Dr. Suppan International Institute

Der Netzwerk Insider

Oktober 2002

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Sicherheit in Wireless LAN: Eine endlose Geschichte?

von Dr. Simon Hoff und Hans Peter Mohn

Die Nutzer sind verunsichert: Es gibt wohl kaum einen Bereich in der Kommunikationstechnik, der so dynamisch und damit so schwer einschätzbar ist, wie der Bereich der drahtlosen und mobilen Datenkommunikation und speziell der WLAN. In der "Buchstabensuppe" von IEEE 802.11 brodeln neue Techniken. Manche dienen der natürlichen Fortentwicklung des Systems (z.B. 802.11a und 802.11g) und manche sind aus der Not geboren.

In die letztere Kategorie gehört die Arbeit der "Task Group i", kurz TGi, die in 802.11i münden wird und ihre Wurzel in einem GAU der WLAN-Standardisierung hat. Leider haben sich die in IEEE 802.11 spezifizierten kryptographischen Mittel als vollständig unzulänglich erwiesen. Die eingesetzte Verschlüsselungsmethode ist innerhalb von kürzester Zeit gebrochen worden. Mit allgemein zugänglichen Werkzeugen hat sich der Einbruch in fremde WLAN scheinbar zum Volkssport entwickelt. Hektisch haben daraufhin die WLAN-Ausrüster ihre Systeme mit proprietären Zusatzfunktionen versehen,

Misslungene
IEEE 802.11-Buchstabensuppe:
Hilft Nachwürzen?

und IEEE 802.11 war gefordert, den Standard nachzubessern. Als Folge wurde TGi ins Leben gerufen mit dem Auftrag, die Sicherheit in WLAN auf den Stand der Technik zu bringen. Auch wenn der Standard 802.11i noch nicht verabschiedet ist, es lichten sich erste Ergebnisse, die andeuten, in welche Richtung es nun gehen wird. Bis dahin gilt allerdings, dass der WLAN-Anwender sich in einem Dschungel unterschiedlicher Lösungen und Empfehlungen zurecht finden muss.

In diesem Artikel werden wir die Sicherheitsproblematik von WLAN diskutieren und dabei unter anderem die unterschiedlichen Anforderungen von privaten WLAN und öffentlichen Hotspots untersuchen. Wir werden auch der Frage auf den Grund gehen, ob sich mit 802.11i tatsächlich die Lage entscheidend bessern wird oder ob wir uns schon jetzt darauf einstellen sollten, dass es bei einem Sicherheits-Patchwork bleibt. In diesem Zusammenhang lohnt der Blick auf die Verwandten der Mobilfunkszene, denn die haben ja dieselben Grundprobleme; aber hier ist der eben skizzierte GAU bisher ausgeblieben. Es ist daher eine Überlegung wert, ob es da nicht bewährte Techniken gibt, die für ein WLAN wiederverwendbar sind.

weiter Seite 9

Netzwerk- und System-Management

LowCost Tools erobern System-Management

Seit mehreren Jahren werden entweder kostenfrei oder zu geringen Lizenzkosten eine ganze Reihe von Tools im Umfeld des Netzwerk- und System-Managements angeboten. In der Vergangenheit wurden diese Tools eher belächelt, ihr Funktionsumfang war gering, die Bedienung umständlich und Know-how-intensiv und die Qualität der grafischen Repräsentanz (zum Beispiel im Reporting) mager. Hinzu kamen die Bedenken zur weiteren Entwicklung der Tools und die nicht vorhandene Support-Möglichkeit.

Diese Situation ändert sich immer mehr. LowCost Tools nehmen an Attraktivität immer mehr zu.

Dies hat verschiedene Gründe:

- Die Lizenzkosten der traditionellen Tools sind gerade für kleinere und mittelständische Unternehmen einfach zu hoch, in der Summe aller Tools entstehen Lizenzkosten, die mit keinem Argument der Welt zu rechtfertigen sind.

- Die offenbar rückläufige Nachfrage nach hochpreisigen Lizenzen zwingt die Hersteller, die Wartungskonditionen in fast sittenwidrige Höhen zu schrauben (schon 15% sind bei dem Pflegeaufwand der meisten Produkte kaum akzeptabel, jede Wartungsgebühr über 20% hat aus meiner Sicht stark willkürliche Züge).

- Parallel werden die LowCost Tools immer besser, die kontinuierliche Weiterentwicklung trägt ihre Früchte. Gleichzeitig wird angesichts der permanenten Weiterentwicklung auch klar, dass die Befürchtungen in Richtung einer mangelnden Entwicklung für eine Reihe der Tools nicht zutreffen.

- Das Knowhow der Kunden im Umgang mit diesen Tools ist deutlich besser geworden, dies trifft vor allem auf Produkte zu, die aus dem Linux-Umfeld stammen. Auch sind inzwischen viele Tools unter den gängigen Windows-Lösungen verfügbar, die früher nur im Linux-Bereich angeboten wurden.

weiter Seite 3

Zum Geleit

Angriff auf den Feldbus: Ethernet in der Industrie

1986 wurde Ethernet von Siemens zur Überraschung des Marktes im Produktionsumfeld eingeführt. Dies war zum damaligen Zeitpunkt mehr als überraschend, galt doch das CSMA/CD-Verfahren als instabil und unzuverlässig und viele gaben der Ethernet-Technologie auf Dauer gegen die Marktmacht der IBM mit dem Token Ring keine Chance :). Heute ist der Token Ring Historie (bei einer ganzen Reihe von Firmen noch gelebte, lebendige Historie) und Ethernet ist im Fertigungsumfeld zur Vernetzung der großen Steuerungen und der Leitrechnerebene der allseits akzeptierte Industrie-Standard.

Der Großteil eines Fertigungsnetzwerks im Sinne der Zahl angeschlossener Stationen findet jedoch im Bereich der kleinen Steuerungen und der Motorik/Sensorik statt, der so genannten Feldebene. Hier wird der eigentliche Produktionsprozess gesteuert. Dies ist die bisherige Domäne von Profibus, Modbus und den anderen, meist herstellerspezifischen Feldbus-Netzwerken. Da die Hersteller mit der individuellen Auslegung dieser Kommunikations-Lösungen ihre Märkte abgrenzten und den Marktzugang für andere Firmen erschwerten, zeigten sie lange Zeit keine große Motivation, diesen Zustand zu ändern. Speziell Siemens grenzte sich bis noch vor wenigen Wochen gegen einen Ethernet-Kompletteinsatz in der Feldebene ab.

Nun ist der Damm gebrochen. Alle international relevanten Hersteller von Siemens über Schneider bis hin zu Rockwell haben sich zu Ethernet als der zukünftigen neuen Feldbus-Technologie bekannt. Ausnahme bleibt bis auf weiteres der gesamte Bereich Motion Control, da Ethernet im so genannten harten Realzeitbereich von Mikrosekunden zur Zeit keine Antwort auf die dort gegebenen Anforderungen geben kann.

Auf den ersten Blick sollte man also meinen, dass alle betroffenen Anwender erleichtert aufatmen können. Bei näherer Betrachtung wird daraus wohl mehr ein tiefes Luftholen werden. Im Detail wird das "neue" Ethernet in der Produktion anders realisiert als bisher üblich. Dominierten auch in den letzten Jahren noch Yellow Cable und Glasfaser mit Bus- und Sternstrukturen den LAN-Markt in der Produktion, so basiert das zukünftige Ethernet überwiegend auf einer Twisted Pair-Verkabelung. Genau hier liegt ja auch der Preisvorteil für die Hersteller kleinerer Steuerungen. Wer jetzt auf den Gedanken kommt, dass dies doch angesichts der vorhandenen positiven Erfahrungen mit Twisted Pair im Bürobereich doch eine feine Sache ist, der irrt.

Die Kombination aus notwendigen Entfernungen, Zahl und Lokation der Steuerungen sowie verfügbarer Platz für Verteilertechnologie führt in vielen Fällen zu einer Twisted Pair Ketten-/Bus-Schaltung. Dies hat gravierende Konsequenzen für die einzusetzenden Switches, werden doch nur wenige Ports pro Switch benötigt. Berücksichtigt man noch die Umgebungsbedingungen mit Temperatur, Feuchtigkeit, Vibration und Stoß so wird schnell klar, dass in der Regel die aus dem Büroumfeld bekannten Produkte hier kein Heimspiel haben werden.

So hat sich in der Produktion in den letzten Jahren auch still und heimlich ein eigener Netzwerk-Markt entwickelt, der nun zu explodieren scheint. Die Hauptanbieter heißen hier nicht CISCO, Nortel oder Enterasys sondern Siemens und Hirschmann. Spätestens bei der Betrachtung des IP67-Switches von Hirschmann oder der Twisted Pair-Steckertechnik von Siemens fällt auf, dass die bekannten Büroprodukte im harten Fertigungsbereich nichts zu suchen haben.

So sind im Produktionsbereich mit dem Eindringen von Ethernet in den Feldbusbereich ganz eigene und neue Infrastrukturen gefordert. Weder die vorhandenen Verkabelungs-Standards nach EN50173 noch die bekannten Design-Alternativen Lokaler Netze sind hier ohne weiteres verwendbar. So stellt sich auch die allseits beliebte Frage nach Spanning Tree oder OSPF, nach Layer-2 kontra Layer-3-Design hier definitiv nicht. Beide sind in dieser Umgebung schlicht und ergreifend sobald Realzeit gefragt ist unbrauchbar.

Aber auch das, was die traditionellen Steuerungshersteller anbieten, kann nicht unhinterfragt akzeptiert werden. So ist die Konzentration auf eine vieradrige Kabel- und Steckertechnik angesichts der aktuellen Trends im Chip-Markt (Wechsel von der 100 Mbit/s zur 1000 Mbit/s Chipgeneration) sowie der erheblichen Vorteile von Gigabit für Realzeitanwendungen kaum zu verstehen. Dies gilt auch für entsprechende Stecksysteme wie den M12, die maximal eine Übergangsbedeutung haben können.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-
VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Zum Geleit

Für die meisten bestehenden Feldbus-Umgebungen ist zudem eine Migration erforderlich, die neben der Ablösung auf Layer-2 auch eine Befassung mit den eigentlichen Steuerungsfunktionen auf Layer-5-7 erfordert. Speziell im Bereich Layer-3/4 unterscheiden sich die Ansätze der verschiedenen Herstellergruppen auch in der Frage einer realzeitfähigen Flusssteuerung sehr stark.

Die Ablösung der Feldbusse Richtung Ethernet ist ein Muss. Und sie wird schnell kommen, zu groß sind die Kostenvorteile auch für Hersteller und Anwender. Aber wir treffen hier auf eine ganz eigene Netzwerk-Welt mit eigenen Spielregeln (ich erinnere mich da an meinen ersten Arbeitstag nach der Hochschulzeit im Stahlwerk bei Thyssen).

Wir haben das Industrie-Ethernet für Sie aufgearbeitet. Ab November starten unsere Seminare (siehe Seiten 5 und 6) zu diesem Thema. Von der Verkabelung über die Redundanz- /Verfügbarkeitsfrage bis zur Anwendungs-Funktionalität. Ob Profibus oder Modbus, wir informieren über den zukünftigen Einsatz von Ethernet auch im Feldbusbereich.

Und es wird spannend. Auch die traditionellen LAN-Hersteller a la CISCO haben erkannt, dass hier einer der weltweit größten Märkte für Netzwerktechnik liegt. Sie werden sich dem Marktvorsprung von Siemens und Hirschmann nicht kampflos ergeben. Da ich selber aus dem Fertigungs-Umfeld komme, freue ich auf einen spannenden Wettbewerb in den nächsten Monaten. Hoffentlich unterschätzen CISCO und Co. nicht die Anforderungen des harten Produktionsumfelds. Hier reicht gutes Marketing alleine nicht aus. Hier ist auch Kenntnis über den Produktionsprozess gefordert. Schließlich kauft der Kunde in vielen Fällen ja gar kein Datennetz sondern eine schlüsselfertige Anlage.

Ich würde mich freuen, Sie in unseren Seminaren zu diesem Thema begrüßen zu können.

Ihr
Dr. Jürgen Suppan

drsuppan@comconsult-akademie.de

LowCost Tools

Fortsetzung von Seite 1

Natürlich werden LowCost-Produkte nicht für jeden eine Alternative sein. Der Konfigurations- und Customizing-Aufwand wird in größeren Projekten nicht tragbar sein. Auch sind diese Tools häufig nicht für einen intensiven Mehrbenutzer-Einsatz ausgelegt (dies kann partiell durch eine Web-Oberfläche oder den Einsatz des Windows-Terminal-Servers kompensiert werden).

Aber gerade für die kleineren Kunden mit dem schmalen Geldbeutel wird es Zeit, sich diesem Thema zu widmen. Aus diesem Grund haben wir für sie eine Untersuchung gestartet und nach geeigneten Tools Ausschau gehalten.

Wir werden ihnen ausgewählte Produkte auf dem Netzwerk- und System-Management-Forum 2002 in einem Workshop präsentieren.

Die Inhalte finden Sie auf Seite 4
(Änderungen vorbehalten)

Fax-Antwort an ComConsult 02408/955-399

Nur noch wenige Plätze!

Netzwerk- und System-Management Forum 2002
04.11. - 07.11.02 in Königswinter

Anmeldung

Ich melde mich an zum
Netzwerk- und System-Mangement Forum 2002 in Königswinter

☐ vom 04.11. - 07.11.02 **(mit Tutorium)** zum Preis von € 1.790,-- zzgl. MwSt.

☐ vom 05.11. - 07.11.02 **(ohne Tutorium)** zum Preis von € 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____
(Übernachtung/Frühstück € 110,--)

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Faxen Sie einfach diesen Abschnitt an **02408/955-399** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Netzwerk- und System-Management Forum 2002 - Die Inhalte

Montag, 04.11.02: Tutorium

Netzwerk- und System-Management im Wandel der Anforderungen
- Anforderungs-Profile
- Lösungen
- Das ComConsult 10-Stufen-Modell
- Typische Problembereiche
- Erfolgreiche Umsetzung von SLM
- Markt- und Produktsituation
- Lowcost-Tools
- Anwendungs-Szenarien, Beispiele

Dr. Jürgen Suppan

Dienstag, 05.11.02: Vortragstag

Netzwerk-Technologien im Wandel
- 10 Gigabit Ethernet: Neue Chip-Generation
- SAN-Alternative: 10 Gigabit Fiber Channel
- Neue Generation von Netzwerk-Prozessoren
- WLANs erfolgreich umsetzen

Dr. Franz-Joahim Kauffels

Vom Service-Level- zum Kosten-Management
- Ist Kosten-Management sinnvoll und wirtschaftlich
- Lösungs-Ansätze zum Kosten-Management
- Einbettung in eine SLM-Lösung

Dipl.-Kfm. Martin Woyke

Netzwerk-Management-Lösung der Finanzverwaltung-NRW
- Über 150 Standorte zentral und effizient managen
- Einfluss der Netzwerk-Architekur auf den Management-Bedarf
- Lösungs-Architektur: Zusammenspiel ausgewählte Produkte
- Ausgewählte Kernanwendungen für den zentralen Betrieb
- Projekt-Erfahrungen, Empfehlungen

Karl-Heinz Hommen-Menz

Service Management und Gestaltung von Service-Views mit Impact-Funktionalität
- Praxisbericht zum Einsatz des Service Navigators der HP OpenView Familie vom Landesamt für Datenverarbeitung und Statistik NRW

Klaus Rittinger

ITIL: Zauberwort oder Luftloch
- Auswirkung einer prozessgestützten Organisation auf Wertschöpfung und Wirtschaftlichkeit

Lutz Peichert

Mittwoch, 06.11.02 Workshop-Tag

Workshop A / Vertiefungsvortrag: ITIL für Service Level Management
- Zentrale Prozesse einer ITIL-Lösung für SLM
- Einsatzerfahrungen und Empfehlungen

Leitung: Jürgen Dierlamm

Workshop B: Service-Level-Management
- Live-Vergleich führender Produkte

Leitung: Dr. Jürgen Suppan

Workshop C: Vom Switch-Management zum integrierten QoS- und Security-Management
- Live-Vergleich führender Management-Lösungen

Leitung: Petra Borowka

Workshop D: Von der Protokoll-Analyse zur integrierten Netzwerk-Management- und Service-Level-Management-Lösung
- Live-Vergleich führender Tools

Leitung: Dr. Jochen Wetzlar

Workshop E: Vom Berichts- zum Kosten-Management
- Live Vergleich führender Tools
- Darstellung typischer Lösungs-Szenarien

Leitung: Dr. Jürgen Suppan

Workshop F: Eine integrierte Gesamtlösung auf der Basis der Integration der Produkte verschiedener Hersteller
- Live-Vorführung eines Integrationsansatzes

Leitung: Ralf Horstmann

Workshop G: Capture / Replay-Lösungen als zentrales Element von Verfügbarkeits- und Performance-Management im Rahmen einer Service-Level-Management-Lösung
- Live-Vergleich ausgewählter Produkte

Leitung: Dr. Armin Wachter

Workshop H: Lowcost Tools als ernstzunehmende Alternative
- Live-Präsentation ausgewählter Lowcost-Lösungen

Leitung: Oliver Flüs, Dietlind Hübner

Donnerstag, 07.11.02

Lösungen für Service-Level-Management im Überblick
- SLM-Reporting
- SLM-Messungen
- SLM-Consolen
- Wo stehen die wichtigsten SLM-Produkte

Ralf Horstmann

Folgen und Herausforderungen von IP-VPNs für System-Management
- VPN-Technologien und ihre Bedeutung für sichere System-Architekturen
- Lösungsbeispiele und Einsatz-Szenarien
- Rückwirkung auf System-Management
- Integration des Sicherheits-Managements von VPN-Lösungen in das IT-Management
- Herausforderung Benutzer-, Schlüssel- und Zertifikatsverwaltung
- Folgen für das Client-Management

Dr. Behrooz Moayeri

Netzwerk-Management-Lösungen 2002: neue Lösungsarchitekturen
- Warum die "alten" Ansätze hinterfragt werden sollten
- Neue Funktionsbereiche
- Verschiebung der Tool-Schwerpunkte
- Marktentwicklungen
- Resultierende Szenarien

Petra Borowka

Capture-/Replay-Technologien als Basis von Verfügbarkeit- und Performance-Management als zentrales Element einer SLM-Lösung
- Wie arbeiten Capture-/Replay-Lösungen
- Warum sind sie für eine SLM-Lösung unverzichtbar
- Was leistet ein Robot-System
- Wie gut können Transaktionen sicher bestimmt werden
- Welche Probleme entstehen
- Wie können entstehende Probleme gelöst werden
- Welche Produkte gibt es

Dr. Armin Wachter

Vom Service Level Management zum Service Level Agreement
- Was leistet Service-Level-Management
- Wie wird es umgesetzt
- Was sind zentrale Erfolgs-Faktoren
- Wie wird ein SLA aufgesetzt
- Woran kann ein SLA scheitern
- Wie werden SLAs erfolgreich umgesetzt

Dr. Jürgen Suppan

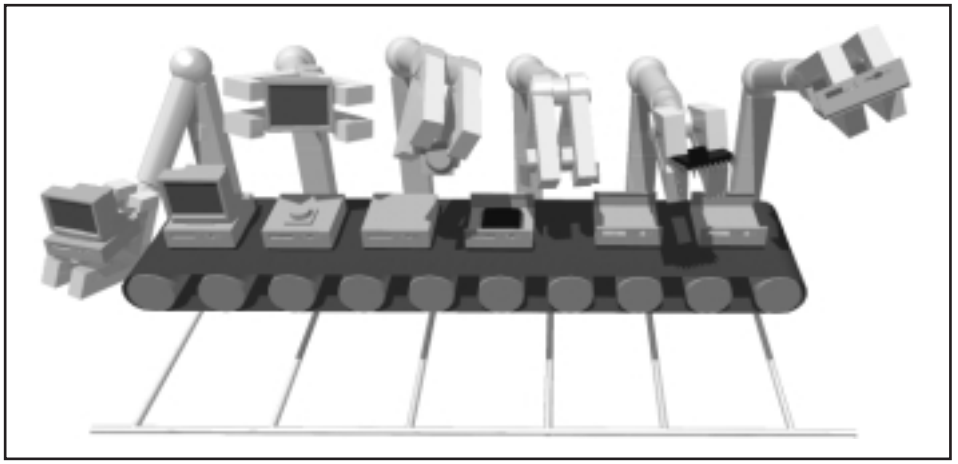
Neues Seminar

Ethernet in der Industrie

Vom 25. bis 29. November 2002 veranstaltet die ComConsult Akademie in Aachen zum ersten Mal ihr neues Seminar "Ethernet in der Industrie".

Zum Thema

Die industrielle Kommunikation zwischen Sensoren, Steuerungen, Robotern und Rechnern befindet sich im Umbruch. Von den heutigen Lösungen werden viele in den nächsten Monaten und Jahren abgelöst werden. Der neue Standard für die Kommunikation in Produktionsumgebungen ist weltweit Ethernet. Die bisherigen herstellerspezifischen Feldbussysteme werden zum großen Teil verdrängt im Sinne einer durchgängigen Kommunikation über alle Unternehmensbereiche. Kommunikation wird damit einfacher, leistungsstärker, herstellerneutral(er) und auch preiswerter. Doch mit dem Eindringen von Ethernet in den Feldbusbereich entstehen viele komplexe Fragen. So lassen sich Netzwerk-Produkte aus dem Bürobereich nicht in jedem Fall im Produktionsbereich einsetzen. Sie sollten zum Beispiel in ihrer Temperatur-, Schock-, Vibrations- und Feuchtigkeitsempfindlichkeit den Eigenschaften der Steuerungen entsprechen, die durch sie vernetzt werden. Ebenso stellt sich sofort auch die Frage, ob Ethernet in der Lage ist, die hohen Realzeitanforderungen aus dem Bereich von Bewegungssteuerungen zu erfüllen. Und damit noch nicht genug, ist zu klären, welche Art der Verkabelung im Fertigungsbereich vorzusehen ist.



Das Seminar wendet sich an alle, die sich mit Ethernet im industriellen Einsatz beschäftigen, Lösungen evaluieren oder auch einsetzen müssen. Dabei sind gleichermaßen Administratoren, Planer und Entscheider angesprochen.

Das Seminar erklärt, wie und in welcher Form ein Ethernet-Netzwerk in einer Produktions-Umgebung erfolgreich realisiert und betrieben werden kann. Die bestehenden Normungs-, Produkt- und Marktentwicklungen werden erläutert. Die typischen Ethernet-Probleme werden dargestellt und Lösungsansätze werden präsentiert. Nicht zuletzt wird die Frage beantwortet, für welche Art von Anwendungen Ethernet geeignet ist und für welche nicht.

Die Teilnehmer erfahren
- Ob und wie weit eine Ethernet-Lösung die Anforderungen der Produktion erfüllen kann
- Welche Art von Feldbussystem durch Ethernet problemlos verdrängt werden kann und welche nicht; wie die Realzeiteignung von Ethernet zu bewerten ist
- Wie die Stabilität und Zuverlässigkeit von Ethernet und Ethernet-Produkten zu bewerten ist
- Wie sie die Leistung einer derartigen Lösung beeinflussen können und welche typischen Fehler sie dabei unbedingt vermeiden müssen
- Welche Anforderungen die Netzwerk-Produkte im Produktionsbereich erfüllen sollten und wie die Marktsituation demgegenüber aussieht
- Was bei der Realisierung von Verkabelungslösungen im Fertigungsbereich zu beachten ist, welche Standards und Produkte existieren und was fehlt
- Wie sich ausgewählte Hersteller gegenüber dieser Entwicklung positionieren
- Wie die diversen Normierungsbestrebungen (z.B. IAONA) einzuschätzen sind

Inhalt 1. und 2. Tag

Das Leistungsverhalten von Ethernet

"Ethernet und die Fertigungsindustrie"
- Gründe für den "Siegeszug" von Ethernet
- Netzwerktrends in der Fertigungsindustrie
- Wer arbeitet an dem Thema, wer ist relevant, was gibt es schon, woran wird noch gearbeitet?
- Was muss ein Fertigungsnetzwerk können?

"Grundlagen der Kommunikation"
- Das ISO/OSI-Referenzmodell
  – Grundsätzliche Architektur eines Kommunikationssystems
  – Aufgaben der verschiedenen Kommunikationsebenen
  – Protokolle und Protokollbausteine
  – Verbindungsorientierte und verbindungslose Protokolle

Elementare Mechanismen von Kommunikationssystemen
- "Shared Ethernet" nach IEEE 802.3
- Überblick über wichtige 10/100 Mbit/s Ethernetvarianten

Optimale Auslegung von Ethernet-Netzwerken

"Shared Networks" kontra "Switched Networks"
- Wann macht was im Produktionsbereich Sinn?

Vor- und Nachteile von "Switched Ethernet"
- Aufbau und Arbeitsweise von Ethernet-Switches
- Vollduplex Ethernet
- Echtzeitfähigkeit von Ethernet: Voraussetzungen, Verfahren
- Risiken geswitchter Netzwerke und wie sie vermieden werden
- Industrie-taugliche Buchungsfaktoren in der Planung geswitchter Netzwerke

Aufbau redundanter Netzwerkstrukturen
- Link Aggregation • Classic Spanning Tree
- Rapid Spanning Trees für den Fertigungsbereich
- Routing-Verfahren: OSPF / VRRP

Management von geswitchten Netzwerken
- SNMP / RMON • Fehlersuche in geswitchten Umgebungen

Ethernet in der Industrie

Inhalt 3. bis 5. Tag

Netzwerkprotokolle und ihre Industrie-Tauglichkeit

Wie funktioniert heute ein Fertigungsnetzwerk?
- Wie sieht ein Fertigungsnetzwerk aus?
- (Feld-)Bussysteme
  - Spezifika
  - Nachteile
- Tauglichkeit von Ethernet für industrielle Netzwerke

TCP/IP - ein Überblick

TCP/IP Kommunikationsprotokolle
- IP, TCP, UDP:
  - Paketaufbau
  - Adressierungskonzepte
  - Protokollfunktionen
  - Flusskontrolle
  - Retransmission
- Steuerungsmechanismen:
  - Flusskontrolle und Quittierung,
  - Fehlersituationen und -behebung

TCP/IP Anwendungsprotokolle in einer kurzen Übersicht
- http, FTP, SNMTP

Bewertungen für den industriellen Einsatz

Der Veranstalter behält sich Änderungen im Programm vor.

Erfolgreiche Umsetzung von Ethernet-Netzwerken in der Produktion

Strukturierte Verkabelung nach EN 50173
- Struktur und Topologie
- Kabelmedien und Stecker
- Einsatzgebiete heute
- Anwendbarkeit für industrielle Netzwerke

Industrielle Verkabelungen
- Anforderungen der Industrie
- Normierung industrieller Datenverkabelung
- Materialauswahl
- EMV in der Industrie

Aktive Komponenten für den industriellen Einsatz
- Anwendungsgebiete: Produktionshalle, Maschine
- Besondere Schutzvorkehrungen
- Redundanzverfahren

Aktuelle Herstellerlösungen
- Brauchen wir hersteller-spezifische Lösungen?
- Wer wird sich durchsetzen?

Industrial Ethernet Varianten heute

Die wichtigsten Lösungen für Industrial Ethernet
- EtherNet/IP
- Modbus/TCP
- Interbus on Ethernet
- ProiNet

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Ethernet in der Industrie

Ich melde mich an für das Seminar
Ethernet in der Industrie

☐ vom 25. - 29.11.02 in der AGIT Aachen zum Preis von € 1.990,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Hotelzimmer

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Anzeige

Nur noch wenige Tage: 10 % Frühbucherrabatt bis 15.10.02

Wireless LAN Forum 2002

25.11. - 27.11.02 in Königswinter

Bis zum 15.10.2002 bieten wir eine Vorbuchungsphase für das Forum an. Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

3 Tage (mit Wireless LAN Grundlagenreport) zum Preis von € 1.655,-- statt 1.838,-- zzgl. MwSt.
3 Tage (ohne Wireless LAN Grundlagenreport) zum Preis von € 1.430,-- statt 1.590,-- zzgl. MwSt.

Alle Teilnehmer, die unsere Frühbucherphase bis zum 15.10.02 nutzen, bekommen zusätzlich zum ermäßigten Frühbucherrabatt ein Exemplar des brandaktuellen Technologie Reports

Wireless LAN Sicherheitsreport kostenfrei bis 15.10.02

Alle Teilnehmer, die das Wireless LAN Forum 2002 mit dem Wireless LAN Grundlagenreport buchen, erhalten ebenfalls den Wireless LAN Sicherheitsreport kostenfrei obendrauf.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Wireless LAN Forum 2002

Ich melde mich an zum
Wireless-LAN-Forum 2002
vom 25.11. - 27.11.02in Königswinter

☐ **mit Wireless LAN Grundlagenreport und Wireless LAN Sicherheitsreport** zum Preis von € 1.655,-- zzgl. MwSt.*

☐ (ohne Wireless LAN Grundlagenreport) **mit Wireless LAN Sicherheitsreport** zum Preis von € 1.430,-- zzgl. MwSt.*

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____
(Übernachtung/Frühstück € 110,--)

* Preise gültig bis 15.10.02

_____ Name	_____ Vorname
_____ Firma	_____ Funktion
_____ Straße	_____ PLZ, Ort
_____ Telefon	_____ Fax
_____ eMail	_____ Unterschrift

Neuer Sonderreport des Labors der ComConsult Technologie Information

Wireless LAN Sicherheitsreport

Sicherheit ist ein Schlüsselthema bei der Einrichtung von Wireless LANs. Zu einfach ist das Abhören einer unprofessionell gesicherten Installation, eine einfache 128-Bit-Verschlüsselung ist unzureichend. Neben dem allgemeinen Bestreben nach Sicherheit gibt es mindestens folgende Anwendungsbereiche, in denen weitergehende Sicherheitsmaßnahmen zwingend erforderlich sind:

- **Notebooks von Führungskräften mit Wireless-Anschluss**
- **Konferenz- oder Besprechungsbereiche**
- **Einsatz von Wireless LANs in sensiblen Anwendungsbereichen wie Medizintechnik oder Personalverwaltung**

Hier setzt unser brandaktueller Sonderreport zum Thema Sicherheit in Wireless LANs an. Wir haben für Sie die bestehenden Sicherheitsrisiken untersucht, beschreiben die zur Zeit verfügbaren Gegenmaßnahmen und geben einen Ausblick über die in den nächsten Monaten zu erwartenden Lösungen inklusive der gerade laufenden Normungs-Aktivitäten. Dieser Report ist für jeden Planer und für jeden Betreiber einer Wireless-LAN-Lösung ein absolutes Muss!

Bereits Anfang 2001 hatten erste Untersuchungen amerikanischer Universitäten deutliche Schwächen im Konzept des IEEE-Standards 802.11 aufgezeigt, die vorgestellten Szenarien waren aber noch eher theoretischer Natur und setzten mit einigem Know-how gepatchte Treiber voraus. Mittlerweile lösen in regelmäßigen Abständen Meldungen über weiterhin explodierende Umsatzzahlen Nachrichten über die mangelnde Sicherheit dieser Netze ab. In Teilen dieser Berichterstattung werden Funknetze und Sicherheitsstandards ironisch als Widerspruch in sich bezeichnet.

Wie so oft vermischen sich auch hier Mythos, Hören-Sagen und Wirklichkeit. Wo liegen denn die spezifischen Probleme von Funknetzen und ihre Ursachen? Eine Sicherheitsanalyse von Funknetze unterliegt speziellen Aspekten, wobei neben funktechnischen und netzwerktechnischen Besonderheiten eben auch betriebliche Gesichtspunkte eine große Rolle spielen. Der Report lenkt Ihren Blick auf die grundsätzliche Problematik und stellt verschiedene Lösungsmöglichkeiten vor.

Im ersten Teil werden nach einer genauen Analyse der Sicherheitsfeatures aktueller Produkte die bekanntesten Angriffsszenarien auf WLANs vorgestellt und Sie in die Lage versetzt, das jeweiliges Gefährdungspotenzial realistisch einzuschätzen.

- Was bedeutet eigentlich Session-Hijacking?
- Mit welchem Aufwand können verschlüsselte WLANs abgehört werden?
- Soll WEP-Verschlüsselung eigentlich eingesetzt werden oder besser nicht?
- Was verstehen Hersteller unter "Closed System"?
- Welche weiteren Lösungsansätze stehen zur Verfügung?
- Wie werden sich Funknetze in der Zukunft weiterentwickeln?

Welche grundlegenden Design-Entscheidungen müssen Sie bereits heute berücksichtigen, um auf die neue WLAN-Generation umsteigen zu können. Worauf sollten Sie bei kurzfristigen Investitionsentscheidungen achten?

Im zweiten Teil des Reports werden die IEEE-Standards 802.1x und 802.11i vorgestellt und ihr Einfluss auf das Design sicherer WLANs untersucht. Ein letzter Teil stellt so genannte "strukturierte Funknetze" vor, untersucht Sicherheitskonzepte wie VPN oder Firewalls auf ihre Tauglichkeit, Wireless LANs abzusichern und diskutiert ausführlich die Rolle des Clients, denn wie man leicht einsieht, können Wireless Drucker, Notebooks und PDAs nicht einheitlich behandelt werden.

Bei der Betrachtung vieler dieser funkspezifischen Probleme treten am Rande auch einige Gesichtspunkte von kabelgebundenen Netzen zu Tage:

- Wie sicher ist eigentlich Ihr kabelgebundenes LAN?
- War Ihnen bewusst, dass auch reine ethernet-basierte Unternehmensnetze, in denen keinerlei Funktechnik eingesetzt wird, mit Hilfe der WLAN-Technologie ausgespäht werden können?

Funknetze - und das machen die beschriebenen Lösungen deutlich – lassen sich im Gegensatz zur häufig kolportierten Meinung sicher betreiben. Jedoch handelt es sich hierbei nicht um ein einfach zu installierendes Plug'n'Play-Produkt, Funknetze benötigen eine spezielle Infrastruktur und müssen zudem in einen unternehmensweiten Sicherheitsstandard integriert werden.

Der Report hilft Ihnen bei der Bewertung aktueller und zukünftiger Technologien und gibt Ihnen Argumentations- und Entscheidungshilfen genauso wie detaillierte technische Informationen. Er ist damit ein unverzichtbares Hilfsmittel für Betreiber und Verantwortliche und die ideale Ergänzung zum Wireless LAN Grundlagenreport.

Der Wireless LAN Sicherheitsreport ist wie der Wireless LAN Grundlagenreport zu beziehen über den Verlag (ComConsult Technologie Information).

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung

Ich bestelle

☐ **Wireless LAN Sicherheitsreport**
zum Preis von € 298,--
zzgl. MwSt. und Versandkosten

☐ **Wireless LAN Grundlagenreport**
zum Preis von € 349,--
zzgl. MwSt. und Versandkosten

_____
Unterschrift

_____
Name, Vorname

_____
Firma, Abteilung

_____
Straße

_____
PLZ, Ort

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von € 5,-- zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports € 10,-- zzgl. MwSt. (Bei Versendungen ins Ausland € 25,-- bzw. bei 2 oder mehr Reports € 30,-- zzgl. MwSt.)

Sicherheit in Wireless LAN: Eine endlose Geschichte?

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung und blickt auf jahrelange Projekterfahrung im Bereich lokaler Netze und mobiler Kommunikationssysteme zurück.
hoff@comconsult.com

Dipl.-Ing. Hans Peter Mohn ist bei der ComConsult Beratung und Planung für die Erstellung und die Organisation des Betriebes von IT-Sicherheitsmaßnahmen zuständig.
mohn@comconsult.com

Fortsetzung von Seite 1

Die Beliebtheit von Wireless LAN als drahtlose Erweiterung traditioneller LAN ist ungebrochen. Nicht nur in den klassichen Anwendungsbereichen der Produktion, Logistik, Medizin und im privaten Sektor sind WLAN auf dem Vormarsch. Moderne Arbeitsmethoden sind nun einmal geprägt von Mobilität.

Typisch sind kleinen Projektgruppen, die aufgabenorientiert aus verschiedenen Fachabteilungen gebildet werden und deren Arbeitsplatz dort ist, wo Teammitglieder sich aktuell zusammenfinden. Dabei ersetzt der Notebook zunehmend den klassischen Desktop PC als Arbeitsplatz, und das WLAN erlaubt auf komfortable Weise den mobilen Zugang zu allen benötigten Informationen unabhängig vom aktuellen Aufenthaltsort. Der Grundgedanke, dass ein Arbeitsplatz nicht ortsgebunden sondern personengebunden sein sollte, ist nicht neu. Er ist schließlich ein Motor für die Weiterentwicklung mobiler Kommunikationssysteme. Jedoch kann GSM mit GPRS zur Zeit nicht wirklich die Bandbreite liefern, die ein mobiler Internet- und Intranetzugang erfordert, und UMTS kommt auch nicht recht voran. Daher wundert es nicht, dass öffentliche WLAN (so genannte Public Spots oder Hotspots) wie Pilze aus dem Boden sprießen.

Hierbei kommen fast ausschließlich Systeme nach den Standards der Serie IEEE 802.11 des Institute of Electrical and Electronics Engineers (IEEE) zum Einsatz. Genauer gesagt sind es Systeme nach IEEE 802.11b, welche zusammen mit der Ausrüsterinitiative WECA, die mit dem WiFi-Zertifikat für die Interoperabilität von WLAN-Produkten sorgt, die Grundlage für das Wachstum im WLAN-Bereich geschaffen haben.

Die Kommunikation über Funk bedeutet immer Übertragung auf einem Shared Medium. Neben der Möglichkeit der gegenseitigen Störung von Sendungen bedeutet ein Shared Medium stets auch die prinzipielle Abhörbarkeit, die Möglichkeit des unerlaubten Zugangs zum WLAN und die Störbarkeit von Übertragungen (ob beabsichtigt oder nicht). Neben Mechanismen zur geregelten simultanen Nutzung des Mediums durch mehrere Nutzer, erfordert ein System zur Datenübertragung über Funk immer auch Mittel zur Authentifizierung der Teilnehmer dem Netz gegenüber und die Verschlüsselung der Daten zumindest auf der Funkstrecke. In diesen grundsätzlichen Anforderungen unterscheiden sich WLAN nicht von mobilen Kommunikationssystemen wie GSM.

1. WLAN nach 802.11 im Überblick

Zunächst wollen wir kurz die grundlegenden Konzepte und die Terminologie der Wireless LAN erläutern. Eine detaillierte Darstellung von Arbeitsweise, Einsatzbedingungen und Produkten kann im Technologie Report "Wireless LANs" gefunden werden (siehe [1]).

Grundsätzlich hat ein WLAN zwei Komponenten: ein mobiles Endgerät (Client) und einen Access Point, der als Basisstation die Kommunikation zwischen mobilen Endgeräten und der kabelgebundenen Infrastruktur herstellt. Mobile Endgeräte kommunizieren entweder mit einem Access Point oder direkt miteinander. Im letzteren Fall spricht man auch von einem so genannten Ad-hoc-Netzwerk. Ein Access Point versorgt eine Funkzelle, in der 802.11-Terminologie als Basic Service Set (BSS) bezeichnet. Die Reichweite eines Access Points zur Versorgung einer WLAN-Zelle liegt typischerweise in Gebäuden im Bereich von 10 m bis 100 m (unter Idealbedingungen). Der tatsächliche Empfangsbereich hängt von den verwendeten Antennen, der Sendeleistung und den konkreten baulichen Gegebenheiten ab. Mit speziellen Richtantennen können Punkt-zu-Punkt bei Sichtverbindung mit WLAN auch wesentlich höhere Distanzen (mehrere km) zwischen Gebäuden überbrückt und so zwei LAN-Segmente über Wireless Bridges gekoppelt werden.

Um ein flächendeckendes WLAN aufzubauen, wird das Versorgungsgebiet mit sich typischerweise überlappenden Zellen abgedeckt. Zusammengenommen bilden diese Zellen das so genannte Extended Service Set (ESS). Zur Kommunikation mit der Infrastruktur ist das ESS an ein drahtgebundenes LAN gekoppelt, das Distribution System (DS), das seinerseits mit der weiteren Netzinfrastruktur verbunden ist (siehe Bild 1). Das ESS und DS bilden ein flaches Layer-2-Netz.

WLAN ermöglichen eine Mobilität auf Layer 1 und 2. Das Endgerät kann sich innerhalb einer Funkzelle bewegen. Eine geeignete Kodierung auf Layer 1 und Automatic-Repeat-Request (ARQ)-Mechanismen auf Layer 2 können bis zu einem gewissen Umfang die Schwankungen in der Empfangsqualität ausgleichen. Ein WLAN-Client kann sich aber auch innerhalb eines ESS von einer Zelle in eine andere bewegen, ohne dass dabei eine Kommunikationsbeziehung auf höheren Protokollebenen abbricht. Diese Übergabe von einem Access Point zum anderen heißt BSS-Transition. Allgemein wird im Mobilfunk für diesen Vorgang die Bezeichung Handover verwendet.

Sicherheit in Wireless LAN: Eine endlose Geschichte?

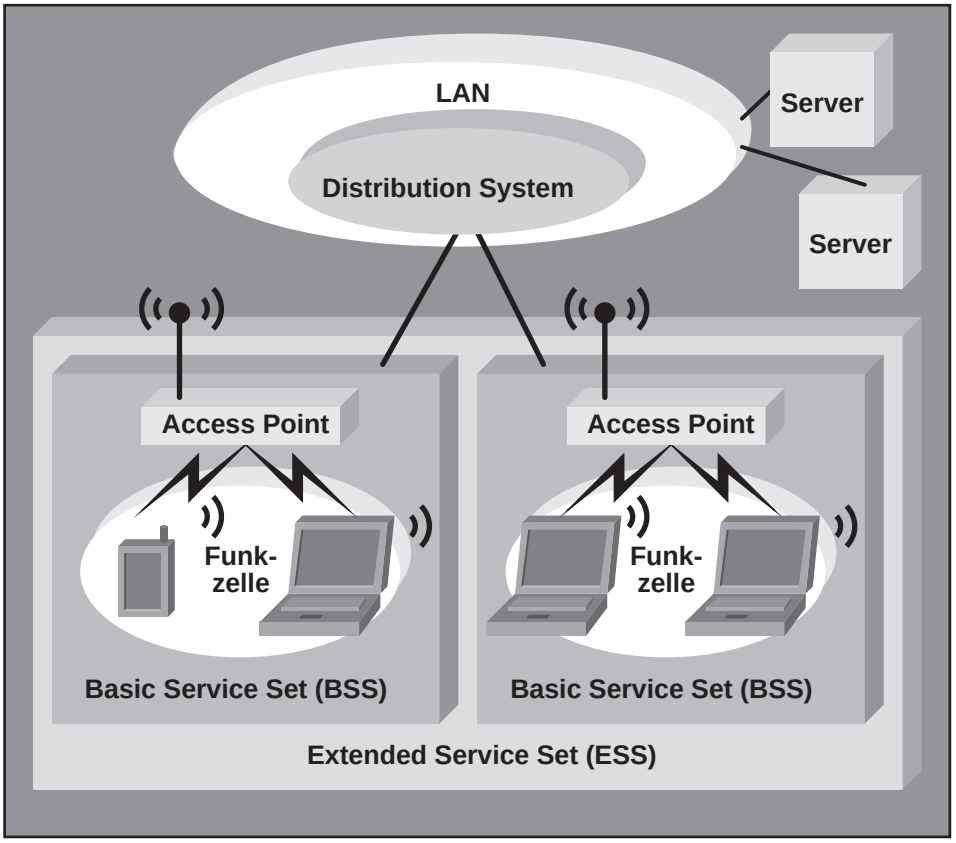


Bild 1 WLAN-Aufbau

Wie die anderen IEEE-Standards für Lokale Netze definiert 802.11 lediglich die Protokolle zur physikalischen Übertragung und zum Kanalzugriff sowie das Netzmanagement für diese Protokollebenen.

802.11 spezifiziert fünf Varianten zur physikalischen Übertragung und ein gemeinsames Verfahren für den Kanalzugriff, siehe [3], [4], [5]. Neben der Übertragung mit Infrarot sind im Industrial-Scientific-Medical-Frequenzband (kurz: ISM) bei 2,4 GHz zwei Verfahren festgelegt worden: Direct Sequence Spread Spectrum (DSSS) und Frequency Hopping Spread Spectrum. 802.11 erlaubt dabei Datenraten von 1 Mbit/s oder 2 Mbit/s. DSSS wurde in Ergänzung 802.11b zur Übertragung höherer Datenraten bis maximal 11 Mbit/s erweitert und hat sich inzwischen als Marktführer im WLAN-Bereich etabliert. Datenraten bis zu 54 Mbit/s bietet 802.11a im 5-GHz-Bereich (5150 - 5350 MHz und 5470 - 5725 MHz). Erste Produkte für 802.11a sind seit einigen Monaten verfügbar, jedoch noch nicht für den Betrieb in Deutschland zugelassen. Auch das ISM-Band bei 2,4 GHz ist noch nicht ausgereizt: Eine weitere Erweiterung der Datenrate (ebenfalls bis 54 Mbit/s) bei 2,4 GHz ist als 802.11g bereits in Arbeit. Mit Vorstandardprodukten wird noch dieses Jahr gerechnet. Die Verabschiedung des Standards wird jedoch höchstwahrscheinlich erst 2003 stattfinden.

Der Kanalzugriff (Medium Access Control, MAC) geschieht für alle spezifizierten Übertragungstechniken einheitlich über Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Dies ist ein Best-Effort-Verfahren, welches das Medium zufallsgesteuert (also ohne Bandbreitengarantien) auf die drahtlosen Clients aufteilt. Netto bleiben nach Abzug des Protokoll-Overheads für MAC und physikalische Übertragung beispielsweise für 802.11b maximal etwa 6 Mbit/s übrig.

2. Sicherheitsmechanismen in 802.11 oder Sicherheit, die keine ist

Wie bereits erwähnt, ist Funk immer ein Shared Medium und neben der Regelung des Kanalzugriffs müssen Sicherheitsmechanismen implementiert werden, wenn die Sicherheitsziele Vertraulichkeit, Zugangskontrolle, Datenintegrität erreicht werden sollen. In 802.11 wird hierzu das als Wired Equivalent Privacy (WEP) bezeichnete Verfahren spezifiziert, das zur Verschlüsselung und Authentisierung eingesetzt wird.

WEP benutzt RC4, ein symmetrisches Verschlüsselungsverfahren, das zu den so genannten Stromchiffrierern gehört. Mit einem Startwert (Seed) wird dabei ein Pseudozufallszahlengenerator initialisiert. Für jedes zu übertragende Byte einer Nachricht wird eine neue Zufallszahl gewürfelt. Das verschlüsselte Byte ergibt sich einfach durch eine XOR-Verknüpfung mit der Zufallszahl. Die Entschlüsselung funktioniert analog: Der Empfänger benutzt denselben Startwert wie der Sender für die Initialisierung des Zufallszahlengenerators. Für jedes empfangene Byte der Nachricht würfelt der Empfänger eine neue Zahl, führt eine XOR-Verknüpfung mit dem verschlüsselten Byte durch und erhält den Klartext, siehe Bild 2. Der gemeinsame Startwert wird dabei aus einem geheimen Schlüssel berechnet, der bei Sender und Empfänger vorliegen muss.

Nehmen wir jetzt an, ein Angreifer kann die verschlüsselte Übertragung zwar belauschen, kennt jedoch den verwendeten Startwert nicht. Solange der Zufallszahlengenerator im statistischen Sinne eine genügend gute Qualität hat, sorgt die XOR-Verknüpfung dafür, dass die übertragenen Daten im Wesentlichen den Informationsgehalt eines Rauschens haben und ein Angreifer daraus nicht ohne Weiteres auf den ursprünglichen Inhalt rückschließen kann.

Spannend wird es, wenn bei einer späteren Übertragung noch einmal der gleiche Startwert verwendet wird. Nehmen wir an, der Angreifer hätte dies herausbekommen und beide verschlüsselten Nachrichten C und C' aufgezeichnet. Zur Verschlüsselung der Klartexte P und P' wurde RC4 mit demselben Startwert initialisiert. In Konsequenz hat RC4 beide Male eine identische Folge B von Zufallszahlen (Schlüsselstrom) geliefert. Übertragen wurde also einmal $C = P \oplus B$ und das andere mal $C' = P' \oplus B$. Der Angreifer rechnet nun ganz einfach $C \oplus C' = (P \oplus B) \oplus (P' \oplus B) = (P \oplus P') \oplus (B \oplus B) = P \oplus P'$ und hat fast gewonnen, denn jetzt weiß der Angreifer schon, dass er die XOR-Verknüpfung zweier Klartexte in Händen hält. Er kennt zwar die beiden Klartexte nicht unmittelbar, oft genug reicht aber bereits dieses Wissen, um die Klartexte mit statistischen Mitteln zu rekonstruieren. Können Teile des einen Klartextes von C "geraten" werden, hat man automatisch den entsprechenden anderen Teil des Klartextes von C'. Dies fällt umso leichter, je öfter derselbe Schlüsselstrom verwendet wird.

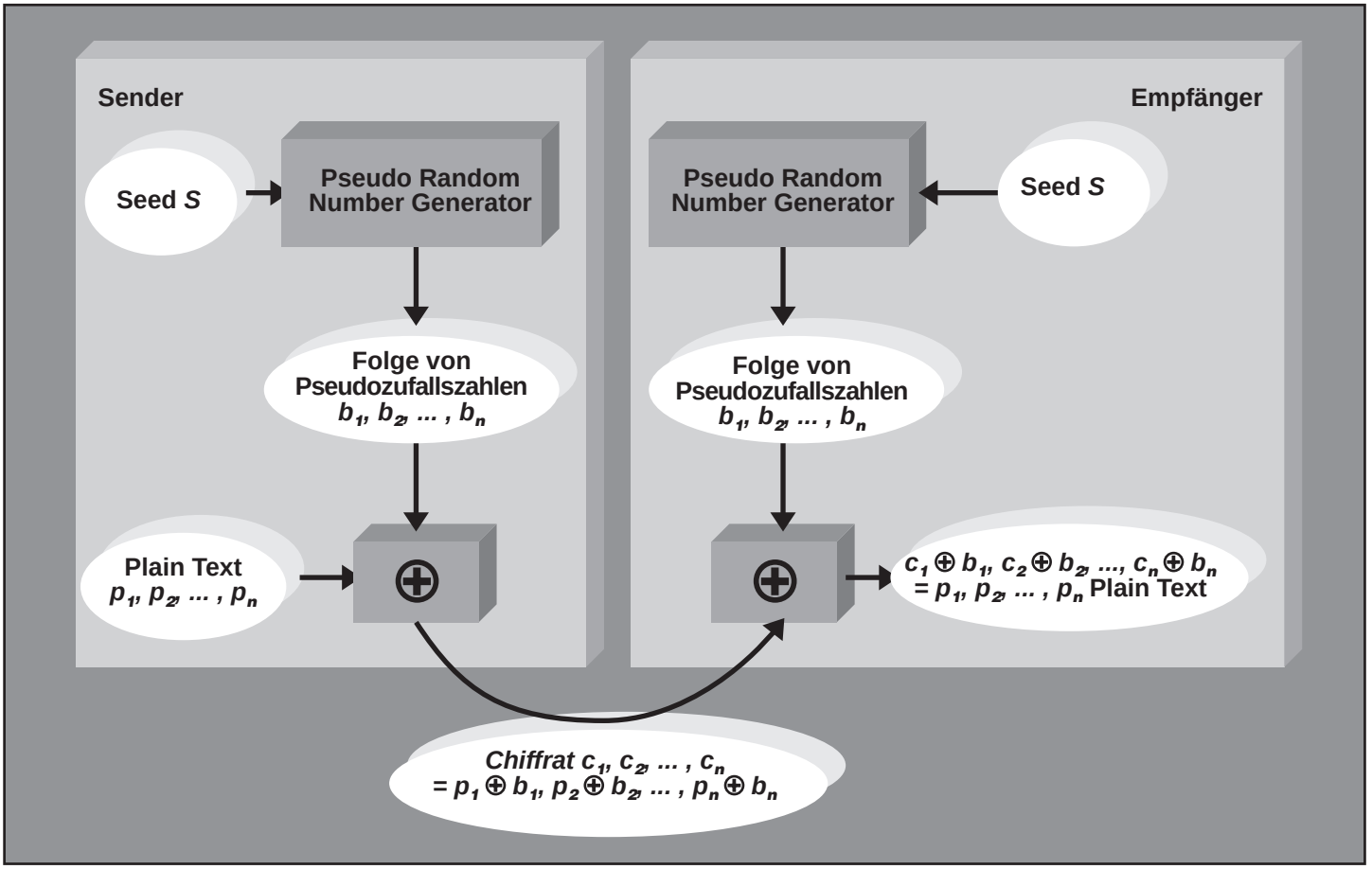
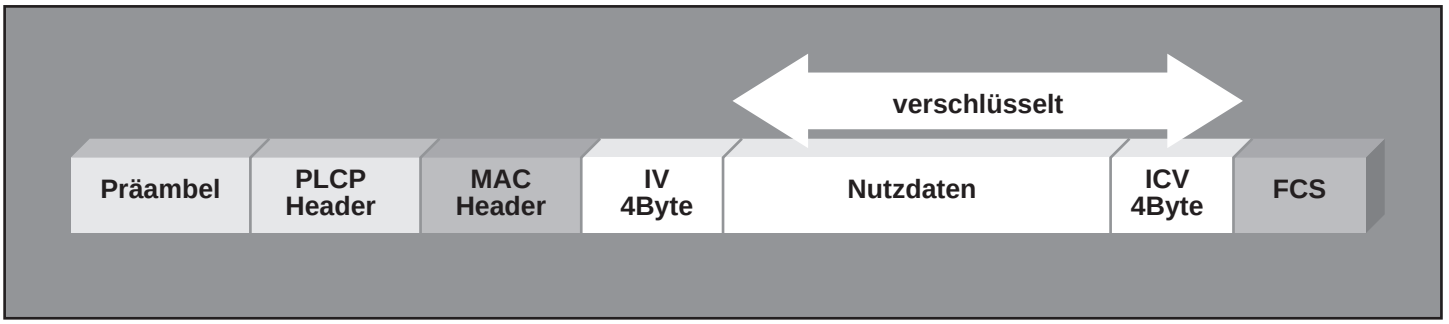


Bild 2 Verschlüsselung mit Zufallszahlen

Die Grundregel bei der Verwendung von RC4 (und allen anderen verwandten Verfahren) lautet daher, "niemals" denselben Schlüsselstrom mehrfach zu verwenden. Das heißt insbesondere, dass der Startwert, der zur Initialisierung benutzt wird, erst nach einer möglichst langen Zeit wiederverwendet wird. Die Kunst bei der Benutzung von RC4 liegt also in der geschickten Konstruktion des Startwerts aus einem geheimen Schlüssel.

Übertragen wir nun diese Situation auf WEP. Die Operationen von WEP sind einfach beschrieben: Es sind zwei Schlüssellängen spezifiziert: 40 Bit und 104 Bit. Über die Art und Weise, wie diese Schlüssel auf Access Points und Clients verteilt werden und, wie sich die Kommunikationspartner auf einen gemeinsamen geheimen Schlüssel einigen, sagt der Standard nichts aus. WEP beginnt mit der Annahme, dass jeder Teilnehmer in einem BSS mit einem gemeinsamen Schlüssel (in der Praxis von Hand) konfiguriert ist. Die Verschlüsselung erfolgt pro Paket, und zwar wird die MAC-Nutzlast zusammen mit einem CRC-Feld zur Integritätsprüfung (Integrity Check Value, ICV) mit RC4 verschlüsselt. Damit von Paket zu Paket nicht derselbe Initialisierungswert für RC4 verwendet wird, gibt es zusätzlich einen 24 Bit langen Initialisierungsvektor (IV). Schlüssel und IV zusammen bilden den RC4-Initialisierungswert für das zu übertragende Paket. Damit der Empfänger auch weiß, welcher Wert für den IV zu benutzen ist, wird der IV im Klartext einfach im Header des MAC-Pakets mit übertragen (siehe Bild 3)!

Bild 3 MAC-Frame-Format bei Verwendung von WEP



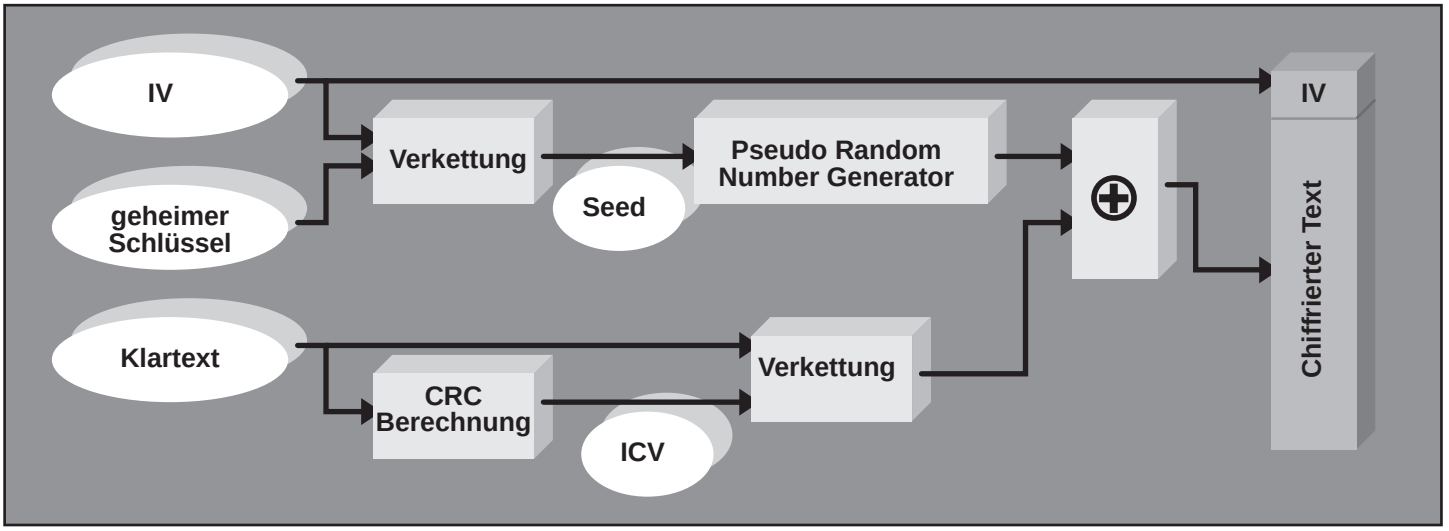


Bild 4 Verschlüsselung mit WEP

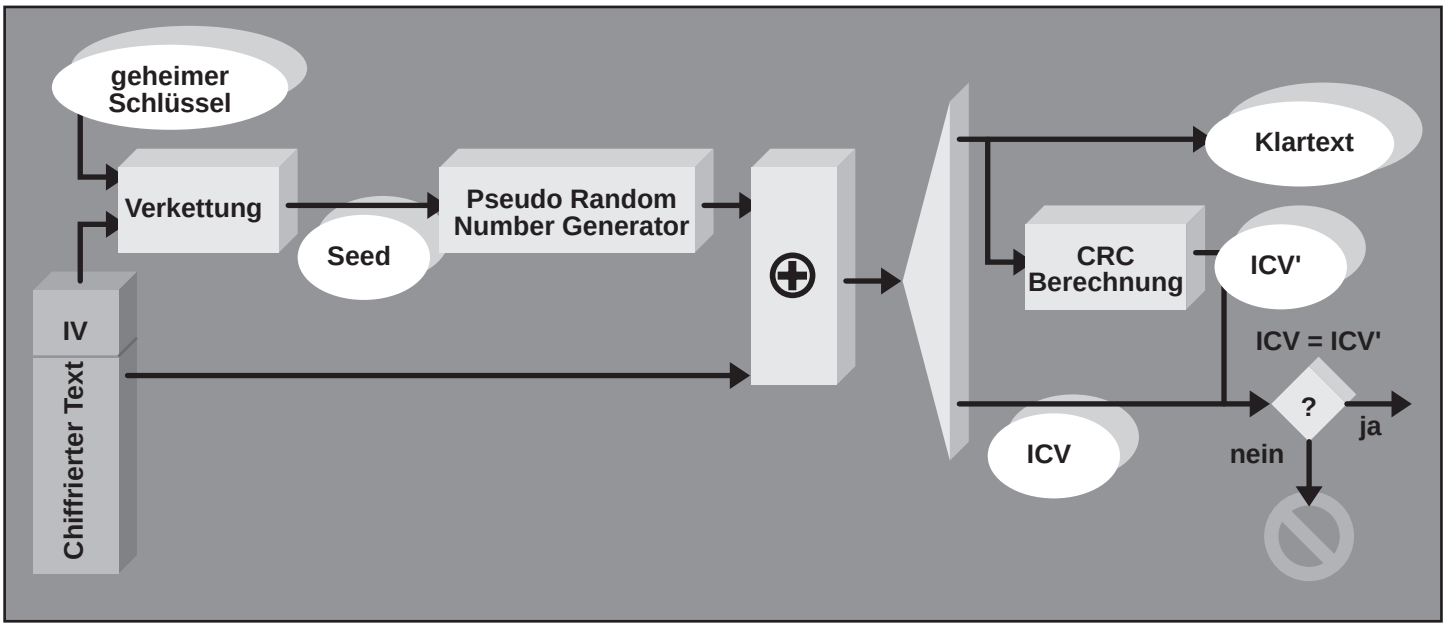
Für das nächste zu übertragende Paket wiederholt sich das Verfahren mit einem neu gewählten Wert für den IV. Bild 4 und Bild 5 zeigen schematisch den Aufbau für Ver- und Entschlüsselung.

Die Verwendung eines IV mit einer Länge von 24 Bit bedeutet, dass ein Pool von 2^{24} (also etwa 16 Millionen) verschiedenen Initialisierungswerten für RC4 vorliegt. Spätestens danach wiederholt sich erstmalig ein IV, was bei einer Rate von 11 Mb/s und einem genügend ausgelasteten Access Point nach einigen Stunden der Fall wäre. Für das dann gesendete Paket wird ein bereits benutzter Schlüsselstrom wieder verwendet. Eigentlich müsste jetzt ein neuer geheimer Schlüssel (40 Bit oder 104 Bit) zwischen den Kommunikationspartnern im BSS (also zwischen Clients und Access Point) vereinbart werden. Dazu sagt der Standard allerdings nichts. Des Weiteren macht der Standard keine Aussage darüber, wie die IVs zu erzeugen sind. Einige Hersteller machen es sich daher einfach und setzen in ihren WLAN-Adapter den IV bei ihrer Initialisierung auf 0 und inkrementieren paketweise um 1. Im Regelfall kommt es dann bereits sehr früh zu einer Wiederholung des IV, und der Entschlüsselung durch den Angreifer, wie oben beschrieben, steht nichts mehr im Wege.

Normalerweise hätten diese simplen Überlegungen schon ausgereicht, um jegliches Vertrauen in IEEE 802.11 zu verlieren.

Es kam jedoch noch schlimmer: Bedingt durch die charakteristischen Eigenschaften von RC4 und der Tatsache, dass zur Verschlüsselung der IV einfach an den Schlüssel angehängt wird und anschließend im Klartext übertragen wird, kann sogar der geheime Schlüssel ermittelt werden. Das ist zwar mathematisch nicht so trivial wie die obigen Überlegungen (siehe [10]), funktioniert in der Praxis jedoch blendend, wie man sich am Beispiel des Tools airsnort überzeugen kann [7].

Bild 5 Entschlüsselung mit WEP



Ist der Schlüssel einmal bekannt, sind alle Tore offen. Man nehme einen Protokollanalysator für WLAN – etwa das kostenlose Ethereal [8] – und jeglicher Verkehr kann im Klartext aufgezeichnet werden. Das ist nur ein kleiner Auszug der bisher bekannten Angriffe, die durch die Schwäche von WEP ermöglicht werden. Als weitere Beispiele seien nur die Möglichkeit sich am Access Point auch ohne Kenntnis des geheimen Schlüssels zu authentifizieren und die Möglichkeit, unter Ausnutzung einer Schwäche der CRC-Kodierung für den ICV, Pakete "beliebig" zu fälschen, ohne dass der CRC dies bemerkt, genannt (siehe auch [9]).

Kurz, es war ein Desaster und ein immenser Gesichtsverlust für die IEEE, der sich vor etwas mehr als einem Jahr abgespielt hat.

3. Die Qual der Wahl in 802.11i: Abwärtskompatibel mit gestopften Löchern oder in neuen Hosen gehen

Unter der Bezeichnung "MAC Enhancements for Enhanced Security" arbeitet die Arbeitsgruppe TGi an einer neuen Sicherheitslösung für WLAN, siehe [11]. Der Standardentwurf 802.11i nimmt langsam stabile Züge an. Optimisten rechnen zwar mit einer Verabschiedung noch dieses Jahr, aktuell sollte man trotzdem noch eher von 2003 ausgehen.

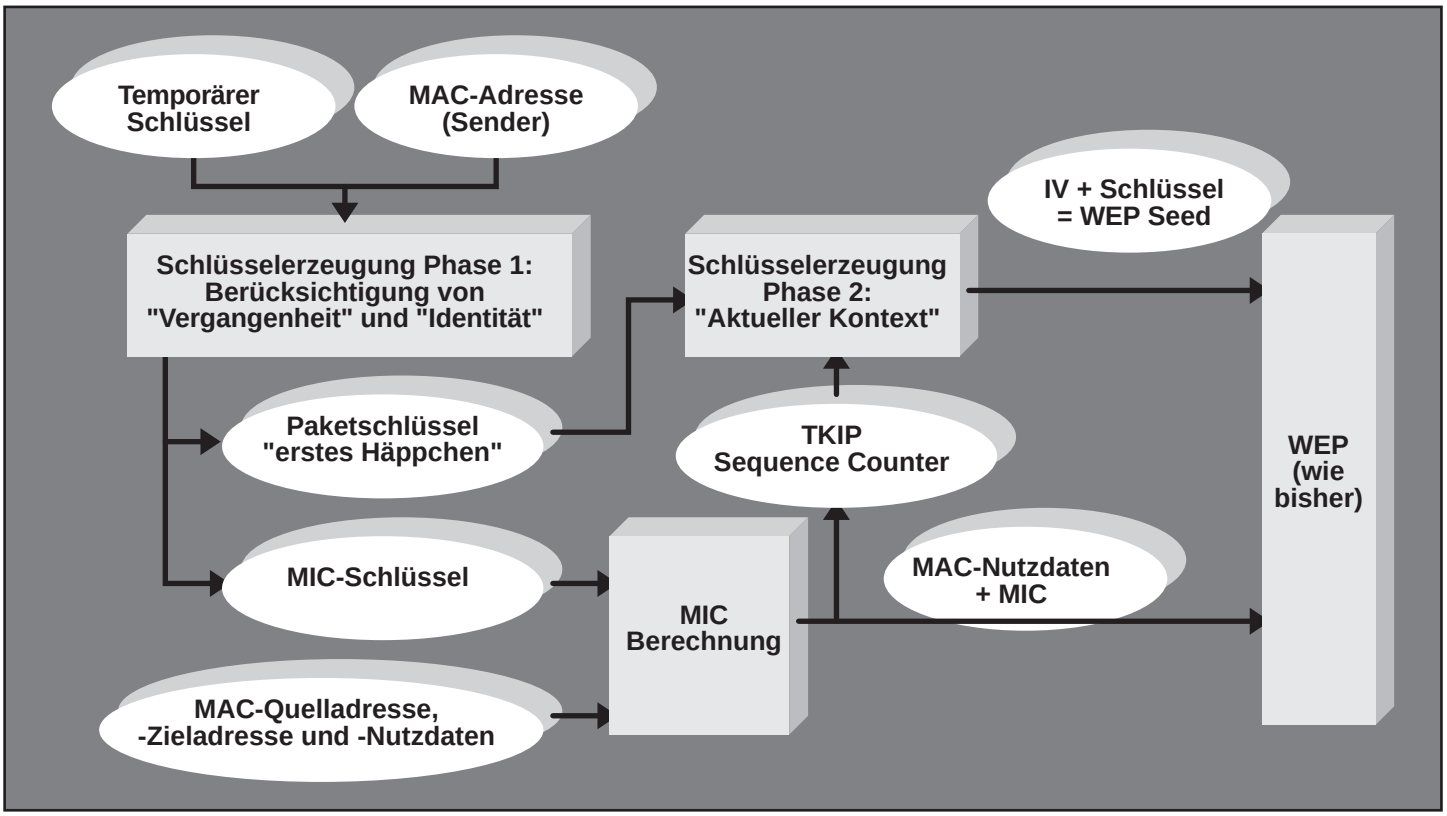
Folgende Anforderungen standen bei der Arbeit im Vordergrund:

- Pakete müssen authentifiziert und nicht nur verschlüsselt werden.
- Ein Schlüssel wird nur für ein Paket benutzt.
- Pakete müssen eine verschlüsselte Sequenznummer tragen.
- Kommunikationspartner müssen sich gegenseitig authentifizieren.

Ein Kernproblem der verbesserten Sicherheitslösung war die Abwärtskompatibilität. Soll es möglich sein, ein bestehendes WLAN-System gemäß des aktuell noch gültigen Standards nachträglich mit dem neuen Standard aufzurüsten, darf höchstens ein Update der Firmware erfolgen. Die Konsequenz wäre in diesem Fall, dass es bei RC4 bleibt. Es mussten also zwei Verschlüsselungsverfahren festgelegt werden: Eines, das als temporäre Lösung nach wie vor auf WEP basiert, jedoch die gröbsten Schwächen beseitigt und eines, das zwar neue Hardware erfordert, aber langfristig tragbar ist.

Betrachten wir zunächst die abwärtskompatible Lösung, das Temporary Key Integrity Protocol (TKIP). Eines ist klar: Es ist nur möglich, im Rahmen der Festlegungen von WEP, die nicht in Hardware gegossen wurden, die bislang erkannten Schwächen bei Auswahl und Erzeugung der Startwerte für RC4 möglichst gut zu umschiffen. Wesentliche Elemente in TKIP sind: Pro Paket wird ein neuer Schlüssel durch Anwendung einer Hash-Funktion auf dem geheimen symmetrischen Schlüssel, dem IV und einer Paketsequenznummer erzeugt, um das Problem des bisher statischen WEP-Schlüssels zu umgehen. Ein zusätzlicher Message Integrity Check (MIC), der neben den Nutzdaten auch die Quell- und Zieladressen des MAC-Pakets berücksichtigt und verschlüsselt übertragen wird, authentifiziert das Paket (siehe Bild 6). Die Entschlüsselung funktioniert prinzipiell ähnlich unter Umkehrung der Operationsrichtungen.

Bild 6 Verschlüsselung mit TKIP (vereinfacht und unter Vorbehalt)

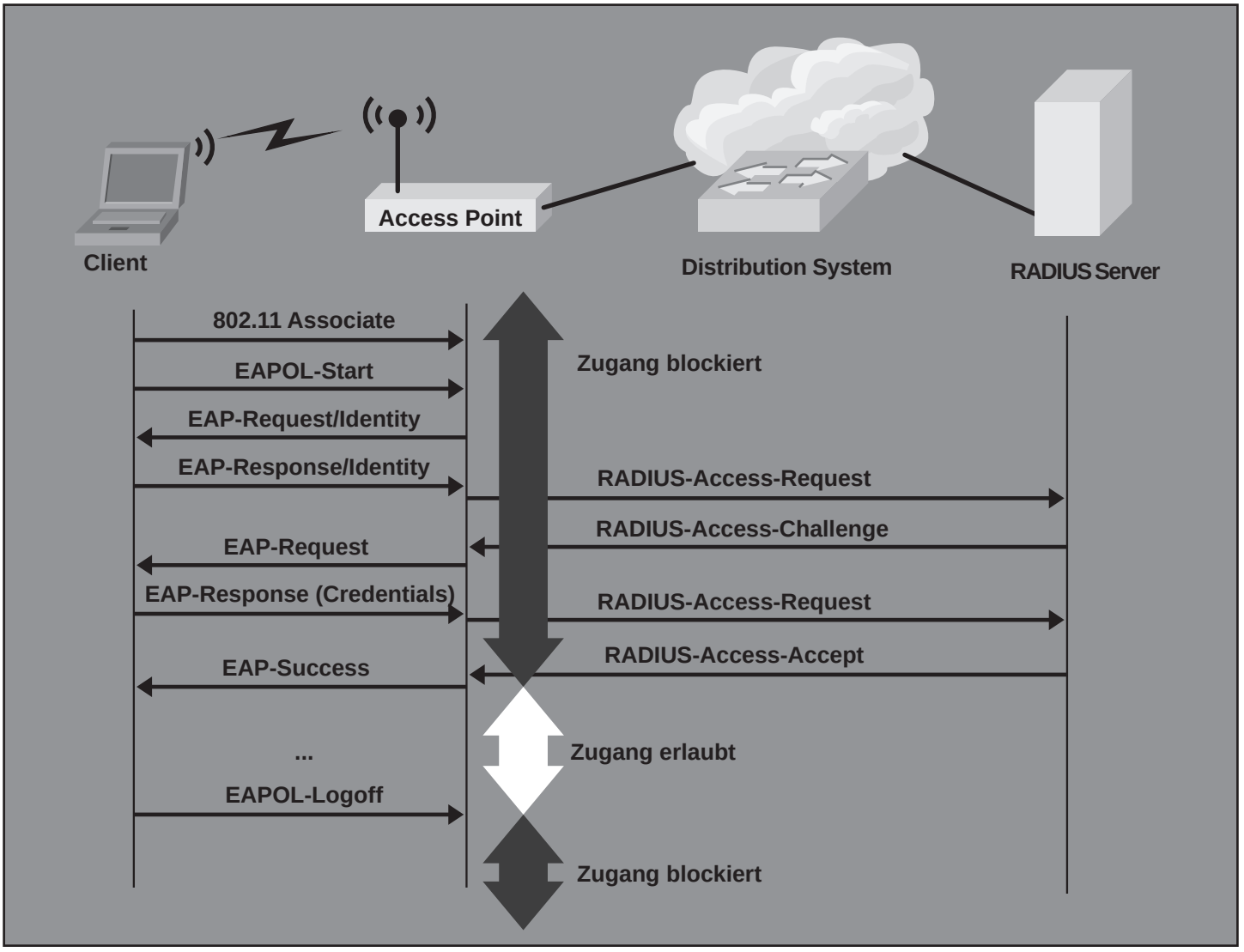


Außerdem ist ein Mechanismus festgelegt, der dafür sorgt, dass ein neuer Schlüssel bereitgestellt werden kann, um eine Wiederholung des Initialisierungswertes für RC4 zu vermeiden. Für diese Schlüsselverwaltung und -verteilung greift 802.11i auf einen anderen Standard zurück und zwar auf IEEE 802.1x [12]. Dieser Standard ist zur portbasierten Netzwerkzugangskontrolle für kabelbasierte Netze entworfen worden. Grundsätzliche Idee in 802.1x ist, dass die Freischaltung eines Netzwerkports erst dann erfolgt, wenn der Nutzer sich erfolgreich dem Netz gegenüber authentifiziert hat. Die Authentisierung erfolgt also auf Schicht 2. Damit so etwas überhaupt funktioniert, muss 802.1x eine Schnittstelle zwischen Client, Netzelement und einem Authentisierungssystem spezifizieren. Hand in Hand geht damit die Festlegung einer Funktion zur Schlüsselverwaltung und -verteilung, also genau die fehlende Funktion zur Auffrischung des symmetrischen Schlüssels für RC4.

Der nächste Schritt ist nur konsequent: In 802.11i wird für die Authentifizierung von Client und Access Point auf die Authentifizierung gemäß 802.1x verwiesen, welche damit die bisherige Authentifizierung in 802.11 ersetzt. Eigentlich ein eleganter Schachzug: Die Frage der Authentifizierung für den WLAN-Zugang wird von der Standardisierung der WLAN-Übertragung entkoppelt. Für Übertragung, siehe 802.11, für Authentifizierung siehe 802.1x. Unangenehm ist nur, dass 802.1x seinerseits nichts anderes als eine Schnittstelle zu einem Authentisierungssystem darstellt. 802.1x nutzt hierzu das Extensible Authentication Protocol (EAP). Als Authentifizierungs-Instanz dient ein RADIUS-Server. Bild 7 zeigt das Grundprinzip der Authentifizierung.

Bis auf die unschöne Lösung zur Verschlüsselung (WEP bleibt WEP), auf die wir gleich noch eingehen, wären wir eigentlich fertig. Wäre da nicht das Problem des leicht zugänglichen Shared Mediums in WLAN. Hier sind nun einmal Attacken möglich, die in kabelbasierten geswitchten Netzen keine besondere Rolle mehr spielen. Eine Untersuchung der University of Maryland hat kürzlich die Angriffsmöglichkeiten auf eine Implementierung von 802.1x unter Verwendung von EAP-MD5 als Authentifizierungsmechanismus aufgezeigt (siehe [16]). Dieser Veröffentlichung wurden zwar einige Schwächen vorgehalten, sie macht jedoch deutlich, dass die Auswahl des Authentifizierungsmittels mit Vorsicht zu genießen und diese Debatte noch nicht abgeschlossen ist.

Bild 7 Authentisierung eines WLAN-Client über 802.1x und EAP



Der aktuelle Trend in 802.11i geht dahin, dass der Standard kein spezielles Authentifizierungsverfahren und Schlüsselverteilungsverfahren als zwingend vorschreiben wird. Wer legt nun das Authentifizierungsverfahren fest? Der Betreiber des WLAN? Selbst bei firmeninternen WLAN ist dies nicht einfach. Man denke nur an das Problem unternehmensweiter einheitlicher Sicherheitsrichtlinien in global operierenden Unternehmen. Noch unangenehmer wird es für öffentliche Hotspots, die schließlich davon leben, dass einem jeden Kunden ein möglichst unproblematischer Netzzugang ermöglicht wird. Es bleibt jedoch abzuwarten, was in dem endgültig verabschiedeten Standard festgelegt wird.

TKIP wird als eine temporäre Lösung verstanden. Als langfristige Lösung sieht 802.11i den Einsatz des Advanced Encyption Standard (AES) in einem speziellen Modus vor, dem Offset Codebook (OCB). Genauer gesagt wird AES von OCB verwendet. Mit OCB werden alle oben genannten Anforderungen an ein Verschlüsselungsverfahren für WLAN erfüllt, insbesondere die Anforderung der Datenintegrität und -authentizität. Zur Schlüsselverwaltung und -verteilung für OCB setzt 802.11i wieder 802.1x voraus.

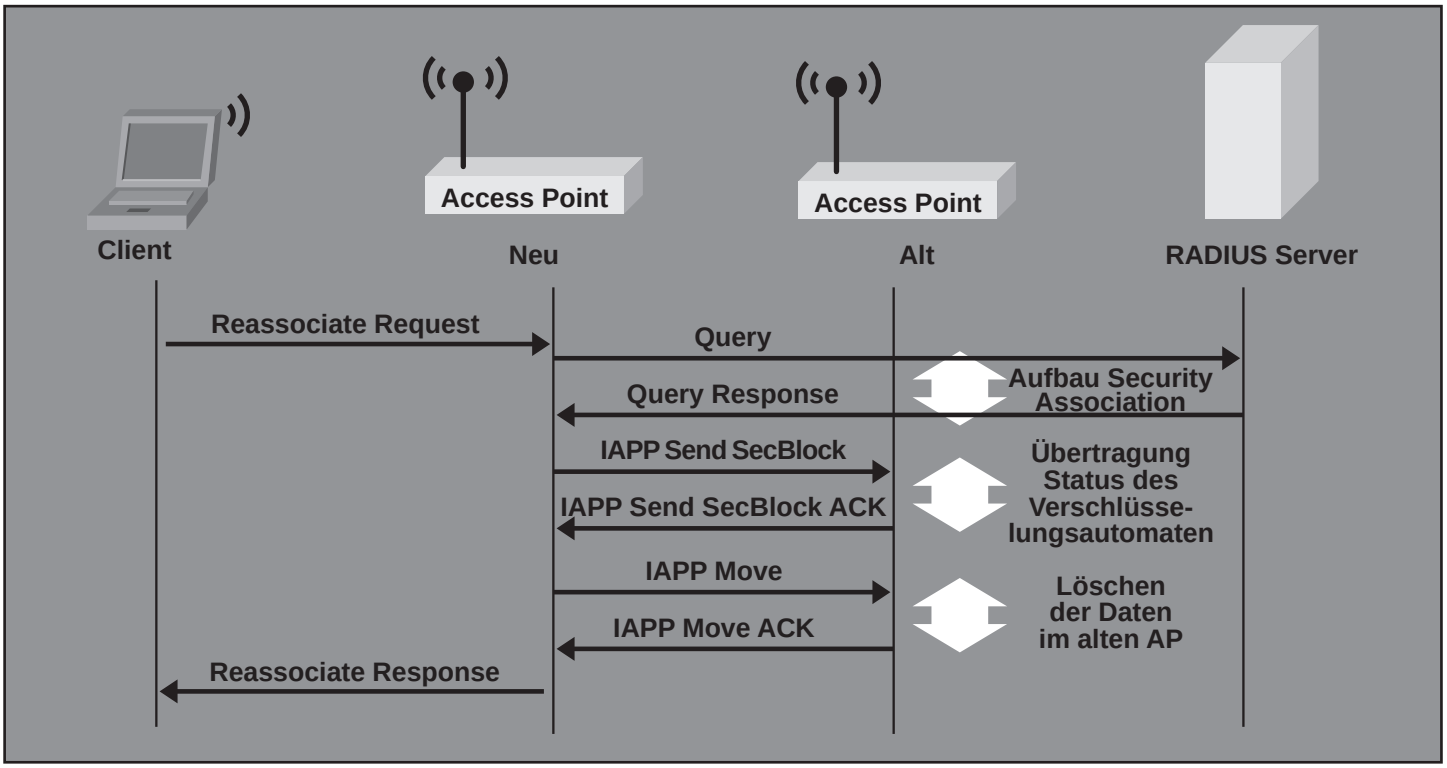
AES ist der offizielle Nachfolger des DES und basiert auf einer Ausschreibung, die das National Institute of Standards and Technology (NIST) im Zeitraum 1997 bis 2001 durchgeführt hat. Letztlich musste aus einer großen Menge eingereichter Algorithmen ein Kandidat für den neuen Standard ausgewählt werden. Folgende Anforderungen waren zu erfüllen:

- Es musste sich um einen symmetrischen Blockchiffrier-Algorithmus mit einer Blocklänge von mindestens 128 Bit handeln.
- Schlüssellängen von 128, 192 und 256 Bit mussten unterstützt werden.
- Der Algorithmus musste eine effiziente Implementierung sowohl in Hardware als auch in Software zulassen und durfte dabei nicht zu viele Ressourcen beanspruchen (Hintergrund dieser Anforderung war, dass der Algorithmus auch in Systemen mit sehr eingeschränkten Ressourcen einsetzbar sein sollte, z.B. Smart-Cards).
- Der Algorithmus sollte resistent gegen alle bis dato bekannten Verfahren der Kryptoanalyse sein, dies betraf neben der schon als klassisch zu betrachtenden differentiellen und linearen Kryptoanalyse auch neuere Methoden wie z.B. Power- oder Timing-Attacken.
- Der Algorithmus musste frei sein von jeglichen patentrechtlichen Ansprüchen.

Die Wahl fiel schließlich auf den Rijndael-Algorithmus der Belgier Joan Daemen und Vincent Rijmen, nicht zuletzt wegen seiner Effizienz und seines geringen Ressourcenbedarfs. Für weitere Informationen sei auf die Originalarbeit verwiesen [13].

Egal ob mit TKIP oder AES/OCB gearbeitet wird, durch die Einführung von verschlüsselten Sequenznummern wird eine kryptographische Session zwischen Client und Access Point etabliert. Das hat natürlich Auswirkungen auf die Mobilität. Was passiert, wenn sich ein Client von einer Funkzelle (einem BSS) in eine andere Zelle bewegt? Im aktuellen 802.11-Standard würde einfach eine neue Assoziation und WEP-Authentifizierung am neuen Access Point durchgeführt. Das geht in der Regel schnell genug, ohne dass höhere Protokolle etwas davon spüren und ohne dass eine Kommunikation zwischen den Access Points erforderlich ist. Mit 802.11i ist der Aufwand ungleich höher und es ist naheliegend, eine Session von einem Access Point zum nächsten mitzunehmen (Bild 8). Das erfordert natürlich ein Protokoll zwischen den Access Points und damit ein Handover zwischen Funkzellen, wie es im Prinzip ähnlich in Mobilfunknetzen wie GSM abläuft. Um ein Mehr an Intelligenz im Access Point kommt 802.11 sowieso nicht herum; man denke nur an Quality of Service.

Bild 8 Schneller Handover zwischen 802.11i-Access-Points



Die Erweiterung 802.11i wird natürlich auch Auswirkungen auf die Interoperabilität mit Geräten nach dem aktuellen Standard haben. Ein Access Point nach 802.11i darf durchaus gleichzeitig mit Geräten nach dem aktuellen Standard und mit Geräten nach 802.11i kommunizieren. Für Clients ist das nicht der Fall. Hier gilt entweder 802.11i oder die aktuelle Weise, jedoch nicht beides gleichzeitig. Zusätzlich wird ein Mechanismus in 802.11i enthalten sein, der eine Client-Konfiguration vorsieht, die ausschließlich die erweiterten Sicherheitsmechanismen erlaubt und die Kommunikation mit einem Access Point nach dem aktuellen Standard explizit verbietet. Dies erlaubt einerseits die sanfte Migration zu den erweiterten bzw. neuen Sicherheitsmechanismen und andererseits die Umsetzung strenger Sicherheitspolitiken.

Um ein erstes Fazit zu ziehen: Die Welt ist mit 802.11i alles andere als einfacher geworden. Die Komplexität eines sicheren WLAN und damit der Aufwand für Planung, Aufbau und Betrieb werden deutlich über dem der WLAN nach der aktuellen Version von IEEE 802.11 liegen. Allerdings hat gerade die Einfachheit eines WLAN in der Vergangenheit einen nicht unerheblichen Anteil am Erfolg der Technik gehabt, trotz seiner Unsicherheit.

4. Warum nicht gleich IP-VPN für private WLAN?

Auch wenn 802.11i zunächst mit TKIP an den Start gehen wird, nach dem aktuellen Stand der Technik bietet 802.11i ein durchaus akzeptables Sicherheitsniveau. Gegen gewisse Attacken kann sich jedoch ein WLAN nie wehren. Denial of Service ist in Funknetzen immer mit erstaunlich geringem Aufwand möglich. In einem unlizensierten Frequenzband, in dem sich mehrere Systeme ungeregelt tummeln, wie dem ISM Band bei 2,4 GHz, in dem auch 802.11b operiert, muss mit Störungen gerechnet werden. Von Gesetzgeber oder Regulierungsbehörde wird hier nur in gewissen Einzelfällen eine Unterstützung zu erwarten sein.

Warum also dieser Aufwand mit 802.11i? Warum nicht konsequent jegliche Sicherheitsmechanismen aus 802.11 streichen, das WLAN als reines Übertragungsmedium, wie Ethernet oder Token Ring betrachten und sich vollständig auf die Aufgabe konzentrieren, die Übertragung auf dem Medium Funk zu optimieren? Das WLAN würde damit automatisch als un-sicherer Bereich zu klassifizieren sein. Ob der Zugriff auf interne Ressourcen über ein WLAN erfolgt oder über das Internet, würde keinen Unterschied machen: Mit den Mitteln eines IP-VPN mit IPSec würde die Übertragung gesichert (Bild 9). Der grundsätzliche Aufbau ist vergleichsweise einfach, die Protokolle standardisiert, die Technik ist in der Praxis bewährt und es gibt genügend Produkte auf dem Markt. Im einfachsten Fall wird die IP-VPN Lösung, die man beispielsweise bereits zur Anbindung von mobilen Mitarbeitern einsetzt, für die Absicherung des WLAN noch einmal verwendet.

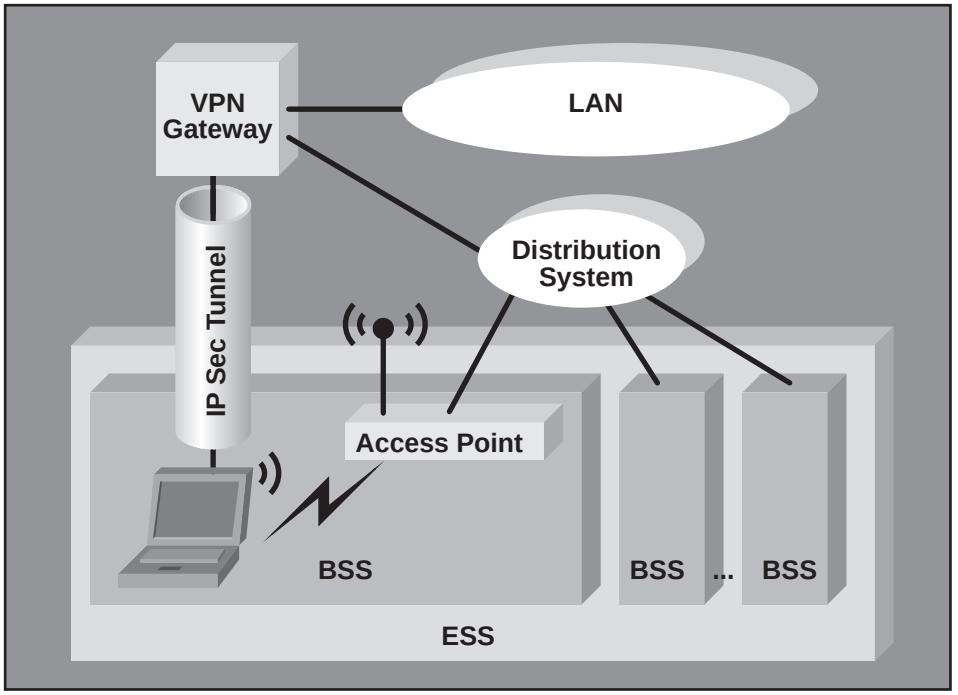


Bild 9 Absicherung des WLAN mit einem VPN

Dies ist tatsächlich zur Zeit die einzige Alternative, ein sicheres WLAN aufzubauen, will man nicht auf herstellerspezifische WLAN-Erweiterungen zurückgreifen. Und mit einem gewissen Abstand betrachtet, hat man mit 802.11i dieselbe Komplexität erreicht, die ein IP-VPN zum Schutz des WLAN benötigt.

Jedoch hat auch ein IP-VPN mit IPSec seine Tücken. IPSec sieht lediglich eine gegenseitige Authentifizierung der Kommunikationspartner auf Systemebene vor; die Identität des Benutzers wird nicht geprüft. Hier sind verschiedene Ansätze zur Lösung des Problems denkbar und zum Teil durch Hersteller von VPN-Produkten realisiert worden, allerdings werden hierdurch mangels Standard erneut Inkompatibilitäten geschaffen. Das aktuelle Lösungsspektrum reicht von der SmartCard-basierten Kopplung der Systemidentifikation an den Benutzer über Erweiterungen des Internet-Key-Exchange-Protokolls (IKE), Verwendung ineinander geschachtelter Tunnelmechanismen bis zur nachgelagerten Authentifizierung jenseits des VPN-Tunnels, z.B. an einer Firewall, wobei alle Ansätze sowohl Vor- als auch Nachteile aufweisen.

Die Verwendung eines IP-VPN wurde auch in 802.11i diskutiert und zugunsten der bereits vorgestellten Erweiterung verworfen. Als wesentliche Gründe wurden genannt, dass eine Authentisierung auf Schicht 2 schneller, einfacher und preiswerter sei und der Client keinen Zugang auf Netzwerkebene benötigt, um sich zu authentifizieren. Trotzdem ist das Authentifizierungsproblem auch in 802.11i nicht gelöst, die Verantwortung wurde einfach nach Außen geschoben.

Unabhängig davon, welche Mechanismen zur Absicherung eines WLAN eingesetzt werden, gilt: Der WLAN-Einsatz muss in der Sicherheitspolitik besonders berücksichtigt werden und ein umfassendes Sicherheitskonzept muss erarbeitet werden. Das WLAN darf dabei nicht isoliert vom Rest der IT-Infrastruktur betrachtet werden, denn gerade im ganzheitlichen Ansatz liegt die Basis für effektive und effiziente Sicherheit. Die gewissenhafte Planung und Konfiguration der Sicherheitseinstellungen, deren regelmäßige Überprüfung und die Überwachung des Kommunikationsverkehrs hinsichtlich möglicher Angriffe sind obligatorisch. Einmal mehr gilt: Nicht die Technik allein, sondern striktes Configuration Management und gelebte Sicherheitsprozesse sind die Grundlage für ein sicheres Netz.

Sicherheit in Wireless LAN: Eine endlose Geschichte?

5.
Öffentliche WLAN sind anders, auch bei der Sicherheit

Für öffentliche Hotspots muss das WLAN so ausgelegt sein, dass es mit einer Vielzahl von unterschiedlich konfigurierten Clients zurechtkommt. Gerade hier liegen einige Probleme.

Sind Schlüsselmanagement und Authentisierung speziell für die Clientseite nicht genau standardisiert, kann der Betreiber des Hotspots nicht automatisch davon ausgehen, dass das System eines Kunden die vom Hotspot angebotenen Verfahren auch unterstützt. Der Betreiber wird also gewisse Vorgaben machen müssen, mit dem Risiko nicht genügend potentielle Kunden zu erreichen.

Die nächste Frage wäre, wie für die Authentifizierung der richtige Schlüssel zum Kunden wandert. 802.11i drückt sich hier im Gegensatz zu mobilen Kommunikationssystemen um ein fundamentales Element herum: Der genauen Normung von Apparat und Methode zur Authentifizierung eines Teilnehmers dem Netz gegenüber.

Beispielsweise legt das Global System for Mobile Communications (GSM) hierzu das Subscriber Identity Module (SIM) fest. Dies ist eine Chip-Karte mit standardisierten Schnittstellen und standardisierten Grundfunktionen, die in jeder Mobilstation ("Handy") zu finden ist. Auf dieser Chipkarte sind auf eine vergleichsweise sichere Art (unter anderem) alle Elemente gespeichert, die gebraucht werden, um sich als Teilnehmer dem Netz gegenüber auszuweisen. Der Zugang zum SIM geschieht über eine PIN. GSM legt hierzu die notwendigen Protokolle zwischen SIM-Karte, Mobilstation und dem eigentlichen Mobilfunknetz fest. Mit diesem Mittel ist es dann auch vergleichsweise einfach möglich, ein Roaming zwischen verschiedenen Netzbetreibern zu implementieren. Egal, ob man sich in Hong Kong oder in München in ein GSM-Netz einbucht, die Prozeduren (und insbesondere die SIM-Karte) bleiben genau gleich.

Diese Lücke klafft in 802.11i. Die Festlegung eines einheitlichen Authentifizierungsapparates wie in GSM fehlt. In Konsequenz muss sich jeder Betreiber eine eigene Lösung ausdenken bzw. eine proprietäre Lösung einkaufen. Natürlich könnte jede dieser Lösungen konform mit 802.11i sein, jedoch nicht automatisch interoperabel zwischen Hotspots verschiedener Betreiber. Man könnte fast versucht sein, einfach alle Sicherheitsmechanismen (sprich: WEP, TKIP, 802.1x) für das WLAN abzuschalten. Das grundsätzliche Problem bliebe jedoch erhalten, denn man hat es einfach auf die Netzwerkschicht geschoben. Die Ursache dieser Lücke im Standard ist nicht im technischen Bereich zu sehen: Man hatte öffentliche WLAN einfach nicht als wichtig genug angesehen. Der Aspekt der öffentlichen WLAN (in korrekter Terminologie als Operated WLAN bezeichnet) und des Roaming zwischen Operated WLAN ist jedoch bereits bei TGi von 802.11 angesprochen und diskutiert worden. Wir werden diesen Aspekt im nächsten Kapitel noch weiter erörtern.

Die Probleme gehen leider noch weiter, denn der Hotspot soll ja schließlich einen Internet-Zugang anbieten. Die Frage ist, wie die IP-Konfiguration für einen Client im Hotspot geschieht. Spontan werden Sie vielleicht sagen: "Natürlich über das Dynamic Host Configuration Protocol (DHCP)". Jedoch kann das nicht automatisch von jedem Client erwartet werden, und außerdem ist nicht jeder Nutzer autorisiert oder hat das Wissen, auf seinem Rechner entsprechende Konfigurationen vorzunehmen. Im Idealfall kommt ein Hotspot also ohne jegliche Vorgaben bezüglich der IP-Konfiguration des Clients aus. Hierzu werden typischerweise Proxies eingesetzt. Der Proxy-Server beantwortet ARP-Request des Clients, der seinen Default-Gateway sucht und lernt dabei die IP-Adresse des Clients, die ja im ARP-Request übertragen wird (Proxy-ARP). Da ein Client eine beliebige IP-Adresse verwenden kann, muss der Proxy-Server alle Adressen hinter Network Address Translation (NAT) verbergen. Stellvertretend antwortet der Proxy auf alle DNS Name-Query und antwortet auf alle HTTP-Anfragen. Ein Beispiel für ein Hot-Spot-System, das einen solchen Proxy einsetzt, ist der Broadband Building Services Manager von Cisco, dessen traditioneller Einsatzbereich eigentlich aus dem Bereich des Angebots von Kommunikationsdiensten in Hotels kommt.

In punkto Sicherheit liegt der Schwerpunkt auf dem Schutz vor unberechtigter Nutzung der Kommunikationsressource, sprich: der angebotenen Dienstleistung (typischerweise ein Internet-Zugang über das Hotspot). Die Authentifizierung eines Teilnehmers als zahlungskräftigen Kunden (Subscriber) und die Abrechnung des genutzten Dienstes stehen also im Vordergrund. Sollte der Kunde über einen darüber hinaus ungesicherten Hotspot über das Internet auf private Daten zugreifen, liegt es in der Verantwortung des Kunden, die Übertragung geeignet (typischerweise mit einem IP-VPN) abzusichern.

Ganz so einfach darf man es sich natürlich nicht machen: Ein Hotspot ist meist ein Netz, das Dritten gegenüber Telekommunikationsdienste erbringt (üblicherweise einen Internetzugang über den Hotspot), und es fällt damit in Deutschland unter das Telekommunikationsgesetz.

Die Verfügung 154/1999 der Regulierungsbehörde für Telekommunikation und Post für die Benutzung des ISM-Frequenzbands bei 2,4 GHz für WLAN (synonym: Radio LAN, RLAN) hat unter anderem in Ziffer 11 spezifiziert: "Soweit mit RLAN-Funkanlagen grundstücksüberschreitende Übertragungswege betrieben werden sollen, die für Telekommunikationsdienstleistungen für die Öffentlichkeit (...) genutzt werden", ist "eine Lizenz der Klasse 1, 2 oder 3 erforderlich". Unter den allgemeinen Hinweisen Ziffer 2 wird dieser Sachverhalt für den Internet-Zugang konkretisiert: "Werden die RLAN-Übertragungswege zur Erbringung eines Internet-Angebots genutzt, so stellt dies in der Regel bereits eine Telekommunikationsdienstleistung" dar, die "einer Lizenz der Klasse 3 bedarf."

Hier muss der Hotspot-Betreiber prüfen, ob diese Klausel für ihn zutrifft. Wenn ja, muss eine Lizenz beantragt werden. Eine Lizenz der Klasse 3 als solche kostet zwar keine Lizenzgebühr, jedoch bedeutet die Beantragung einer Lizenz der Klasse 3 bereits, dass der Betreiber gewisse Befähigungsnachweise erbringen muss. Insbesondere muss ein Sicherheitskonzept vorgelegt werden, welches nachweist, dass speziell dem Datenschutz und dem Fernmeldegeheimnis genügend Rechnung getragen wird.

Die Forderung des Sicherheitskonzepts, eigentlich auch ohne Lizenz eine Selbstverständlichkeit, hat auch wirtschaftliche Hintergründe. Nehmen wir an, ein Hotspot basiert auf dem aktuellen 802.11-Standard (ob WEP aktiviert ist oder nicht, tut nichts zur Sache). Ein Kunde bucht sich ein, weist sich aus und surft im Internet. Ein Angreifer kapert seine Sitzung und surft seinerseits unter dem Konto des eigentlichen Nutzers im Internet. Wird der eigentliche Nutzer nach Volumen berechnet, bleibt er auf den Kosten sitzen. Wird der Nutzer nach Zeit abgerechnet, hat der Betreiber einen finanziellen Schaden. Scheinbar reden wir hier nur über ein paar Euro. Der Verlust kann sich jedoch durchaus summieren, wenn dies bei vielen Sitzungen im Hotspot passiert und der Betreiber viele Hotspots unterhält. Schlimmer wiegt jedoch der unter Umständen immense Vertrauensverlust, der die unmittelbare Folge wäre.

Eine weitere Schwierigkeit liegt in der Verwendung von NAT, das entweder aus den eben diskutierten Gründen der bequemen Handhabung unterschiedlich konfigurierter Clients oder einfach aus dem Umfang des Pools an Internet-Adressen resultiert. Ein nicht unbeträchtlicher Teil der Kunden wird den Hotspot als Zugang für ein IP-VPN mit IPSec nutzen, um auf das heimische Intranet zuzugreifen. Unangenehmerweise kann IPSec im so genannten Authenitcation Header als Bestandteil des IP-Payload eine kryptographische Prüfsumme übertragen, die aus IP-Header (ohne variable Felder, z.B. TTL, CRC, jedoch inklusive IP-Adressen) und Daten berechnet wird. Ändert sich die Source-IP-Adresse durch NAT, stimmt die Auswertung des Authentication Headers nicht mehr mit dem erwarteten Ergebnis überein. Der Empfänger würde das Paket als manipuliert bzw. gefälscht verwerfen. Der Proxy müsste also das Paket entschlüsseln und wieder verschlüsseln können, um NAT korrekt durchzuführen. Das geht natürlich nicht. Die eingesetzten VPN-Produkte müssen daher NAT-Traversal unterstützen. Dies gilt jedoch nicht für alle Produkte. Beispielsweise hat Microsoft eine entsprechende Erweitung für die in Windows XP "eingebaute" VPN-Lösung zwar noch für 2002 angekündigt, aktuell unterstützt IPSec mit Windows-Bordmitteln dieses Feature jedoch noch nicht.

Öffentliche Hotspots haben insgesamt einen Anspruch an die Sicherheit, der eher mit dem mobiler Kommunikationssysteme zu vergleichen ist. Allerdings fehlen gerade für Hotspots allgemeinverbindliche Festlegungen. Dies hat zur Folge, dass jeder Betreiber eines Hotspots für sich eine technische Lösung entscheiden muss. Jeder Hotspot bedeutet also aus der Kundenperspektive meist einen neuen Netzzugang, eine neue Vertragsbeziehung mit eigenen Abrechnungsmodalitäten, eine weitere Nutzer-Kennung mit einem weiteren Passwort und ggf. eine weitere Netzkonfiguration. Etwas überspitzt kann durchaus behauptet werden, das spätestens nach dem fünften unterschiedlich "gebastelten" Hotspot 90% der Nutzer entnervt aufgeben werden. Hier besteht also ein unmittelbarer Handlungsbedarf!

6. Wireless LAN und mobile Telekommunikation: Konkurrenz oder Konvergenz?

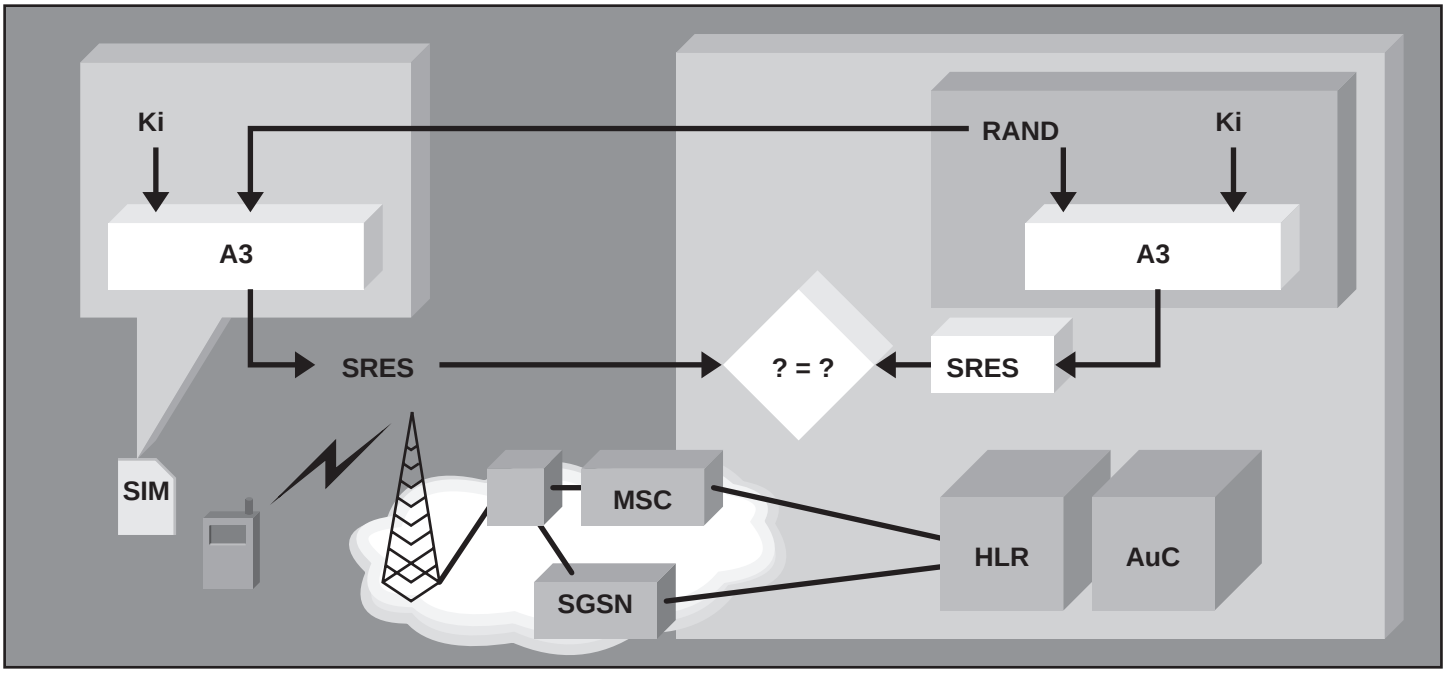
In den vorangegangenen Betrachtungen wurde deutlich, dass ein sicheres WLAN mehr und mehr Elemente integrieren muss, wie man es sonst nur von der Mobilkommunikation (etwa GSM) her kennt. Daher lohnt es sich, einen etwas genaueren Blick auf die Sicherheitsmechanismen in GSM zu werfen.

Ein Mobilfunknetz nach dem GSM-Standard enthält eine Infrastruktur zur netzwerkübergreifenden Authentifizierung und Dienstprofilverwaltung der Teilnehmer. Die eigentliche Authentifizierung erfolgt zwischen SIM und dem Authentication Center (AuC), einem der zentralen Teilnehmerverwaltung (Home Location Register, HLR) zugeordneten Netzelement. Zur Authentifizierung wird ein geheimer Schlüssel Ki verwendet, der im SIM des Teilnehmers und im AuC des Heimatnetzes des Teilnehmers gespeichert ist.

Bucht sich eine Mobilstation in einem fremden Netz ein, ist der erste Kommunikationspartner ein Mobile Switching Center (MSC) für leitungsvermittelte Dienste oder ein Serving GPRS Support Node (SGSN) für paketvermittelte Dienste des fremden Netzes, in dessen Einzugsbereich sich der Teilnehmer befindet. Aus einer Identifikationsnummer des Teilnehmers erkennt das MSC oder der SGSN, dass es sich um einen Teilnehmer aus einem anderen Netz handelt. Es kontaktiert daraufhin das HLR des Heimatnetzes, das seinerseits das AuC zum Beginn der Authentifizierung auffordert.

Das AuC schickt hierzu eine Zufallszahl RAND als Challenge zur SIM des Teilnehmers (wieder über MSC oder SGSN des besuchten Netzes). Die SIM nimmt den geheimen Schlüssel Ki und RAND als Eingabe zu einem als A3 bezeichneten Algorithmus. Das Ergebnis wird an das AuC des Heimatnetzes geschickt. Das AuC führt dieselbe Operation durch und wenn das Ergebnis der empfangenen Zahl entspricht, ist der Teilnehmer (genauer gesagt das SIM) authentifiziert (Bild 10).

Bild 10 Authentifizierung in GSM



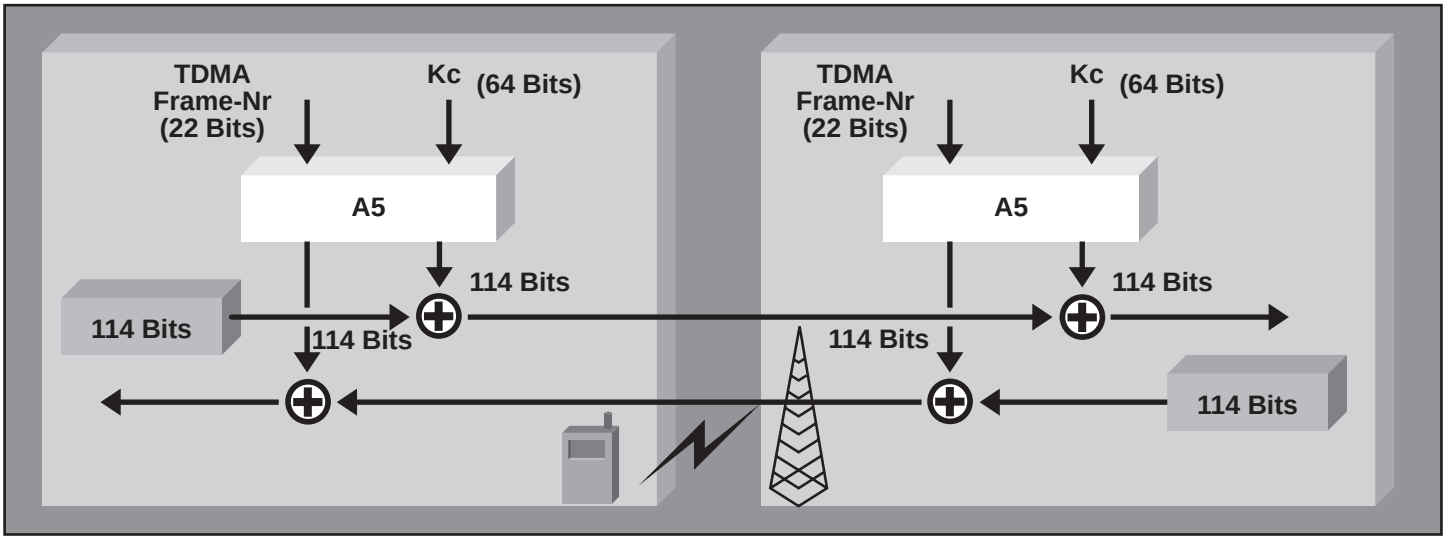


Bild 11 Verschlüsselung in GSM

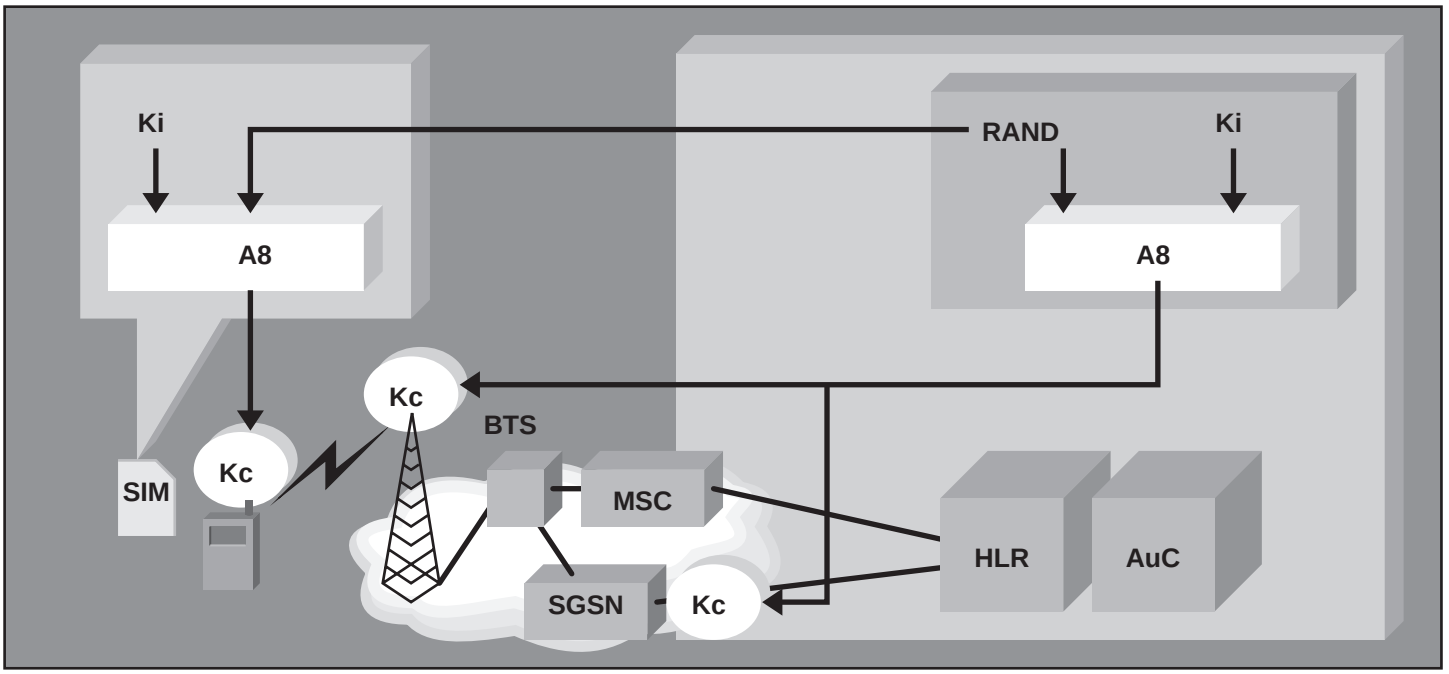
Das Ergebnis wird dem besuchten Netz mitgeteilt, und der Teilnehmer kann im fremden Netz Dienste nutzen, als ob er im Heimatnetz wäre. Dem besuchten Netz ist der Algorithmus A3 vollkommen egal. Nur die Schnittstellen und Protokolle von Mobilstation (mit SIM) und MSC/SGSN und HLR/AuC müssen genau festgelegt sein. Tatsächlich darf jeder Netzbetreiber den Algorithmus A3 eigenverantwortlich festlegen, der Standard macht hier keine Vorgaben.

Ist der Teilnehmer authentifiziert, können Dienste genutzt werden (Telephonie, Internetzugriff, etc.). GSM legt hierzu ein symmetrisches Verschlüsselungsverfahren fest, bei dem die entsprechenden Endpunkte einen gemeinsamen geheimen Schlüssel Kc verwenden. Für leitungsvermittelte Dienste (Sprache, Circuit Switched Data) ist der Endpunkt im Netz die Basisstation (Base Transceiver Station, BTS), für GPRS ist es der SGSN.

Ähnlich der Verwendung des RC4 in WEP wird der eigentliche Schlüsselstrom aus dem Schlüssel Kc und einer zusätzlichen Information, die sich bei jeder Übertragung ändert, gebildet. Bild 11 zeigt dies exemplarisch für die Verschlüsselung an der BTS. Für die Verschlüsselung am SGSN ist das Prinzip das gleiche, nur wird die LLC-Rahmennummer als "Initialisierungsvektor" verwendet. Der verwendete Algorithmus A5 muss international festgelegt sein. Er ist nicht im GSM-Standard veröffentlicht, ist jedoch Bestandteil des GSM Memorandum of Understanding, einer verbindlichen Erklärung aller GSM-Betreiber.

Der gemeinsame Sitzungsschlüssel Kc wird aus dem geheimen Schlüssel Ki bei jeder Authentifizierung gebildet (Bild 12).

Bild 12 Erzeugung des Sitzungsschlüssels in GSM



Der Algorithmus A8 ist - analog zur Authentifizierung - Sache des Netzbetreibers und wird meist zusammen mit A5 als eine Einheit implementiert. Die Authentifizierung geschieht bei jeder erneuten Einbuchung eines Teilnehmers in ein GSM-Netz (Location Update) und kann je nach Parametrierung des Netzbetreibers sogar periodisch erzwungen werden (im Rahmen eines Periodic Location Update).

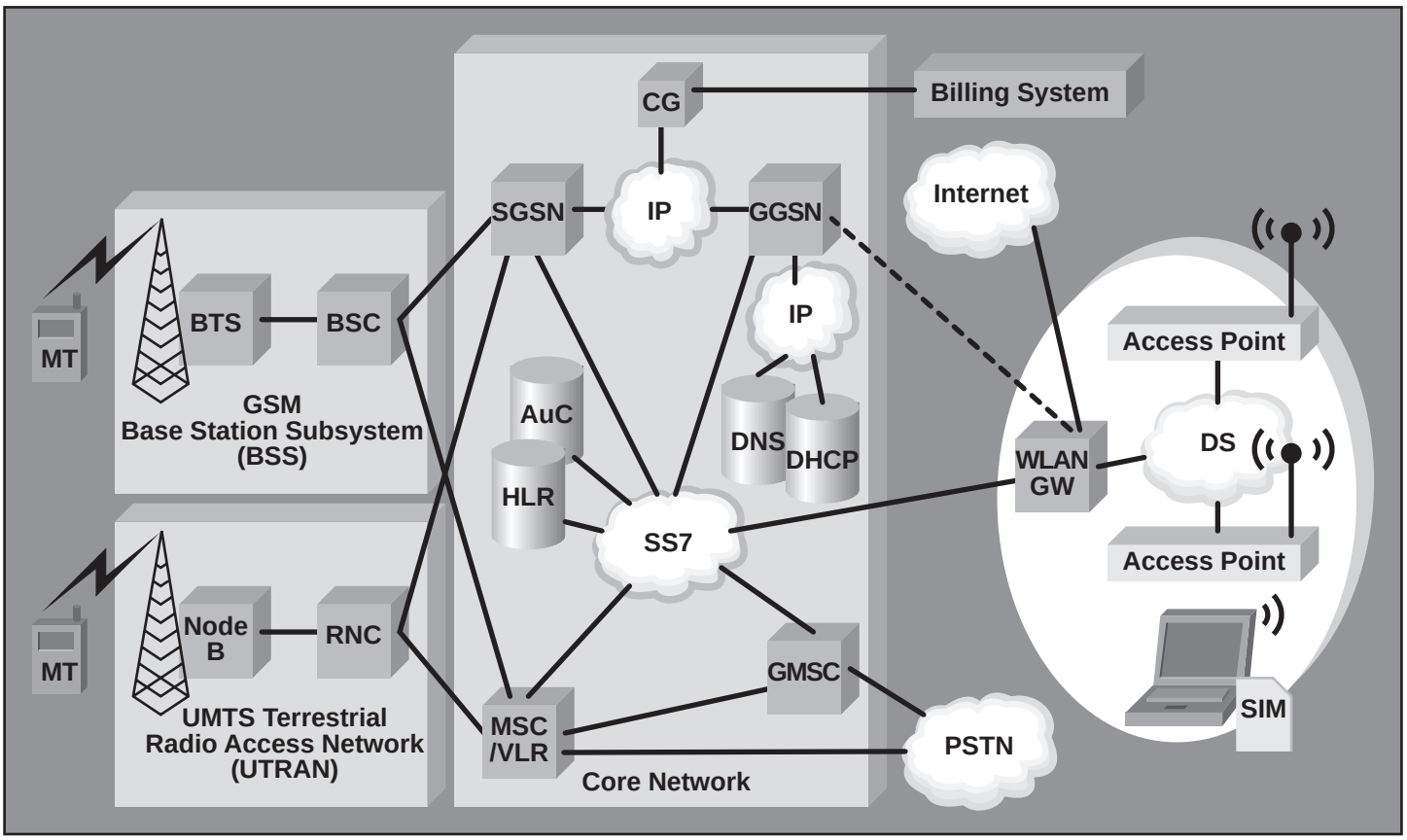
Diese Mechanismen sichern insgesamt ein vergleichsweise hohes Maß an Sicherheit zu. Zumindest sind seit dem Startschuss für GSM vor etwa 10 Jahren keine Desaster wie im Falle eines WLAN nach IEEE 802.11 bekannt geworden.

Eine GSM-SIM ist eigentlich ein universelles Authentifizierungsgerät mit einer fast weltweit einheitlichen Infrastruktur. Die Idee ist nun so simpel wie naheliegend: Warum nicht eine GSM-SIM zur Teilnehmer-Authentifizierung in einem (öffentlichen) WLAN nutzen, wie in Bild 13 skizziert (siehe hierzu auch [2])?

Hier gibt es tatsächlich erste Lösungen, etwa von Nokia und Ericsson, die eine Anbindung eines WLAN über ein entsprechendes Gateway an eine GSM-Infrastruktur erlauben. Die Authentifizierung geschieht über ein GSM-SIM, das im Fall der Nokia-Lösung einfach in den WLAN-Adapter eingeschoben wird. Genauso wie Mobiltelefone in einem fremden GSM-Netzwerk eingebucht werden können (sofern ein entsprechendes Roaming-Agreement zwischen den Betreibern vorliegt), wird Roaming auch für diese WLAN-Inseln unterstützt. Analog funktioniert die Abrechnung. Der Teilnehmer findet die Kosten für die Nutzung des WLAN einfach auf seiner GSM-Abrechnung. Das öffentliche WLAN nutzt also für spezielle Funktionen, die sonst neu zu implementieren wären, einfach eine bestehende GSM-Infrastruktur und ist so quasi zu einem vereinfachten Base Station Sub-System geworden.

Eine solche Lösung ist zwar besser als ein Hot-Spot-Patchwork der Marke Eigenbau, weil es standardisierte GSM-Techniken nutzt. Jedoch geschieht dies auf proprietäre Weise, denn das Interworking zwischen WLAN und GSM bzw. UMTS ist zur Zeit noch nicht standardisiert! Geplant ist dies erst für die Release 6 von UMTS und aktuell hat man erst den Status einer Machbarkeitsstudie erreicht (siehe [15]). Zur Erinnerung: Nächstes Jahr (vielleicht sogar noch Ende dieses Jahres - auch wenn alle Anzeichen dagegen sprechen) werden wir in Deutschland den Start von UMTS mit Release 99 erleben. Danach kommt Release 4, Release 5 und schließlich Release 6. Hier wird der Erfolg und der resultierende Marktdruck die Standardisierung gegebenenfalls erheblich beschleunigen. Immerhin haben sich IBM und Nokia ehrgeizige Ziele gesetzt: Bis 2006 sollen aus dieser Kooperation weltweit 100.000 Hot-Spots entstehen! Das Problem eines fehlenden Standards für ein sicheres Roaming hat bereits zu einer gemeinsamen Initiative von Wireless ISPs (kurz: WISP) und Ausrüstern geführt. Pass-One wurde im April 2002 ins Leben gerufen und Ende Juni dieses Jahres haben bereits mehr als 20 WISPs (dabei einige Mobilfunknetzbetreiber aus Nord-Amerika) und 30 WLAN-Ausrüster der Planung der Entwicklung eines global akzeptierten Service Level Standards für Hotspots zugestimmt [14]. Hier geht es natürlich nicht nur um Sicherheitsaspekte; Accounting, Billing, Session Management, etc. spielen eine genauso große Rolle. Ob wir am Ende zwei Lösungen sehen werden, eine GSM/UMTS-konforme Lösung und eine Pass-One-Lösung, kann zur Zeit noch nicht abgeschätzt werden.

Bild 13 Anbindung eines WLAN an eine GSM- oder UMTS-Infrastruktur



Hoffen wir jedoch das Beste, denn zwei Standards sind zwar besser als keiner, aber meist immer noch einer zuviel.

7. Fazit

WLAN nach dem aktuellen Standard IEEE 802.11 ohne weitergehende Schutzmechanismen lassen sich in den seltensten Fällen mit einer Sicherheitspolitik vereinbaren. Zur Zeit bleiben dem Betreiber eigentlich nur IP-VPN mit IPSec, um ein WLAN geeignet abzusichern.

Mit IEEE 802.11i kann ein WLAN zwar im Rahmen des WLAN-Standards ordentlich gesichert werden, jedoch um den Preis einer erheblich komplexeren Infrastruktur, die den Vergleich zum Aufwand eines IP-VPN nicht scheuen muss. Der Preis der Sicherheit scheint also der Verzicht auf Einfachheit. Doch gerade diese Einfachheit in Aufbau und Konfiguration eines WLAN nach dem bisherigen Standard ist eine der treibenden Kräfte für den Erfolg von WLAN. Es bleibt abzuwarten, mit welchen Kosten in Anschaffung und Betrieb ein WLAN nach IEEE 802.11i verbunden ist; preiswerter wird es jedenfalls nicht.

Zumindest für den Bereich der öffentlichen WLAN ist Bewegung in die Standardisierung gekommen und es ist zu hoffen, dass sich eine Vereinheitlichung im Hot-Spot-Bereich auch auf die private WLAN-Anwendung positiv auswirkt. Bis dahin werden trotz IEEE 802.11i sehr heterogene Sicherheitsinfrastrukturen für private WLAN entstehen, da der Standard an wesentlichen Stellen Freiheitsgrade lässt. Große und selbst mittlere Unternehmen werden also nicht um die Festlegung eines Unternehmensstandards herumkommen, der genau beschreibt, wie mit den Freiheitsgraden IEEE 802.11i umzugehen ist, oder man wird von vorneherein auf einen IP-VPN Unternehmensstandard setzen. Das Kapitel "Sicherheit in WLAN" ist also längst noch nicht abgeschlossen.

9. Literatur

[1] C. Höchel-Winter, Wireless LAN Grundlagenreport ("Wireless LANs - Arbeitsweise, Einsatzbedingungen, Produkte"), Technologie Report, ComConsult Technologie Information, März 2002.

[2] S. Hoff, J. Wetzlar, "Konvergenz zu IP in mobilen Kommunikationssystemen - Weniger ist mehr", Der Netzwerk Insider, Dr. Suppan International Institute, Juni 2002.

[3] ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[4] IEEE Std 802.11b, "Higher-Speed Physical Layer Extension in the 2.4 GHz Band", 1999.

[5] IEEE Std 802.11a, "High-speed Physical Layer in the 5 GHz Band", 1999.

[6] Regulierungsbehörde für Telekommunikation und Post, Mitteilung 325/2002, "Frequenznutzung im 5-GHz-Bereich für WLANs (Wireless Local Area Networks) Anhörung zu einer Allgemeinzuteilung".
Verfügbar unter http://www.regtp.de/tech_reg_tele/start/fs_06.html

[7] AirSnort Homepage http://airsnort.shmoo.com/

[8] Ethereal Homepage http://www.ethereal.com/

[9] W. A. Arbaugh, N. Shankar, Y.C. J. Wan, "Your 802.11 Wireless Network has No Clothes", University of Maryland, März 2001.
Verfügbar unter http://www.drizzle.com/~aboba/IEEE/

[10] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4".
Verfügbar unter http://www.drizzle.com/~aboba/IEEE/

[11] IEEE 802.11 Homepage http://grouper.ieee.org/groups/802/11/index.html

[12] IEEE Std 802.1x, "Port-Based Network Access Control", 2001.

[13] J. Daemen, V. Rijmen, "AES Proposal: Rijndael", 1999.

[14] Pass-One Homepage http://www.pass-one.com/

[15] 3GPP TR 22.934, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking; (Release 6)", Februar 2002.
Verfügbar unter http://www.3gpp.org/

[16] A. Mishra, W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1x Standard", Februar 2002.

Sicherheit in Wireless LAN – Abk.

A	AES	Advanced Encyption Standard
	ARP	Address Resolution Protocol
	ARQ	Automatic Repeat Request
	AuC	Authentication Center
B	BSC	Base Station Controller
	BSS	Basic Service Set
	BTS	Base Transceiver Station
C	CG	Charging Gateway
	CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
	CRC	Cyclic Redundancy Code
D	DECT	Digital Enhanced Cordless Telecommunications
	DES	Data Encryption Standard
	DHCP	Dynamic Host Configuration Protocol
	DNS	Domain Name System
	DS	Distribution System
	DSSS	Direct Sequence Spread Spectrum
E	EAP	Extensible Authentication Protocol
	EAPOL	EAP over LAN
	ESS	Extended Service Set
	ETSI	European Telecommunications Standards Institute
G	GGSN	Gateway GPRS Support Node
	GMSC	Gateway MSC
	GSM	Global System for Mobile Communications
H	HLR	Home Location Register
I	IAPP	Inter Access Point Protocol
	ICV	Integrity Check Value
	IEEE	Institute of Electrical and Electronics Engineers
	IKE	Internet Key Exchange
	ISM	Industrial, Scientific and Medical
	IV	Initialization Vector
M	MAC	Medium Access Control
	MIC	Message Integrity Check
	MSC	Mobile Switching Center
N	NAT	Network Address Translation
	NIST	National Institute of Standards and Technology
O	OCB	Offset Code Book
P	PSTN	Plublic Switched Telecommunications Network
R	RADIUS	Remote Authentication Dial-in User Service
	RNC	Radio Network Controller
S	SGSN	Serving GPRS Support Node
	SIM	Subscriber Identity Module
	SS7	Signalling System No. 7
T	TKIP	Temporary Key Integrity Protocol
U	UMTS	Universal Mobile Telecommunications System
V	VPN	Virtual Private Network
W	WECA	Wireless Ethernet Compatibility Alliance
	WEP	Wired Equivalent Privacy

Zum Schwerpunktthema

WLAN-Sicherheitsprobleme – unkonventionelle Gedanken

von Dr. Franz-Joachim Kauffels

Die Diskussion über WLAN-Sicherheit wird normalerweise mit dem gleichen Schema geführt wie schlechthin bei derartigen Diskussionen. Meiner persönlichen Ansicht nach führt dies zu falschen Hoffnungen.

Der Autor gibt zu, schon vor der Auseinandersetzung mit drahtlosen Netzen graue Haare gehabt zu haben. Die Netze selbst haben nicht zu wesentlich mehr Kopfschmuck in dieser Hinsicht beigetragen. Was aber im Zusammenhang mit Datenschutz und Datensicherheit bei drahtlosen Netzen so alles gesagt und geschrieben wird, kann dem gestandenen Stephen King Fan die Farbe aus dem Gesicht treiben, oder eben aus den Haaren wie beim Autor. Um es direkt zu sagen: soviel Quatsch auf einem Haufen habe ich noch nie wahrnehmen müssen. So genannte Experten raten zu unglaublichen "Sicherheitsmitteln" unter völliger Ignoranz der Eigenheiten der Wellenausbreitung. Es geht vielfach schon damit los, dass zu so genannten "Messungen" Notebooks mit WLAN-Adapterkarten ausgestattet werden. Die dann erhaltenen "Messungen" messen lediglich, wie sich dieses Notebook in der Hand seines Bedieners in diesem Moment angesichts der ankommenden elektromagnetischen Wellenfront fühlt. Die Chips in den WLAN-Adaptern haben manchmal enorm miserable Empfänger. So etwa wie die Ohren eines Kindes, dem man sagt, es soll aufräumen, Rasen mähen oder spülen. "Misst" man mit diesen Geräten dann, dass z.B. auf dem Parkplatz neben dem Gebäude nichts mehr zu "hören" ist, sollte man nicht den Schluss daraus ziehen, dass die elektromagnetischen Wellen des WLAN dort "enden".

Messungen darf man nur mit professionellem Equipment ausführen, wenn man aussagekräftige Ergebnisse haben möchte.

Durch eine Mehrfachanwendung der Super-Heterodyneschaltung kann man einen enorm empfindlichen und trennscharfen Empfänger bauen. Wenn ich als externer Angreifer ein WLAN abhören möchte, baue oder besorge ich mir zu allererst einen entsprechend empfindlichen Empfänger. Dann kann ich nämlich auch weit außerhalb des eigentlichen Arbeitsbereiches des WLANs alle Signale decodieren und bleibe dabei völlig unauffällig.

Erste Untersuchungen haben ergeben, dass die allermeisten Betreiber von WLANs offensichtlich überhaupt keinen blassen Schimmer davon haben, was sie tun und wie leicht es ist, den Datenschutz von WLANs auzuhebeln. Das ist schon keine Fahrlässigkeit mehr, sondern himmelschreiende Dummheit! So hat z.B. die Wirtschaftsprüfungsgesellschaft Ernst & Young festgestellt, dass bei 80% der stichprobenartig in Wien gefundenen 200 WLANs noch nicht einmal die einfache WEP-Verschlüsselung aktiviert war, sondern die gesamten Daten fröhlich unverschlüsselt durch den Äther marschierten. Dabei wird völlig vergessen, dass der potentielle Schaden nicht auf das eigene Unternehmen beschränkt bleibt, sondern vielmehr üblicherweise auch die Daten von Kunden und Geschäftspartnern betroffen sind. Es gibt Stimmen, die sagen, der Bezug auf solche Ergebnisse sei unseriös, weil es auch viele Testnetze gibt,

die in solche Messungen einfach einfließen und bei denen es völlig gleichgültig ist, ob die Daten nun verschlüsselt sind oder nicht. Wie auch immer, ist es völlig gleichgültig, ob nun "2,3", "50" oder "85%" der angemessenen Netze "echte" Netze und dennoch unverschlüsselt sind. Meine innere Stimme sagt mir, dass jeder Unfug, der von Seiten der Betreiber möglich ist, auch gemacht wird. Eine Abhilfe ist es in der Tat, wenn die WLAN-Teile von den Herstellern direkt so vorkonfiguriert werden, dass die Verschlüsselung per Default eingeschaltet wird. Dann muss der Benutzer/Administrator es explizit ausschalten. Das wäre mit einer Aktion verbunden, die rein statistisch möglichst vermieden wird. Noch besser wäre es, wenn man die Verschlüsselung gar nicht mehr abschalten könnte. Herkömmliche Sicherheitsstrukturen sind beim Einsatz von WLANs vielfach machtlos, da sie davon ausgehen, dass die Daten im Unternehmen "innerhalb" des eigenen Netzwerks bleiben.

Generell ist folgendes festzuhalten:

- WLANs sind äußerst einfach zu stören, und das gleich in mehrfacher Hinsicht
- Alle über das WLAN gesendeten Daten können auch weit außerhalb des eigentlichen Aktionsbereiches des WLANs immer decodiert werden
- Die Kanaltrennung in WLANs bietet keinerlei Schutz
- Der WEP-Algorithmus bietet fast keinen Schutz

Der Autor

Dr. Franz-Joachim Kauffels ist einer der bekanntesten und erfahrensten Referenten der Netzwerkszene. Bekannt geworden durch vielfältige Publikationen, Seminare und Kongresse setzt sich der selbständige Unternehmensberater für eine fortschrittliche und wirtschaftliche Nutzung der neuen Technologien ein.

WLAN-Sicherheitsprobleme – unkonventionelle Gedanken

Im folgenden Abschnitt werden wir die Bedrohungen weiter ausführen. Nur durch eine geeignete Kombination von zusätzlicher Verschlüsselung, Firewalls, Einsatz eines VPN und MAC-Authentifizierung lässt sich im Rahmen einer allgemeinen Sicherheitspolitik Schlimmeres abwenden. Also müssen wir uns, wenn man es seriös machen will, mit dem Gesamtthema der Sicherheit in Netzen unter besonderer Berücksichtigung funktechnisch angeschlossener Endgeräte befassen.

Der Autor steht mit seiner Meinung nicht alleine. Eine Sprecherin von Cisco Systems hat es treffend formuliert: "bevor Daten auf ein WLAN gehen, müssen sie für einen externen Angreifer völlig unbrauchbar gemacht werden."

Bedrohungen für WLANs

In diesem Abschnitt wollen wir die weiter oben gemachten Thesen vertiefen und weitere Hinweise geben. Wir kommen durch die Funknetze in eine absurde Situation: einerseits arbeitet man mit Hochdruck daran, die heutigen Unternehmensnetze hochverfügbar zu machen. Die Verfügbarkeit 99,999 ("five nine") klappt noch nicht in jedem Fall, aber die Anstrengungen der letzten zwei Jahre beginnen, in dieser Hinsicht Wirkung zu zeigen. Besonders die Arbeiten von Petra Borowka (siehe die Neuauflage* von "Internetworking") haben hier durch vernünftige, fundierte mathematische Analyse zu wirklich guten konstruktiven Lösungen in der Praxis geführt. Sowohl für den Serverbetrieb als auch für Anwendungen wie Voice over IP ist eine sehr hohe Verfügbarkeit des Netzes wichtig.

* heißt im Handel "Netzwerk Technologien"

Grade die WLANs sind aber in ihrer heutigen Form nur dann als zuverlässig einzustufen, wenn man die von den Herstellern gegebenen Möglichkeiten sinnvoll ausschöpft. Dennoch kann man sie ganz einfach völlig lahmlegen. Es wird also nichts anderes übrig bleiben, als die "ordentliche" vernetzte DV des Unternehmens (oder was sich dafür hält) von den WLANs so zu separieren, dass Rückwirkungen ausgeschlossen werden können.

Es sei noch darauf hingewiesen, dass es außer den IEEE 802.11 WLANs noch mindestens ein Dutzend Systeme für drahtlose Informationsübertragung gibt, die im täglichen Einsatz gut funktionieren die trotz vergleichbarer Bedrohungslage dennoch kaum extravagante Sicherheitslücken mit sich bringen, einfach weil es sehr viele "harmlose" Anwendungsbereiche gibt und weil es immer definierte Übergabepunkte zwischen den drahtlosen Systemen und dem Rest der DV gibt.

Bedrohungen durch Störungen des Gesamtverkehrs

Wenden wir uns der ersten These zu: WLANs sind äußerst einfach zu stören, und das gleich in mehrfacher Hinsicht.

Der einfachste Angriff ist die Störung durch einen Störsender. Ein solcher Störsender ist einfach zu bauen: man benötigt einen Oszillator, der in etwa auf der mittleren Sendefrequenz schwingt und einen Frequenz-Modulator, der die primäre Zeichenschwingung des Oszillators so mit einem relativ niederfrequenten Signal moduliert, dass das Ausgangssignal über den Frequenzbereich aller Kanäle des WLAN "wandert". Also benötigt man nur zwei Schwingkreise, die sich z.B. durch je zwei rückgekoppelte Logikgatter, z.B. NANDs, leicht herstellen lassen. Man muss dann nur den niederfrequenten und den hochfrequenten Oszillator in Reihe schalten und schon hat man das gewünschte Gerät. Streng genommen ein Chip, zwei Kondensatoren und einen Widerstand, mit einem Schaltungstrick und der richtigen Chipfamilie lassen sich die für die Schwingkreise eigentlich notwendigen Spulen noch einsparen. Das Ganze kann man in der Luft zusamenlöten und zusammen mit einer 9V Batterie braucht man den Platz einer Streichholzdose. Bei Freaks ist so etwas auch als Peilsender bekannt. Schicken Sie dann einem Bekannten in der anzugreifenden Firma anonym einen Kaktus mit dem Sender unten im Blumentopf und für eine geraume Zeit können Sie den WLAN-Datenverkehr

knicken. Die Frage ist, ob jemand auf die Idee kommt, den Störsender zu suchen oder wie lange die Batterie hält. Sie können den Störsender auch in das Polster eines Polsterumschlages stecken. Aus ästhetischen Gründen lehne ich das Verbergen des Senders in einem Schokoriegel ab. Diese Schaltung kann jeder, aber auch wirklich jeder schnell bauen und die notwendigen Einzelteile kosten unter 5 Euro. Mit diesem Störsender erhalten Sie gleichzeitig das beste Kosten/Spaßfaktor-Verhältnis. Der Spaß ist besonders groß bei Hotspots, wenn man all die frustrierten Geschäftsleute auf ihren Notebooks verzweifelt herumhämmern sieht und mit dem Peilsender in der Zigarettenschachtel verschwinden kann, bevor man selbst angepeilt wird. Mit Skateboard oder Rollerblades ist man in jedem Fall schneller als die Anpeilung. Gegenmaßnahmen gibt es kaum, weil die Schaltungen individuell gemacht werden können und man bei einer Störung auch nicht so schnell auf den Störsender kommt. Mit den puckligen Adapterkarten in Notebooks kann man den Störsender nicht finden, wohl aber mit einer konventionellen Dreieckspeilung. Eine Verbesserung der Schaltung ergibt sich, wenn man noch einen Timer dranbaut, der den Störsender nur manchmal aktiv werden lässt. Dann dauert das Suchen länger. Noch besser wird die Schaltung natürlich, wenn sie weiter miniaturisiert wird.

Die nächste Methode, das WLAN in den Keller zu bringen, ist ein Angriff auf den Zugangsalgorithmus. Wie eigentlich überall bekannt, ist das DCF-Verfahren empfindlich gegen eine zu hohe Anzahl von Stationen, eine zu kleine durchschnittliche Paketlänge, ein zu hohes Verkehrsaufkommen usf. Daraus ergibt sich direkt ein bunter Strauß von Möglichkeiten.

WLAN-Sicherheitsprobleme – unkonventionelle Gedanken

Man könnte z.B. von einer getunten Station aus ordentlich Last generieren. Ich warte eigentlich auf die ersten Analysetools, die das zu Messzwecken sowieso können. Man schickt dann den Algorithmus in die Knie. Weiterhin könnten sich zu Hunderten Stationen anmelden, die alle gar nicht zugelassen sind. Der Algorithmus muss das dann sortieren. Dafür braucht er eine gewisse Zeit, in der er keine weiteren Anfragen mehr beantworten und schon gar keine Pakete via Access Point weiterleiten kann.

Oder man baut eine Station so um, dass sie sich immer mit dem kürzesten Intervall vorpfuscht und dann ein langes Paket schickt. Dann stehen alle anderen Stationen im Regen. Ich muss aufhören, darüber nachzudenken, denn dieser Algorithmus ist in dieser Hinsicht so schlapp, dass man sozusagen im Minutentakt neue Angriffsmöglichkeiten findet. Solange dieser Algorithmus nicht geändert wird, und danach sieht es nicht aus, gibt es keinerlei wirkungsvolle Gegenmaßnahmen.

Etwas wertvoller als der Störsender, aber ebenso leicht zu bauen, wäre ein Repeater, also ein Empfänger mit nachfolgendem Sender. Durch entsprechende Platzierung könnte man dafür sorgen, dass die Ordnung in den Funkzellen durcheinander kommt, weil Geräte den eigentlichen Wirkungsbereich des BSS verlassen. Um die Störung zu beseitigen, muss man den Repeater physisch finden. Auch in diesem Falle ist eine Prävention unmöglich.

Wie Sie leicht sehen, ist ein Funksystem seiner Natur nach sehr verletzlich gegen solche Arten von Angriffen. Jeder Schüler, der erfolgreich mit seinem Elektronik-Experimentierbaukasten gearbeitet hat, hat die notwendigen Grundlagen dazu. In jedem Elektronikshop gibt es die passenden Einzelteile. Man kann sogar bei dem Peilsender auf eine passende hochfrequente Ausführung der Oszillatoren verzichten, es reicht völlig, wenn man eine niedrigere Frequenz nimmt, deren soundsovielte Harmonische 2,4 GHz ist. Mit Störsender und Repeater kann man für wenig Geld viel Unfug anrichten, wer es vornehmer mag, greift für das gleiche Ergebnis den Zugriffsalgorithmus an. Natürlich sind Besitz und Betrieb von Störsendern und Repeatern in der Bundesrepublik Deutschland verboten und deswegen gebe ich auch die Schaltungen hier nicht explizit an.

Bedrohungen durch Anpeilen

Kommen wir zur zweiten These: die Daten aus dem WLAN können auch weit über dessen eigentlichen Aktionsradius hinaus empfangen und decodiert werden.

Der Grund dafür ist einfach: in den Chips der WLAN-Adapterkarten sind miese kleine Empfängerchen drin, wirklich das Billigste, was ging. Sie werden eigentlich nur noch von den kleinen billigen Senderchen übertroffen.

Messungen* des Labors der ComConsult Technologie Information haben ergeben, dass die Sender so schlecht sind, dass ein gesendetes Signal nicht nur auf dem Kanal, auf dem es sein sollte, sondern auch auf fast allen anderen Kanälen zu finden war. In den Seitenkanälen war es allerdings ein wenig schwächer.

In Kombination mit einem schlechten Empfängerchen ergibt sich dann, dass sich das billige Pärchen genau auf der Hauptfrequenz des Kanals trifft, weil da das Sendesignal gerade so stark ist, dass es von dem miesen Empfängerchen empfangen werden kann.

Ein nur wenig besserer Empfänger empfängt locker auch die Signale auf Kanälen, wo sie nicht hingehören. Ein noch besserer Empfänger kann das auch noch aus etwas größerer Entfernung. Ein hochempfindlicher Peilempfänger mit passender Peilantenne wird ein WLAN-Signal je nach Hindernislage noch auf mehreren Kilometern außerhalb des eigentlichen gedachten Wirkungsbereiches decodieren können.

Die jetzt in neueren Produkten implementierte und z.B. für den Einsatz von WLANs auf dem 5 GHz-Bereich in Deutschland geforderte automatische Anpassung der Sendeleistung hilft dabei gar nichts, denn sie orientiert sich ja an der Empfangslage der "normalen" Empfänger auf den Adapterkarten in den mobilen Geräten. Auch Verfahren wie Frequency Hopping und OFDM nutzen in diesem Zusammenhang überhaupt nichts, denn es ist gleichgültig, ob man empfindliche oder unempfindliche Empfänger auf diese Verfahren einstellt. Generell kann man davon ausgehen, dass man die Daten genausogut an eine Plakatsäule kleben könnte anstatt sie über ein WLAN zu schicken.

Bedrohungen durch Erkundung

Hat man ein WLAN einmal entdeckt, kann man es weiter erkunden. Hierbei sind vor allem folgende Analysatoren bzw. Pogramme eine große Hilfe:

- Sniffer Wireless von Network Associates
- AiroPeek von WildPackets
- NetStumbler im Windows Umfeld
- Ethereal im UNIX-Umfeld

Informationen zu Bezugsmöglichkeiten finden Sie auf den Homepages der Hersteller bzw. unter Suchen nach dem Produktnamen. Bei diesen Suchen finden Sie auch vollständige Anleitungen für die schrittweise Durchführung von Angriffen. Deshalb können wir uns hier kurz fassen.

Neben dem einfachen Abhören von Daten ist es natürlich besonders spannend und Voraussetzung für elegante höherwertige Angriffsmuster, im WLAN als authorisierte Station mitzumischen. Nach IEEE 802.11 muss man mindestens den Service Set Indentifier SSID eines WLANs kennen. Man kann aber auch ein so genanntes Open System konfigurieren, in dem das nicht nötig ist. Mit dem Programm NetStumbler kann man folgendes machen. Das Programm sendet einen Radio Beacon Frame mit einem "empty set SSID" aus. Sollten Access Points so konfiguriert sein, dass sie auf Anfragen von Stationen, die den speziellen SSID nicht kennen, reagieren, werden sie als Antwort auf diesen Beacon einen Frame mit einer Liste ihrer SSIDs und weiterer Information senden. Generell können die Analysatoren den gesamten Datenverkehr eines WLANs aufzeichnen und für die spätere Analyse aufbewahren. Wenn ein WLAN nicht als Open System konfiguriert ist, kommt man mit dem NetStumbler nicht weiter. Mit den Analysatoren kann man aber von jedem beobachteten WLAN die SSIDs ausfiltern, die 802.11-Frames aufnehmen und die gesamten Inhalte zerlegen. Gute Produkte finden auch die Sendefrequenzen und mit ein bisschen Geduld die Hop-Sequenzen heraus. Sie können es auch mit den berühmten SSIDs "tsunami" oder "Linksys" probieren, das sind die Default-SSIDs bei Cisco bzw. Linksys-Produkten. Vielfach macht sich niemand die Mühe, die zu ändern, wenn die APs in Betrieb gehen.

---

* Cornelius Höchel-Winter, Wireless LAN Grundlagenreport ("Wireless LANs: Arbeitsweise, Einsatzbedingungen, Produkte"), Technologie Report der ComConsult Technologie Information, Aachen 2002

WLAN-Sicherheitsprobleme – unkonventionelle Gedanken

Bedrohungen durch den WEP-Algorithmus

Der WEP-Algorithmus bietet nur einen sehr geringen Schutz gegen zufälliges Abhören oder ärmlich ausgestattete Hacker. WEP benutzt einen einfachen Vorwärts-Blockcodierer. WEP ist sicherlich sinnvoll, wenn Ihre Daten sowieso nicht so wertvoll sind, dass sich der Aufwand zur Decodierung lohnen würde.

Die ersten Warnungen zu WEP kamen schon im Herbst 2000 mit der Arbeit von Walker "Unsicher bei jeder Größe: eine Analyse der WEP-Verschlüsselung". Die Hauptschwäche von WEP ist nach dieser Arbeit die Tatsache, dass der verschlüsselte Datenstrom jedes Mal reinitialisiert wird, wenn eine Kollision auf dem gemeinsam benutzten Übertragungsmedium auftritt. Wie wir ja wissen, sind Kollisionen unvermeidlich und mit steigendem Gesamtverkehr steigt die Wahrscheinlichkeit für diese Kollisionen. Wenn der Gesamtverkehr zu gering für Kollisionen ist, dann muss man eben ein bischen nachhelfen. Wenn jemand den Verkehr abhört, kann er den Initialisierungsvektor, den es in jedem Frame gibt, aufnehmen und hat in wenigen Stunden alle Informationen, die er zur Brechung des WEP-Schlüssels benötigt.

Einige Monate waren die Ergebnisse solcher Untersuchungen und Betrachtungen eher akademischer Natur. Dann aber tauchten die Programme AirSnort und WEPcrack auf, die es jedermann möglich machen, WEP zu knacken und zwar nicht nur im Sinne des Lesens der Inhalte, sondern vielmehr im Sinne des Wiedergewinnens des WEP-Schlüssels, erst wenn man den hat kann man richtig mit Angriffen loslegen. In 2001 war der Besitz einer Wireless Adapterkarte mit dem PRISM2-Chipsatz einzige weitere Voraussetzung.

Normalerweise denkt der einfache Benutzer oder Administrator, dass eine 128-Bit-Verschlüsselung "besser" sein muss als eine 64 Bit Verschlüsselung. Dem ist meistens auch so, nicht aber bei WEP, weil WEP hier eine weitere schwere konstruktive Macke hat.

Im Rahmen der 64 Bit Verschlüsselung spezifiziert der Netzwerk-Manager einen 40-Bit-Schlüssel, normalerweise zehn hexadezimale Zahlen. An diesen 40-Bit-Schlüssel wird ein 24 Bit Initialisierungsvektor IV angehängt und dann wird das RC4-Verschlüsselungsverfahren mit diesen Informationen initialisiert.

Bei der 128 Bit Verschlüsselung geht es genauso zu: der Administrator definiert einen 104 Bit langen Schlüssel durch 26 Hexadezimalzahlen. An den Beginn des Schlüssels wird dann die 24 Bit lange IV gestellt und das RC4-Verfahren kann loslegen.

Wie man sieht kommt die Verletzlichkeit des Verfahrens durch die Verwendung von leicht vorhersagbaren Initialisierungsvektoren und die Gesamtlänge des Schlüssels macht daher auch keinen großen Unterschied. Das liegt an der kleinen Anzahl insgesamt möglicher Initialisierungsvektoren, die momentan bei 2 hoch 24 liegt. Wenn der WEP-Schlüssel nicht innerhalb streng festgelegter, kurzer Zeitintervalle gewechselt wird, können allle möglichen IV-Kombinationen aus einer 802.11-Verbindung herausgehört und für das Cracken innerhalb kurzer Zeit verfügbar gemacht werden. Das ist ein klarer Designfehler.

Wie schon gesagt existieren Programme zur Brechung bzw. Wiedergewinnug des WEP-Schlüssels. Abhängig von der Maschine mit der man den Angriff durchführt, von der Anzahl der aktiven Teilnehmer im WLAN und der Anzahl von IV-Retransmissionen wegen Kollisionen dauert es nur ein paar Stunden, bis man den Schlüssel geknackt hat. Natürlich wird es umso schwieriger, desto weniger Verkehr in einem WLAN ist. Sobald man einen gültigen WEP-Schlüssel hat, kann man nunmehr erfolgreich eine Verbindung mit einem AP aufnehmen und Zugriff zum Zielnetz erhalten. Gibt es dann in diesem Netz nicht noch weitere Schutzmaßnahmen, kann der Angreifer im Netz arbeiten und als nächstes versuchen, z.B. Zugang zu Servern zu bekommen. Filter auf MAC-Ebene helfen hierbei auch nicht besonders viel, die kann man mit relativ einfachen Methoden, wie sie in jedem Hacker Buch stehen, auch aushebeln.

Aber auch reines Abhören bringt schon viele interessante Informationen. So kann man z.B. aus einem internen DHCP-Server die IP-Adressen herausbringen. Alleine die Struktur einer IP-Adresse gibt weiteren Aufschluss über das Netz. Fährt man ein DNS lookup gegen die IP Adresse, so kann man z.B. herausbringen, welcher Provider den Internet-Service für das angegriffene Netzwerk leistet. Ein interessantes Programm ist auch Nmap. Dieses Tool kann den gesamten Arbeitsbereich einer IP-Adresse ausleuchten, wie viele Geräte aktiv sind, welche Geräte aktiv sind und welches Betriebssystem benutzt wird. Nmap zeigt auch die offenen und auf Verbindungen wartenden TCP und UDP-Ports. Sehen Sie mal auf die Adresse www.insecure.org/nmap. Das ist schon toll, welchen Unfug man damit anrichten kann.

Noch wirkungsvoller ist natürlich der Diebstahl eines Endgerätes. Dann hat man wirklich alle Informationen, die man benötigt. Da es nun einmal so ist, dass viele Mitarbeiter mobil sein sollen und ihre Notebooks mitnehmen, muss man im Rahmen einer unternehmensweiten Sicherheitsstrategie auch für diesen Fall Vorsorge treffen.

Zwischenfazit

Man muss hinnehmen, dass WLANs in ihrer heutigen Bauweise sehr unsicher sind. Also sollte man eine Gesamtstrategie für das Netzwerk aufsetzen, die diese Tatsache berücksichtigt. Denn auch die weit verbreitete Meinung, dass die Übertragung von Informationen über Drähte sicher sei, ist natürlich falsch. WLANs fügen also einem Netz streng genommen keine besondere zusätzliche Unsicherheit zu. Neu ist nur, dass es jetzt so offenbar wird, dass niemand mehr darum herumkommt. Von daher bin ich eigentlich gar nicht traurig, dass dem so ist. Wie wir sehen werden, war und ist das Einbringen von Sicherheitsmechanismen in den unteren Schichten nicht besonders sinnvoll, der Schutz muss bereits auf der Ebene der Anwendungen und Betriebssysteme beginnen, alles andere ist Flickwerk.

Hilfe naht in zweierlei Hinsicht. Zum einen bieten verschiedene Hersteller wie Cisco Systems eigene Verschlüsselungsverfahren an, die sicherlich besser sind als WEP, weil man es fast gar nicht schlechter machen kann. Um wieviel diese Verfahren allerdings besser sind, lässt sich heute noch nicht sagen. Zum anderen arbeitet auch IEEE 802.11 an Lösungen für diese Probleme und diese Arbeiten werden noch in 2003 zu Ergebnissen führen.

ComConsult Akademie Network Professional Club Corner

Einblicke immer und überall!

Liebe Leserinnen, liebe Leser,

der Club freut sich weiterhin über eine stetig steigende Mitgliederzahl. Wenn das so weitergeht wie bisher haben wir schon Ende diesen Jahres über 2.000 Network Professionals im Club.

Der enorme Zuspruch motiviert uns natürlich, unseren Teil dazu beizutragen, das Angebot weiter auszubauen und neue Möglichkeiten zu erschließen.

Dabei wollen wir uns natürlich nach Ihren Wünschen orientieren.

Dafür werfen wir einen Blick in die Statistik:

Dipl.-Ing. Roland Moos
arbeitet er als Senior-Trainer bei der ComConsult Akademie und im Produkt-Forschungsbereich der ComConsult Technologie Information. Der ComConsult Akademie Network Professional Club ist sein persönliches Steckenpferd.

Mailen Sie Ihre Wünsche an:
roland.moos@comconsult-akademie.de

ComConsult Akademie Network Professional Club

Der Club ist eine kostenfreie Dienstleisung der ComConsult Akademie. Nach der Anmeldung erhalten Sie Ihre persönliche Mitgliedskarte und Ihr Passwort, und können sofort die Leistungen des Clubs unter www.comconsult-akademie nutzen: Teilweise eigens für die Clubseite erarbeitete und geschriebene Informationen über aktuelle Netzwerk-Technologien und die Schwerpunktartikel des Netzwerk Insiders als Jahrbuch. Zur Seminaranmeldung tippen Sie nur Namen und Mitgliedsnummer ein, den Rest erledigen wir. Bei Seminarbesuchen bekommen Sie Treuepunkte gutgeschrieben, die sie gegen Prämien einlösen können: Fachzeitschriften-Abos, Organizer, PDAs, Netzwerkkomponenten, kostenlose Seminarbesuche und Reisen in europäische Metropolen. Jedem Clubmitglied steht seine persönliche Abfrageseite zur Verfügung, die den aktuellen Punktestand anzeigt.

1. Treue-Prämien

Auf der Clubseite des Akademieservers werden die Prämienseiten mit Abstand am häufigsten aufgerufen.

Diesen Monat haben wir die Rubrik "200 Bonuspunkte" um eine neue Treue-Prämie bereichert: Mit dem CASIO TV-970 steht Ihnen jetzt ein Mini-Farbfernseher zur Auswahl. Sein Ti-STN Flüssig-Kristall-Bildschirm (5,86 cm Diagonale) steht für ein scharfes Bild, und das bei knapp 40.000 Bildpunkten. Er kann über vier 1,5 V AA Batterien mit Strom versorgt werden, als Zubehör ist ein Netzadapter sowie ein 12V-Autoadapter erhältlich, mit denen man überall empfangsbereit ist. Meine persönliche "Evaluierung" dieses Artikels: Ein schönes Gerät, das ich seit der letzten Fussball WM nicht mehr missen möchte. Besonders praktisch finde ich den AV-Eingang. Im Urlaub schließe ich meinen Camcorder und die Digitalkamera daran an, mein Sohn bevorzugt sein Nintendo- oder Playstation.

Wir freuen uns, dass die Prämien, die die Teilnehmer unserer Veranstaltungen für ihren Weiterbildungsfleiß und ihre Treue zu unserer Firma belohnen sollen, diesen hohen Anklang finden. Was aber meiner Ansicht nach nicht bedeutet, dass die anderen Club-Angebote weniger relevant sind.

2. Diskussionsforum

Überraschend hoch ist auch der Zugriff auf das Diskussionsforum. Denn nach den Prämienseiten wird das Diskussionsforum am häufigsten genutzt, zeigt die Statistik. Die "stille" Beteiligung steht dabei jedoch noch überproportional hoch über den geposteten Beiträgen. Dabei sollte in unserem Club dasselbe Prinzip gelten, wie auch in unseren Seminaren: Man kann durch Fragen und Diskussionen nur gewinnen, niemals verlieren! Aber ich denke, das wird schon noch mit der Zeit.

3. Online-Glossar

Der große Newcomer im letzten Monat war jedoch das Online-Glossar, das mit Anregungen und Ergänzungen von Mitarbeitern unseres Teams unter meiner Federführung für Sie erarbeitet wurde. Obwohl erst seit Anfang September online sind innerhalb der ersten Wochen so viele Abfragen erfolgt, wie bei den Prämienseiten in einem ganzen Monat. Mit dieser nützlichen Unterstützung für den Berufsalltag haben wir wohl ins Schwarze getroffen. Und Sie können dabei mitwirken: Wir bieten Ihnen die Möglichkeit über ein Formular neue Begriffe vorzuschlagen. Ich möchte mich an dieser Stelle herzlich bei all denjenigen bedanken, die das auch schon getan haben. Zusammen werden wir das Glossar auch weiter beackern, damit es umso mehr Früchte für uns alle trägt.

White Papers und Fachartikel

In unserer Rubrik White Papers und Fachartikel hat sich natürlich auch einiges getan. Neu hinzu gekommen sind diesmal Dokumente über das Layer 3 Switching, über 10 Gigabit Ethernet und auch über die aktuellen Redundanzverfahren.

Linksammlung

Im August dieses Jahres haben wir erstmals eine Linksammlung für die Themenbereiche "Ethernet", "Wireless LAN", "Voice over IP" und auch "Speichernetzwerke" eingeführt. Darin zeigen wir (bewertungsfrei) Informationsquellen auf, die unsere Seminare und Fachartikel gut ergänzen. Diesen Monat haben wir die Themengebiete "Industrial Ethernet" und "Netzwerk Management" aufgenommen. Auf den verschiedenen Linkseiten finden Sie dann wieder Verweise auf Gremien, Produkte, Hersteller, aber auch Grundlagen und viele weitere Ressourcen.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Wireless LAN: Technik, Planung und Betrieb, 28. - 30.10.02 in Köln

Das Seminar führt in die faszinierende Welt der 0ptischen Netze, die ausgehend von den Aufrüstungen der Carrier auch für die Bereiche SAN, LAN-Backbone, MAN und Access eine bisher ungeahnte Leistungsdimension erschließen.
Referent: Dr. Franz-Joachim Kauffels Preis: € 1.590,-- zzgl. MwSt.

Service Level Management in der Praxis, 28. - 30.10.02 in Köln

Das Seminar behandelt die Königsdisziplin des Netzwerk- und System-Managements: Service Level Management, wo die technischen und organisatorischen Fäden einer IT-Organisation zusammenlaufen und die zentrale Schnittstelle zwischen Betreibern und Anwendern innerhalb einer Firma oder zwischen externen Dienstleistern und Anwendern liegt.
Referenten: Heinz Hüsges und Martin Rother (Arxes NCC AG) Preis: € 1.590,-- zzgl. MwSt.

DNS -/IP-Design für Windows 2000 Active Directory, 04. - 06.11.02 in Bonn

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, Michael van Laak, Frank Neunzig Preis: € 1.590,-- zzgl. MwSt.

Internet Information Server in MS Backoffice, 05. - 06.11.02 in Bonn

Das Seminar baut Know-How auf, das einen sicheren Betrieb von IIS gewährleistet, ohne den das heutige und zukünftige Web Storage System kommt nicht auskommt.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.290,-- zzgl. MwSt.

Mobile und drahtlose Datenkommunikation, 05. - 06.11.02 in Bonn

Das Seminar zeigt, wie mobile und drahtlose Kommunikationstechniken für den Zugang zur Infrastruktur genutzt werden können, welche Grenzen aktuell bestehen und welche technischen Weiterentwicklungen in den nächsten Jahren zu berücksichtigen sind.
Referent: Dr. Simon Hoff (ComConsult Beratung und Planung) Preis: € 1.290,-- zzgl. MwSt.

Redundanzverfahren und Design-Konzepte von LANs, 11. - 13.11.02 in Bonn

Das Seminar vermittelt ausgerichtet auf das Client-Server, LAN und RZ-Umfeld Technologien, Methoden und Design-Alternativen zum Aufbau von Netzen im Umfeld steigender Verfügbarkeits-Anforderungen.
Referentin: Dipl.-Inform. Petra Borowka Preis: € 1.590,-- zzgl. MwSt.

Design Windows 2000 Active Directory, 11. - 13.11.02 in Bonn

Das Seminar vermittelt, unterstützt durch den Praxisbezug zu Projekten in diesem Umfeld, wie das Active Directory zu strukturieren ist und legt dabei großen Wert auf den Entwurf der strategischen Komponenten (Domäne, Standort).
Referenten: Markus Holländer, Michael van Laak, Frank Neunzig, ComConsult Beratung und Planung Preis: € 1.590,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 11. - 15.11.02 in Aachen

Das Intensiv-Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan, ComConsult Akademie Preis: € 1.990,-- zzgl. MwSt.

Neue Ethernet Technologien, 11. - 15.11.02 in Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke.
5 Referenten der ComConsult Beratung und Planung Preis: € 1.990,--zzgl. MwSt.

ITIL-Foundation Grundlagen-Seminar, 18. - 19.11.02 in Königswinter

Das Seminar, bei dem am 2. Tag das Foundation-Exam (Prüfgebühr: € 150,-- zzgl. MwSt.) abgelegt werden kann ist die Voraussetzung für die Weiterbildung zum Certifizierten Service Manager nach ITIL.
Referenten: Thomas Engelmann und Dipl.-Kfm. Dipl.-Wirt. Inform. Bernd Holtz (Maxpert AG) Preis: € 990,-- zzgl. MwSt.

Optimale Netzstrukturen für hochverfügbare Serverfarmen, 18. -20.11.02 in Bonn

diskutiert die bestehenden Alternativen in der Anbindung von Servern und Speicher an Netzwerke. Denkbare Architekturen werden speziell unter dem Blickwinkel Performance, Verfügbarkeit und Betrieb gegenüber gestellt und bewertet.
Referent: Dr. Behrooz Moayeri (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

IP-Wissen für die Praxis, 18. -20.11.02 in Königswinter

Das Seminar bietet Grundlagen, Tipps und neueste Entwicklungen und vermittelt praxisnah die für den Betrieb von IP-Netzen notwendigen Basis-Kenntnisse.
Referenten: Dipl.-Inform. Oliver Flüs und Dipl.-Inform. Andreas Meder (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Internetworking, 18. -22.11.02 in Aachen

Das Seminar vermittelt die technischen und methodischen Kenntnisse zur erfolgreichen Strukturierung von Netzwerken mit Switching und Routing wobei Grundlagen-Kenntnisse Lokaler Netzwerk-Technologien erforderlich sind.
Referentin: Dipl.-Inform. Petra Borowka — Preis: € 1.990,-- zzgl. MwSt.

Moderne Datenkommunikation: Durchblick im Netzwerk, 18. -22.11.02 in Aachen

Das Intensiv-Seminar vermittelt Techniken, Verfahren und Systeme der Datenkommunikation für Ein- und Umsteiger. Der Schwerpunkt liegt auf dem erfolgreichen Einsatz der Internet/Intranet-Technologien.
Referent: Dr. Franz-Joachim Kauffels — Preis: € 1.990,-- zzgl. MwSt.

Exchange 2000 Server, Active Directory und Backoffice, 20. -22.11.02 in Köln

Das Seminar befasst sich mit der Implemen-tierung von Exchange 2000 Server im Kontext des Windows 2000 - Active Directory Designs. Es werden Grundkenntnisse über Active Directory und Messaging vorausgesetzt.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) — Preis: € 1.590,-- zzgl. MwSt.

IT Asset-Management wertschaffend einsetzen, 25. -26.11.02 in Bonn

Das Seminar bietet anhand von Analysten-aussagen und Studien einen Überblick der zukünftigen Herausforderungen an ganzheitliches IT-Asset Management und die hieraus entstehenden Kosteneinsparpotentiale.
Referent: Dr. Roger H. Jakobs (ComConsult Kommunikationstechnik) — Preis: € 1.290,-- zzgl. MwSt.

Migration zu Windows 2000 Active Directory, 25. -26.11.02 in Bonn

Das Seminar vermittelt die grundsätzlichen Migrationsansätze und welche Tools in welcher Form dabei eingesetzt werden können.
Referenten: Markus Holländer, Dipl.-Ing. Michael van Laak — Preis: € 1.290,-- zzgl. MwSt.

OSPF und VRRP optimal konfigurieren, 25. -28.11.02 in Aachen

Das Seminar vermittelt die notwendigen Kenntnisse für die Migration und den erfolgreichen Betrieb von OSPF Netzen durch Live-Vorführungen unter Einsatz von Produkten führender Hersteller. Für ein umfassendes, Layer 3 basiertes Redundanzkonzept ist Router-Redundanz unverzichtbar. Optional kann am 4. Tag **1 Übungstag** (mit Übungstag € 1.990,-- zzgl. MwSt.) gebucht werden.
Referent: Markus Schaub (ComConsult Akademie) — 3 Tage ohne Übungstag € 1.590,-- zzgl. MwSt.

Sicherheitslösungen für vernetzte IT-Umgebungen, 25. -29.11.02 in Bonn

Das Seminar beschäftigt sich mit modernen Sicherheitslösungen für den Internet-Zugang, das Mail-System, die Server, die Clienten und das Netz. Referenten: Das IT-Sicherheits-Team der ComConsult Beratung und Planung — Preis: € 1.990,-- zzgl. MwSt.

Ethernet in der Industrie, 25. -29.11.02 in Aachen

Das Seminar das notwendige Wissen, um Ethernet-Netzwerke in industriellen Umgebungen planen und einsetzen zu können. Bisherige "Industrial Ethernet"-Lösungsansätze werden mit herstellerspezifischen (Feld-)Bussystemen verglichen.
Referenten: Dipl.-Ing. Roland Moos, Dipl.-Ing. Hartmut Kell — Preis: € 1.990,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars | Name | Vorname

Termin | Firma, Abteilung | Position, Funktion

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel | Straße | PLZ, Ort

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** | Telefon | Fax

eMail | Unterschrift

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen.

Die Spielregeln:

Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Netzwerk Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her.

Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung.

Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Hub

Hirschmann Modell: ASGE 1 RE, Anzahl 20, Preis 80 EUR, Bemerkung: Hubs sind sehr gut einsetzbar in der Industiellen Ethernet Kommunikation (Automatierungstechnik) für Twisted-Pair und Fiberoptische Übertagungsstrecken mit 10 Mbit zB. als Siemens OLM Diverse Interfacekarten wie OYDE,UYDE,CYDE., Anzeigen-Nr. B20901

IBM Modell: 8230-013, Anzahl 15, Preis 175 EUR, Bemerkung: Alle Geräte sind geprü und in sehr gutem Zustand. Anzeigen-Nr. B20903

Gebote

Router

Cabletron/Enterasys Smart Switch Router 2000, SSR-2-B, Anzahl 1, Preis VB, mit oder ohne Zusatzmodule, Anzeigen-Nr. B20805

Cabletron/Enterasys Smart Switch Router 8000/8600 SSR-8/SSR-16, Anzahl 1, Preis VB, mit oder ohne Zusatzmodule, Anzeigen-Nr. B20804

Cisco Modell 2503, Anzahl 1, Preis VB, Anzeigen-Nr. B20801

Switch/Brücke

IBM Modell: 8229 TR/TR, Anzahl 20, Preis 80 EUR, Bemerkung: Die IBM Brücken 8229 Tokenring/Tokenring sind geprüft und in gutem Zustand Brücke kann umgerüstet werden zu Tokenring / Ethernet Umrüstkosten: Auf Anfrage, Nr. B20902

DEC FDDI Gigaswitch, Anzahl 2, Preis sehr, sehr günstig, VB, Bemerkung: je Switch mit folgenden Linecards bestückt: 3x DEFGL-AA (Rev. F) FDDI Linecard, dual 4x DEFGL-AB (Rev. A, F) FDDI Linecard, single als Reservematerial einsetzbar, anstelle teurer Wartung! Anzeigen-Nr. B20905

Bay/Nortel Chassissystem 3000, Switch 28104/28115, Anzahl 1, Preis VB, Anzeigen-Nr. B20806

Cabletron/Enterasys Smart Switch 6000, Anzahl 1, Preis VB, mit oder ohne Zusatzmodul, Anzeigen-Nr. B20803

Cisco Modell WS-C2924C-XL, Anzahl 1, Preis VB, Anzeigen-Nr. B20802

Sonstiges

Cabletron/Enterasys Funk-LAN-Equipment, Anzahl diverse, Preis VB, Roam About(Access Point, NIC, Antennen, Zubehör), Anzeigen-Nr. B20807

HP ATM/OC-3 Probe Modell J3919A, Anzahl 4, Preis 900,- EUR/Stck., exklusive Versand, Anzeigen-Nr. B20808

Gesuche

Adapter

Cisco Modell AS5260, Anzahl 1, Preis nach Absprache, Bemerkung: CISCO-Access Router AS5260 inklusive 2Mbit/s Primary-Rate Interface AS52_E1_U_60DM (30 Channels) und/oder ausschließlich Interface ohne Route, Anzeigen-Nr. S20701

Router

BinTec Modell: Brick-XM, Anzahl 1, Preis VB, Anzeigen-Nr. S20904

Fax an ComConsult
02408/955-399

☐ **Ich suche**

☐ **Ich biete**

☐ **Antwort auf Anzeigen-Nr.** ☐ _____

Produkt/Komponente/Release/Software

_____

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon

_____

Fax

_____

eMail

Weitere Anzeigen finden Sie auf dem Web-Server der ComConsult Akademie

www.comconsult-akademie.de