
Wireless LAN, alle wissen, dass es nicht sicher ist, alle wollen es, was nun ?



Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen

Dipl.-Math. Wilfried Gericke
IT-Verantwortlicher

Wireless LAN, alle wissen, dass es nicht sicher ist, alle wollen es, was nun ?

Inhalt:

Motivation

WLAN-Sicherheit

Wireless-Gefahren

Wireless LAN Lösungen

Motivation

Die Werbung preist Wireless LAN Lösungen als eine zukünftige Standardtechnologie an, Client an ein vorhandenes Netz anzubinden.

Wer schon einmal Wireless LAN Technologie benutzt hat oder schon einsetzt, ist begeistert (siehe Einsatz auf den letzten beiden DECUS München Symposien)

Die Preise für die WLAN Komponenten sind attraktiv.

Was spricht dagegen ?

Sicherheitsprobleme (ein schneller Notebook kann in kurzer Zeit effektive Angriffe gegen die WLAN Sicherheit starten)

Die folgenden Betrachtungen finden aus der Anwendersicht statt !

Seite 3

WLAN-Sicherheit

Warum ein Wireless LAN einen gewissen Grad an Sicherheit bieten soll, ist nicht Gegenstand des Vortrages.

Im Vortrag selbst werde ich mich auf WLAN Anwendung in einer überschaubaren Umgebung beschränken, wie z.b.

Home-Umgebung

eine Gebäudeumgebung auf einem zusammenhängenden Grundstück

Aus den bisher selbst gemachten Erfahrungen werde ich berichten.

Seite 4

WLAN-Sicherheit

IEEE802.11-Daten				
IEEE	802.11	802.11a	802.11b	802.11g
Frequenz / Ghz	2,4-2,4835 (IR)	5,15 - 5,25 5,25 - 5,35 5,725 - 5,825	2,4-2,4835	2,4-2,4835
Band	ISM 1997	UNII 1999	ISM 1999	ISM 2003
Datenrate (Mbit) pro Kanal	1 2	6, 9, 12, 18 24, 36, 48, 54	11, 5, 5 2, 1	54, 36, 33, 24 22, 11, 6, 5, 5 2, 1
Kompatibilität	802.11	Wi-Fi5	Wi-Fi	Wi-Fi < 11 Mbit

Seite 5

WLAN-Sicherheit

Reichweiten werden bestimmt durch Abstrahlleistung, Antennen-Technik und Örtlichkeit

In der EU ist die Abstrahlung auf 100mW EIRP begrenzt, d.h.

ca 30 m in Gebäuden (abhängig von der Qualität der Wände)

ca 300 m außerhalb von Gebäuden

Die Reichweite kann durch externe Antennen erheblich gesteigert werden

Seite 6

WLAN-Sicherheit

Es stehen mehrere Kanäle zur Verfügung (EU: 13)

Im 802.11b Standard gibt es drei komplett überlagerungsfreie Kanäle

z.B. 1 – 6 – 11

Störquellen: Mikrowellenherde, Bluetooth, Schnurlos-Telephon, Haussprechanlagen (alle bei 2,4 Ghz)

Zugriffsmethoden:

IEEE 802.11 DFC -> CSMA/CA

Seite 7

WLAN-Sicherheit

Integrität -	Es kommt das an, was abgesendet wurde
Vertraulichkeit -	Es können nur berechtigte Empfänger lesen
Authentifikation -	Sender und Empfänger wissen, mit wem sie kommunizieren
Autorisierung -	Darf derjenige das, was er tun will, auch wirklich ?
Protokollierbarkeit -	Kann nachgewiesen werden, dass jemand etwas gesendet hat ?
Verfügbarkeit -	Ist überhaupt die notwendige Performance gegeben ?

Seite 8

WLAN-Sicherheit

WLAN-Signale tauchen überall auf, leider oft auch dort, wo man sie nicht haben will

IT-Manager schöpfen die Schutzmöglichkeiten nicht immer aus.

Sicherheitsmechanismen der Hersteller sind oft umständlich oder verwirrend für den Anwender.

WLAN-Sniffing : Nur ein Sport ?

Hervorragende Hackertools sind im Internet frei verfügbar.

Hersteller sagen: prinzipiell ist es möglich, ein WLAN ausreichend abzusichern.

Seite 9

WLAN-Sicherheit

Wo habe ich als Anwender Einfluss auf die Sicherheit der Übertragung ?

SSID System Set Identifier (Name des Wireless Netzwerkes)

6-Byte großes Code Word

wird im Klartext übertragen

Client (Notebook, PC, PDA,..) kann sich am Access Point nur anmelden, wenn der SSID übereinstimmt (Broadcast SSID = off)

SSID „ANY“ funktioniert, wenn Broadcast SSID = on am Access point bei z.B. öffentlichen Zugängen

Seite 10

WLAN-Sicherheit

Shared Key Identification

Zur Sicherung des Datentransfers zwischen Client und AP wird eine 64- oder 128-Bitverschlüsselung eingesetzt (muss auf beiden Seiten händisch eingesetzt werden).

Da der Schlüssel in Wirklichkeit nur 40 bzw. 104 Bits lang ist (Rest Factory set), sollte nach Möglichkeit immer die stärkere Verschlüsselung eingesetzt werden.

Wie ist der Access Point gesichert ?

Kann jeder über das Netz oder über USB den Access Point konfigurieren ?

Kann jeder an das Gerät (eigentlich sollten nur die Antennen sichtbar/verfügbar sein) ?

Seite 11

WLAN-Sicherheit

MAC-Filterung

Durch Filterung der MAC-Adressen (nicht jeder AP kann dies, dann sollte man einen preiswerten Router/Switch mit integriertem AP einsetzen), kann eine weitere „Behinderung“ möglicher Eindringlinge erzeugt werden!

Natürlich

- können MAC Adressen auf einigen Karten überschrieben werden
- sind durch Brute Force MAC-Adressen knackbar
- ist die Pflege von MAC-Adressen in großen Umgebungen aufwändig

Seite 12

WLAN-Sicherheit

VPN und IPSec

Man kann auf dem Standpunkt stehen, dass es eigentlich nicht so schlimm ist, wenn bekannt ist, dass jemand mit einem Client XY mit einem Knoten YZ kommuniziert.

Nur der Inhalt der Kommunikation soll geheim bleiben.

Dann ist der Einsatz von VPN und vielleicht auch IPSec eine gute Unterstützung.

Mit Hilfe von VPN und IPSec werden auch sichere Verbindungen über das öffentliche Internet aufgebaut.

Seite 13

WLAN-Gefahren

Bekanntlich ist nur der Rechner sicher, der nicht eingeschaltet in einem Panzerschrank steht.

ein Client strahlt ab

ein Client selbst kann die Schwachstelle in einem Netz sein (nicht nur das Netz)

Ist der Rechner Virenverseucht ?

Hat er ein trojanisches Pferd in seinem Speicher ?

Besitzt er wie z.B. ein PDA seine Sicherheit ?

Hat der Client eine Wireless Tastatur, die nicht den Datentransfer verschlüsselt ?

Seite 14

WLAN-Gefahren

Wahl der Passworte bei der WEB-Verschlüsselung ?

Wer ändert bei einem funktionierenden WLAN die Passworte bei der WEP-Verschlüsselung?

Seite 15

WLAN-Lösungen

Der Schutz der Daten sollte nicht teurer sein als die Daten Wert sind !

Der Einsatz von WLAN-Technologie bringt nicht nur in vielen Anwendungsfällen einen Komfortgewinn für den Anwender, sondern auch auf der baulichen Seite sind merkliche Kosteneinsparungen möglich. Auch auf Seiten der Arbeitssicherheit, z.B. keine Stolperkabel, sind Gewinne möglich.

Bei der Wahl der Komponenten sollte auf Qualität geachtet werden !

Seite 16

WLAN-Lösungen

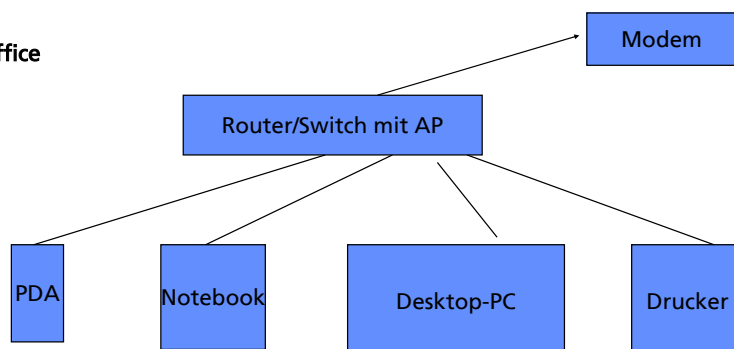
3 verschiedene Szenarien

- home office
- WLAN-Zugang für Gäste
- WLAN-Zugang für Mitarbeiter

Seite 17

WLAN-Lösungen

Home Office



Seite 18

WLAN-Lösungen

WLAN-Zugang für Gäste

Welche Internet-Dienste benötigt der Gast ?

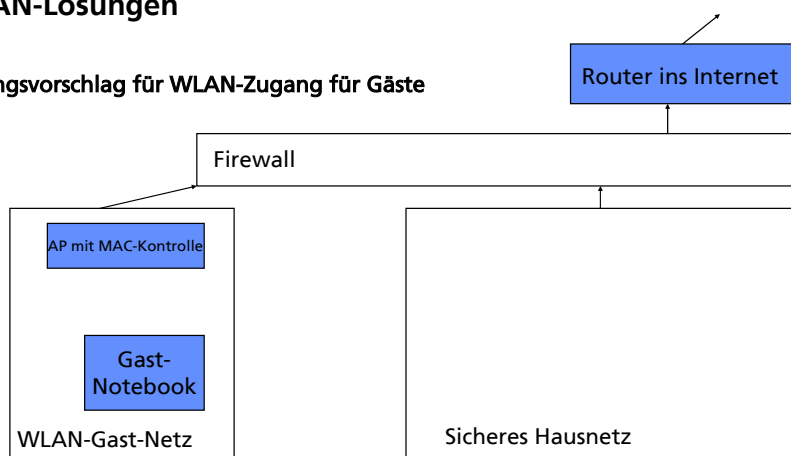
Ist es vielleicht günstiger, dem Gast einen vorkonfigurierten Notebook zur Verfügung zu stellen ?

Auch ein Gast sollte geschützt sein !

Seite 19

WLAN-Lösungen

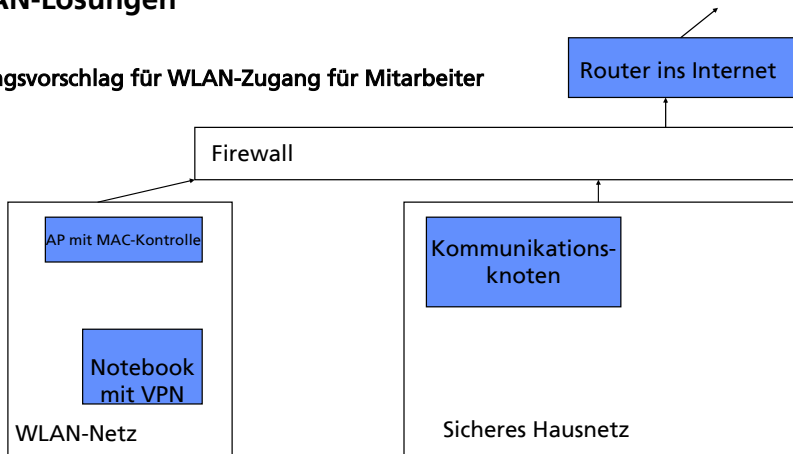
Lösungsvorschlag für WLAN-Zugang für Gäste



Seite 20

WLAN-Lösungen

Lösungsvorschlag für WLAN-Zugang für Mitarbeiter



Seite 21

WLAN-Lösungen

Abschalten der Access Points außerhalb der möglichen Dienstzeit !

Wir wollen den Hackern die Arbeit so schwer wie möglich machen !

Seite 22

Informationsquellen:

Grdschutzhandbuch des BSI

Vortrag von Peter Schürholt auf dem DECUS München Symposium 2003 3B07

Vortrag von Thorsten Kocher auf dem DECUS München Symposium 2003 1F02

Vortrag von Frank Bartel auf dem DECUS München Symposium 2003 3B01

Christoph Bronhold auf dem DECUS München Symposium 2003 1B06