management. Wie oben erläutert beinhaltet WEP bisher kein Key-Management, die Schlüsselvergabe erfolgt i.d.R. manuell und alle Stationen verwenden denselben Schlüssel. Die ad-hoc-Lösung dafür bietet das oben beschriebene 802.1x-Verfahren. Denn nach einer gesicherten und gegenseitigen Authentifizierung von Client und Access Point können WEP-Schlüssel regelmäßig neu generiert (Re-Keying) und den Stationen automatisch übermittelt werden. Bei einer

Neugenerierung von WEP-Schlüsseln im 20- bis 60-Minuten-Takt dürfte es hinreichend schwer sein, selbst RC4-basierte WEP-Verfahren zu knacken.

Man-In-The-Middle
Man-In-The-Middle-Attacken sind nicht immer leicht zu erkennen. Solche Angriffe arbeiten nach dem Prinzip, dass sich eine fremde Station in die Kommunikation zwischen zwei Teilnehmern einmischt und sich zu einer oder zu beiden Seiten für den jeweils anderen Partner ausgibt. In einem WLAN könnte das eine fremde Basis-Station sein, die sich gegenüber Client-PCs genauso verhält, wie der eigentlich gewünschte Access Point. Dazu muss also die Konfiguration des attackierten Access Points bekannt sein. In einem solchen Fall merkt ein Benutzer u.U. gar nicht, dass seine Verbindung umgeleitet wurde. Zufriedenstellend vermeiden lassen sich Man-In-The-Middle-Angriffe nur durch gegenseitige Authentifizierung der Teilnehmer, beispielsweise mit IEEE 802.1x/EAP-TLS oder IPSec.

Intruder-Attacken und Sniffer
Zum Schutz vor unberechtigtem Netzwerkzugang dienen, wie in den Abschnitten 3.2 + 3.3 beschrieben, auch die Funktionen Access Control über MAC-Adressen-Filter und Closed Network. Leider sind aber auch diese Features alleine keine Patentlösung zur Zugangskontrolle. Denn die 802.11-Protokoll-Definition sieht vor, dass sowohl die MAC-Adressen als auch die ESS-ID in Daten- oder Management-Frames über die Luft unverschlüsselt übertragen werden. Das bedeutet, dass mit speziellen Wireless-LAN-Sniffer-Programmen die Informationen ausgespäht werden können und möglicherweise an den Client-Stationen gefälscht werden. Ein einfacher LAN-Sniffer reicht jedoch nicht aus, um die ESS-ID eines geschlossenen Netzes (closed network) ausfindig zu machen.

ELSA AG ● Sonnenweg 11 ● 52070 Aachen ● Germany
Infoline: +49-(0)241-606-5112 ● E-Mail: PreSales@elsa.de ● Internet: www.elsa.com

5 Praktische Ratschläge für sichere WLANs

Sicherheit ist relativ. Damit ist gemeint, dass eine allumfassende Sicherheitslösung nicht pauschal definiert werden kann. Vielmehr müssen die speziellen Anforderungen, der Schutzbedarf, das Risiko und die Bereitschaft der Benutzer untersucht werden, für Netzwerk-Sicherheit evtl. auch Einschränkungen oder Auflagen in Kauf zu nehmen. Die folgenden Beispiele dienen daher lediglich zur Orientierung für die Einrichtung Ihres persönlichen Wireless LANs.

5.1 Sicherheit in kleinen WLAN-Netzen

Bei einer geringen Anzahl von drahtlosen PCs und einer bis zwei Basis-Stationen hält sich der Managementaufwand für ein Netzwerk in Grenzen. Das gesamte LAN mit allen Teilnehmer lässt sich gut überblicken. Häufig werden nicht ganz so hohe Sicherheitsansprüche gestellt wie etwa bei einer Bank oder Versicherung mit kritischen Kundendaten. Deshalb reichen i.d.R. die WLAN-immanenten Funktionen WEP, ACL und Closed Network aus. Das bedeutet, jede Station wird mir ihrer MAC-Adresse am Access Point registriert und erhält manuell einen WEP-Schlüssel zugeteilt. Am besten ist natürlich der Einsatz von WEPplus an allen Stationen. WEP-Schlüssel sollten von Zeit zu Zeit gewechselt werden, z.B. beim Ausscheiden eines Mitarbeiters. Die Closed-Network-Funktion garantiert, dass das Funknetzwerk nicht mit Standardmitteln gefunden wird. Durch die Kombination dieser drei Verfahren und einem Zugangsschutz der Netzwerk-Server mit Benutzername und Passwort kann sich ein kleines Unternehmen vor Angriffen durch bekannte Hacker-Tools hinreichend absichern.

5.2 Wireless-Sicherheit im Unternehmen

Ein mittelständisches oder grosses Unternehmen stellt deutlich höhere Ansprüche an die Netzwerk-Sicherheit. In der Regel ist dazu eine eigene IT-Abteilung für die Betreuung der Netzinfrastruktur zuständig. Aufgrund der Anzahl der Netzteilnehmer und Stationen ist ein zentrales Management zwingend erforderlich. Weiterhin ist im Normalfall bereits eine Ethernet-Verkabelung und ein Netzbetriebssystem vorhanden in das ein Wireless LAN integriert werden soll, ohne dass die physikalische Sicherheit verloren geht.
Die vorgeschlagene Lösung für diesen Fall ist eine Kombination aus IEEE 802.1x mit WEPplus und einer gegenseitigen Authentifizierung auf Basis von digitalen Zertifikaten (EAP-TLS). Eine solche Infrastruktur ist in Abbildung 5) skizziert.

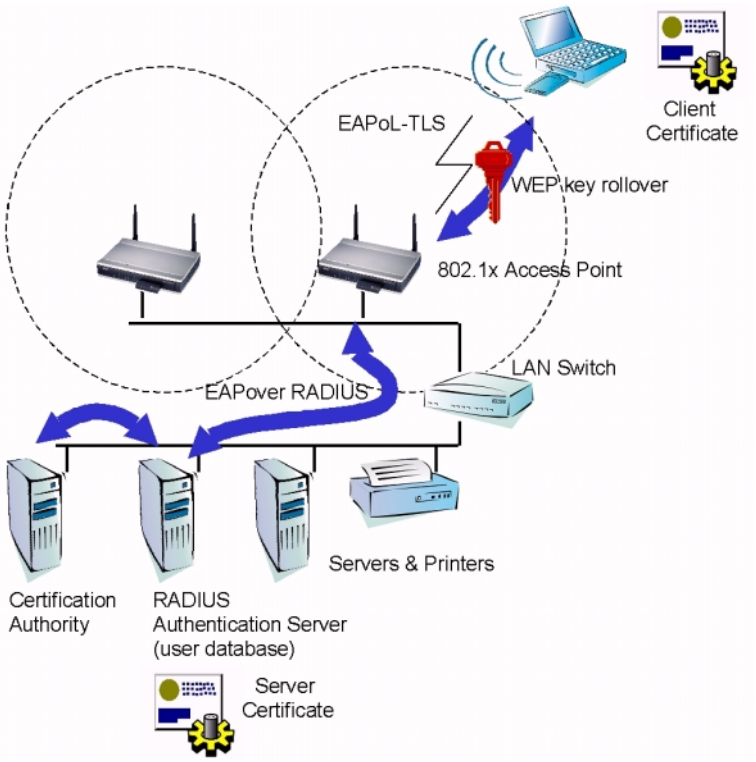

Abbildung 5) IEEE 802.1x im Unternehmen

Jeder Benutzer erhält für seine Wireless-Station ein digitales Zertifikat, die sowohl seine eigene Identität ausweist als auch zur Überprüfung von zulässigen Basis-Stationen genutzt wird. Die Authorisierung und die Verteilung der WEP-Schlüssel erfolgt zentral von einer Benutzerdatenbank im Backbone-Netz der Firma. Die IT-Abteilung hat also die vollständige

Kontrolle über Zugang und Key-Management im Wireless LAN. Es können ausserdem an zentraler Stelle Nutzungsprotokolle angefertigt und ausgewertet werden. Potentielle Einbruchversuche können rechtzeitig erkannt und lokalisiert werden. Auch aus Benutzersicht ist diese Lösung sehr komfortabel, da ein User ausser der Einrichtung seines Zertifikats und seiner gewohnten Netzanmeldung keine weiteren Vorkehrungen treffen muss.

5.3 Sicherheit in Filialunternehmen

Andere Voraussetzungen liegen häufig in Unternehmen mit mehreren Standorten vor. Denn meist ist zur Vernetzung der Filialen oder zur Anbindung von Aussendienstmitarbeitern bereits eine VPN-Infrastruktur vorhanden. Insbesondere dann, wenn mobile Anwender VPN-Clients zur Einwahl ins Unternehmensnetz benutzen, bietet es sich an, diese Infrastruktur für ein Wireless LAN weiterzubenutzen. Die Abbildung 4) skizziert das Szenario.

Das komplette WLAN mit allen Access Points und Client-Stationen ist an jedem Firmenstandort durch ein VPN-Gateway (oder Firewall mit VPN-Funktion) vom Intranet getrennt. Diese „de-militarisierte Zone“ muss dabei nicht unbedingt physikalisch abgegrenzt sein. Häufig eignen sich VLANs (Virtual LANs) besser, weil eine zusätzliche Verkabelung dadurch vermieden wird.

Die Anmeldeprozedur an ein solches WLAN erfolgt für den mobilen Benutzer auf die selbe Weise wie ein Remote-Zugang per Wählverbindung. Er benötigt auf seinem PC den firmeneigenen VPN-Client. Authentifizierung von Benutzern und Schutz der Daten erfolgen ausschliesslich auf Basis dieser VPN-Lösung. Die WEP- oder Access-Control-Funktion auf MAC-Ebene des WLANs kann ausgeschaltet bleiben. Die Gesamtsicherheit wird also von der eingesetzten VPN-/Firewall-Lösung bestimmt.

5.4 Sicherheit an Public Spots

Im Unterschied zu einem geschlossenen Firmennetz gilt es an öffentlichen Access Netzwerken jedem beliebigen Teilnehmer Zugang zu gewähren, sofern er eine gültige Berechtigung vorweist. Dazu werden an allen bisher implementierten Wireless Public Spots Web-basierte Authentifizierungsverfahren mit Benutzername und Passwort eingesetzt. Wie weiter oben im ELSA OUA-Verfahren beschrieben, werden diese Benutzerdaten verschlüsselt übermittelt. Nach der Authentifizierung verläuft der Datentransfer aber i.d.R. unverschlüsselt. D.h. der Benutzer ist selbst für die Vertraulichkeit seiner Daten verantwortlich. Dazu sollten z.B. E-Mails verschlüsselt übertragen werden (z.B. S-MIME, PGP) und Internet-Transaktionen geschützt abgewickelt werden (z.B. via SSL). Abgesicherter Remote Access kann über optionale VPN-Clients realisiert werden.
Auf jeden Fall sollte die öffentliche Basis-Station oder das Access-Netz in der Lage sein, verschiedene Benutzer an einem Public Spot zuverlässig gegenseitig abzuschirmen. Jeder Benutzer muss sicher sein können, dass ein unerwünschter Zugriff auf seine eigene Festplatte zu jedem Zeitpunkt ausgeschlossen ist. Diesen Schutz bietet das Traffic-Lock-Feature aus Abschnitt 3.7.

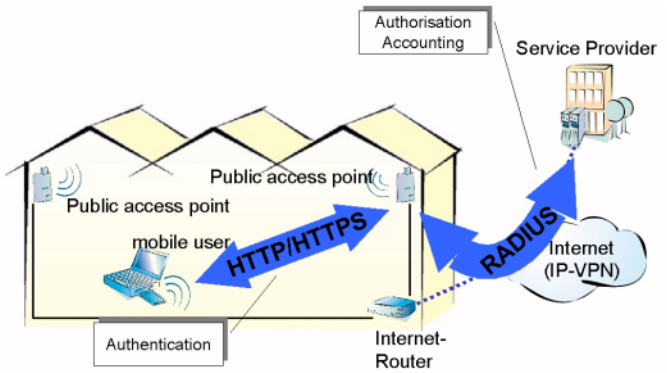

Abbildung 6) Public Spot-Konfiguration

5.5 Allgemeine Sicherheitsrichtlinien

Wie bereits erwähnt ist die Forderung nach Sicherheit nicht pauschal zu beantworten und kann auch nicht durch einen singulären Mechanismus gelöst werden. Tatsächlich besteht ein Security-Konzept immer aus einer Kombination von Funktionen und Vorschriften. Neben den bereits genannten Mitteln auf System- oder Netzwerkebene müssen folgende Richtlinien immer mitberücksichtigt werden:

- Benutzen Sie eingebaute Sicherheitsfunktionen der Komponenten (z.B. WEP, ACL, Closed Network).
- Ergänzen Sie die Low-Level-Funktionen um Authentifizierungs- und Verschlüsselungsverfahren auf Anwendungsebene (z.B. Netzwerk-Login, IPSec, E-mail-Verschlüsselung).
- Nutzen Sie Virenschutz-Programme oder „Personal Firewall"-Funktionen an jedem Arbeitsplatz.
- Gehen Sie sorgsam mit Passwörtern und Schlüsseln um und wechseln Sie diese in regelmäßigen Abständen.
- Überprüfen Sie Log-Files oder Reports regelmäßig, um mögliche Angriffe frühzeitig zu erkennen.
- Vergessen Sie bei der Erstellung des Sicherheitskonzeptes nie, dass Attacken auch von innen ausgehen können.

6 Literaturverzeichnis

[1] „Wireless LAN Study" von der WECA und Microsoft, Oktober 2001

[2] Sultan Weatherspoon: „Overview of IEEE 802.11b Security" http://developer.intel.com/technology/itj/q22000/articles/art_5.htm

[3] IEEE 802.11 Working Groups, http://grouper.ieee.org/groups/802/11/

[4] University of California, Berkley „Security of the WEP algorithm" http://www.isaac.cs.berkeley.edu/

[5] „Weaknesses in the key scheduling algorithm of RC4", Fluhrer, Mantin, Shamir, August 2001 http://www.crypto.com/papers/others/rc4_ksaproc.ps

[6] Airsnort, http://airsnort.shmoo.com

[7] WepCrack, http://wepcrack.sourceforge.net/

[8] IEEE Draft P802.1X/D11, „Standard for Port based Network Access Control"

[9] „An initial Security Analysis of the IEEE 802.1X Standard", University of Maryland, Februar 2002

[10] "PPP EAP TLS Authentication Protocol," IETF RFC 2716, Aboba, B., Simon, D., http://www.ietf.org/rfc/rfc2716.txt

[11] "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," Blake-Wilson, http://ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-00.txt

[12] „Secure Authentication, Access Control, and Data Privacy on Wireless LANs", http://www.funk.com

[13] "Protected EAP", http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-02.txt