WLAN

Präsentation von Frederik Wille, David Kirchhausen Monteiro und Joshua Stock

Gliederung

1. Einleitung (Joshua)
    1. Was ist WLAN?
    2. WiFi, WLAN: Begriffsklärung
    3. Geschichtlicher Hintergrund

2. Funktion (David)
    1. Infrastruktur-/ Ad-hoc-Modus
    2. Beacon
    3. Signal

Gliederung (cont.)

3. Technisch (Frederik)
    1. IEEE
    2. IEEE 802.11 a/b/g/n/ac
    3. Übertragungsraten, Frequenzen
    4. Hardware
4. Sicherheit & Verschlüsselungen (Joshua)
    1. WEP, WPA & WPA2
    2. Gesundheit
5. Zusammenfassung
6. Vorführung

WLAN – Was ist das?

- Lokales Funknetz
- Meist Standard der IEEE-802.11 Familie
- Erweiterung von Ethernet-Netz

WLAN

- Anforderungen:
  - Hoher Durchsatz an Daten
  - Viele mögliche Clients
  - Interkonnektion mit leitungsgebundenen Netzen
  - Zuverlässigkeit und Sicherheit
  - Lizenzfreie Frequenzen
  - Dynamische Konfiguration

WLAN, Wi-Fi - Begriffsklärung

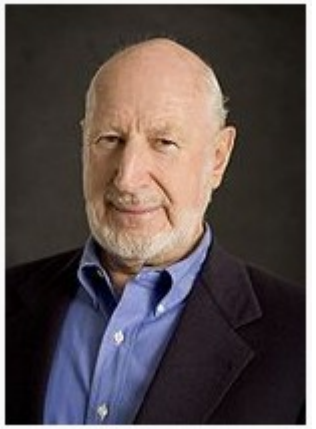
- WLAN bezeichnet Funknetzwerk
- Wi-Fi steht für den Funkstandard

- Wi-Fi Alliance wurde 1999 gegründet
  - Zertifiziert IEEE-802.11 Standards
  - Stellt Interoperabilität sicher
  - Soll Inkompatibilitäten vermeiden

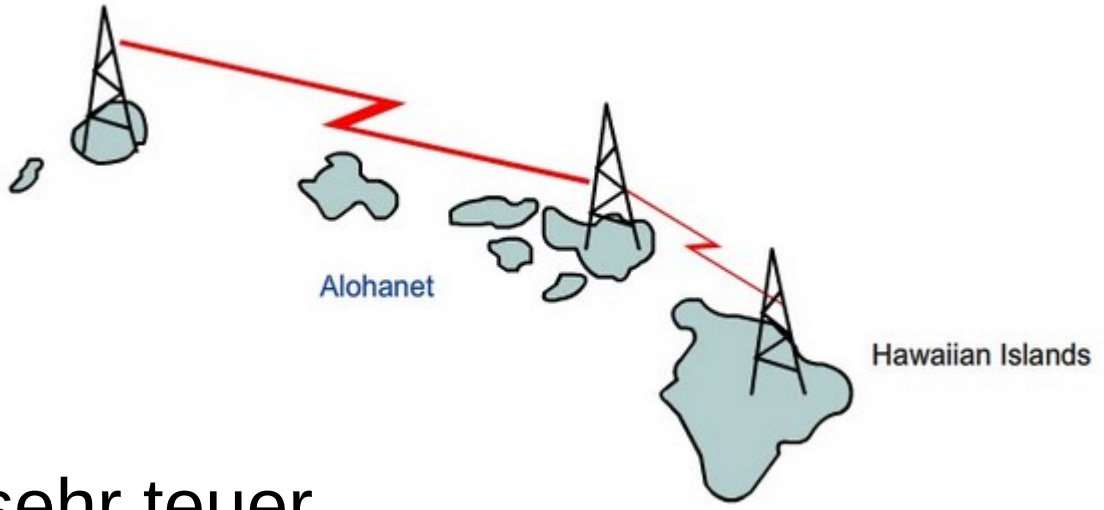
Wi-Fi Alliance

- Testet Komponenten nach eigenen Richtlinien
- Produkte, die Prüfung bestehen, dürfen Logo tragen
- Gebühr für jede Geräteprüfung

Geschichtlicher Hintergrund



- Anfänge 1970
- Von Norman Abramson
  - „ALOHAnet“: Vernetzung von Inseln um Hawaii mit Universität Honolulu
  - Verband Zentral-rechner mit 7 Stationen



- Hardware anfangs sehr teuer

Geräte

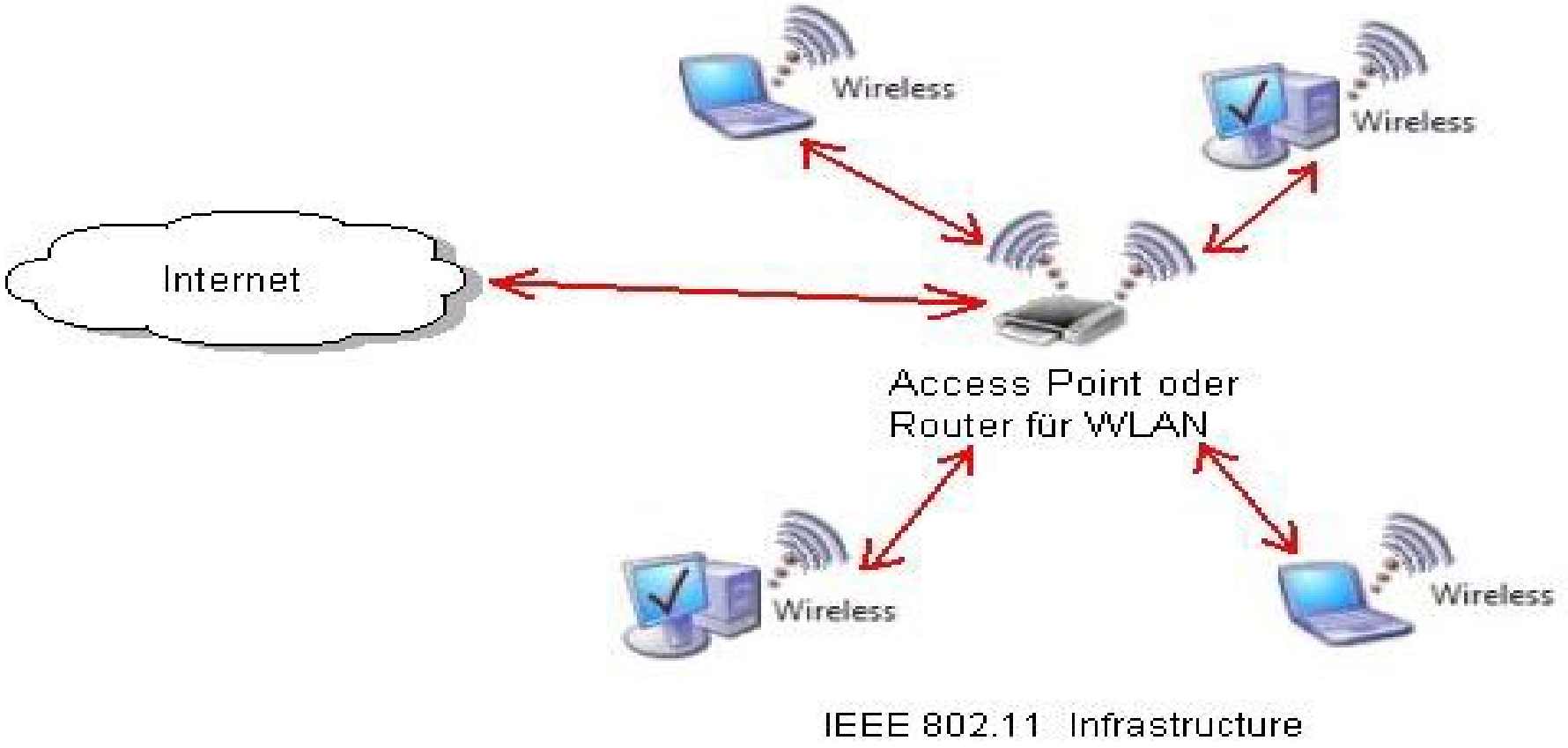
- Access Points
  - Router
  - Repeater
- Klienten
  - Handys
  - Laptops
  - PCs

Infrastruktur - Modus

Infrastruktur-Modus:

- Wireless Acces Point und Router
- Client

Infrastruktur - Modus



Infrastruktur - Modus

- Wireless Acces Point oder Router bilden Basis
- Senden von „Beacons“: Grundlage für Verbindung

Beacon

Beacon:

- Kleines Datenpaket
  - Enthält Informationen über das Netzwerk
  - Wird in festen Intervallen verschickt
  - Wird mit 1MBit/s versendet
  - Kann auch Aufschluss über Signalstärke geben
  - Garantiert keine stabile Verbindung

Beacon

Beacon enthält grundsätzlich 3 Informationen:

- Netzwerkname (SSID)
- Liste unterstützter Übertragungsraten
- Art der Verschlüsselung

Beacon

- Broadcasting kann deaktiviert werden
  → Router wird unsichtbar
- Clienten nehmen aktiv die Verbindung auf
- gespeicherten Netzwerknamen suchen

- Risiko: Simulation des Netzwerkes durch Angreifer

Infrastruktur – Modus

- WLAN Sicherungsschicht: gleiche Adressierung wie Ethernet
- AccessPoint kann leicht Verbindung zu kabelgebundenen Netzen herstellen
- Es muss zwischen 802.11 (WLAN) und 802.3 (Ethernet) konvertiert werden

Verbindungsaufnahme

- IEEE 802.11: drei verschiedene Frame-Typen
- Control-, Management- und Daten-Frames
- WLAN-Adapter müssen nicht alle verstehen
- AccesPoints müssen alle verstehen

Verbindungsaufnahme

Verbindungsaufnahme

- Ethernetpaket wird in WLAN-Paket eingebettet
- Ethernetpaket kann dabei größer sein als normal


Wi Fi
Wireless Network
Wireless Access Point
DSL/Cable
Local Network

Infrastruktur - Modus

- Aufbau größerer WLANs mit mehreren Basisstationen führt in der Praxis zu Problemen

Infrastruktur - Modus

- Frequenzbereich der Basisstationen überlappen sich
  - führt zu Störungen
- Kein Datenaustausch zwischen den Basisstationen

Infrastruktur - Modus

Lösungen :

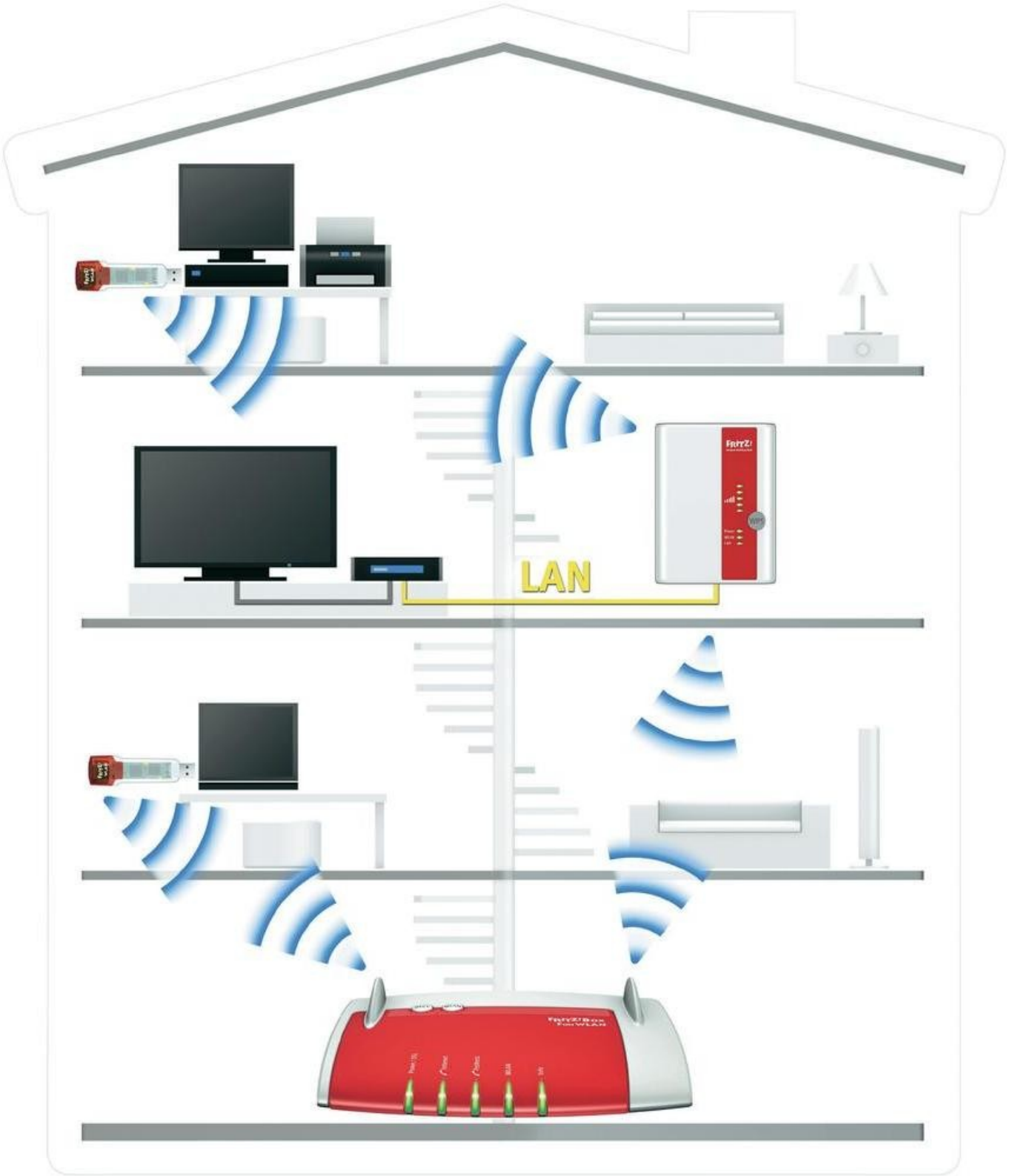
- → Verlagerung der Kontrollfunktion in Basisstation oder Netzwerk
- → Zentrale Instanz kann Frequenzen und Übertragunsraten besser steuern

Infrastruktur - Modus

- Basisstation verliert somit Teil ihrer Funktion
- Muss mit zentraler Instanz kommunizieren können
- An entsprechenden Geräteklassen und Protokollen wird gearbeitet

Infrastruktur - Modus

- Offene Standards wie z.B. Lightweight Asses Point Control
- Problematik: Welches Gerät übernimmt welche Funktion?


LAN

Ad-hoc

- Keine zentrale Station
- Alle sind gleichwertig
- Leicht und schnell aufzubauen

Ad-hoc

IEEE 802.11 ad hoc Netzwerk

Ad-hoc

Vorraussetzungen:

- Alle Stationen benutzen die gleiche SSID
- Optional: die gleiche Verschlüsselung

Ad-hoc

- Kein Acces Point mit koordinierender Funktion
- Endgeräte müssen diese übernehmen

Ad-hoc

- Weiterleiten von Datenpaketen zwischen einzelnen Stationen ist nicht vorgesehen
- Auch nicht ohne Weiteres möglich

Ad-hoc

- Keine Netzwerk-Überblicks-gebenden Informationen werden ausgetauscht
- Nur kleine Reichweite
- Nur für geringe Anzahl von Endgeräten sinnvoll
  - In unmittelbarer Nähe zueinander

Ad-hoc

- Routing-Fähigkeiten auf den Endgeräten
- Aufwertung: Mobiles Ad-hoc Netzwerk

Moblies Ad-hoc

- Viel Forschung
  - Experimentelle Protokolle
  - Standardisierungsvorschläge
  - Kommerzielle Lösungen

Institute of Electrical and Electronics Engineers

- Kurz IEEE (gespr.: I tripple E)
- Berufsverband
- Gegründet 1963

IEEE Standard 802

- Standardisierung des LAN und MAN
- 25 Hauptstandards
- OSI-Modell: Data Link und Physical Layer
- z.B.: Ethernet(.3), WLAN(.11), Bluetooth(.15.1)

OSI Schichtenmodell

OSI-Schicht		Einordnung	DoD-Schicht	Einordnung	Protokollbeispiel	Einheiten	Kopplungselemente
7	Anwendungen (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP LDAP NCP	Daten	Gateway, Content-Switch, Layer-4-7-Switch
6	Darstellung (Presentation)						
5	Sitzung (Session)						
4	Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme	
3	Vermittlung (Network)		Vermittlung	Punkt zu Punkt	ICMP IGMP IP IPsec IPX	Pakete	Router, Layer-3-Switch
2	Sicherung (Data Link)		Netzzugriff		Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)	Bridge, Switch
1	Bitübertragung (Physical)					Bits, Symbole, Pakete	Repeater, Hub

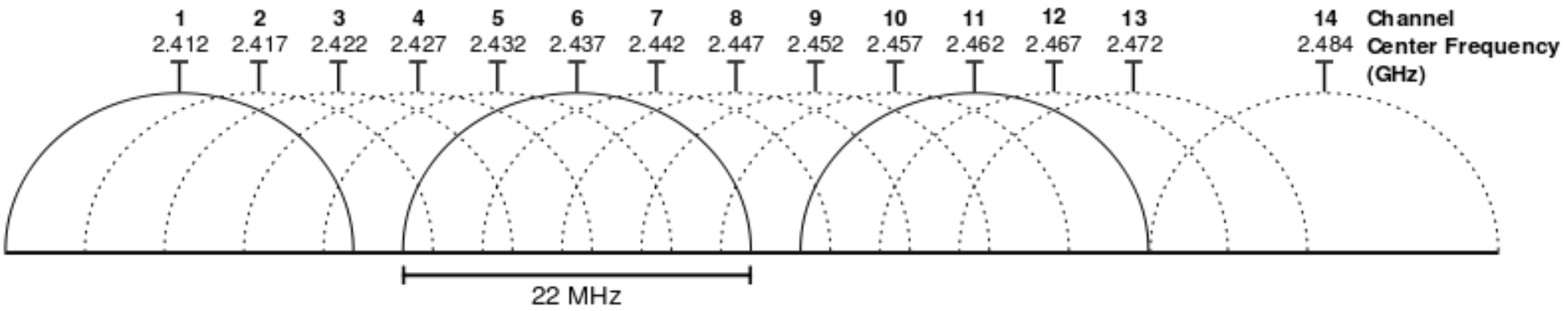
IEEE 802.11

- ISM-Bänder
- Unterstandards(z.B. b,g,n,ac)
- mehrere Kanäle
- CSMA/CA

802.11 Protokolle

TABLE 1: IEEE 802.11 PHY STANDARDS						
Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2013	802.11ac	5	80	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

Kanäle

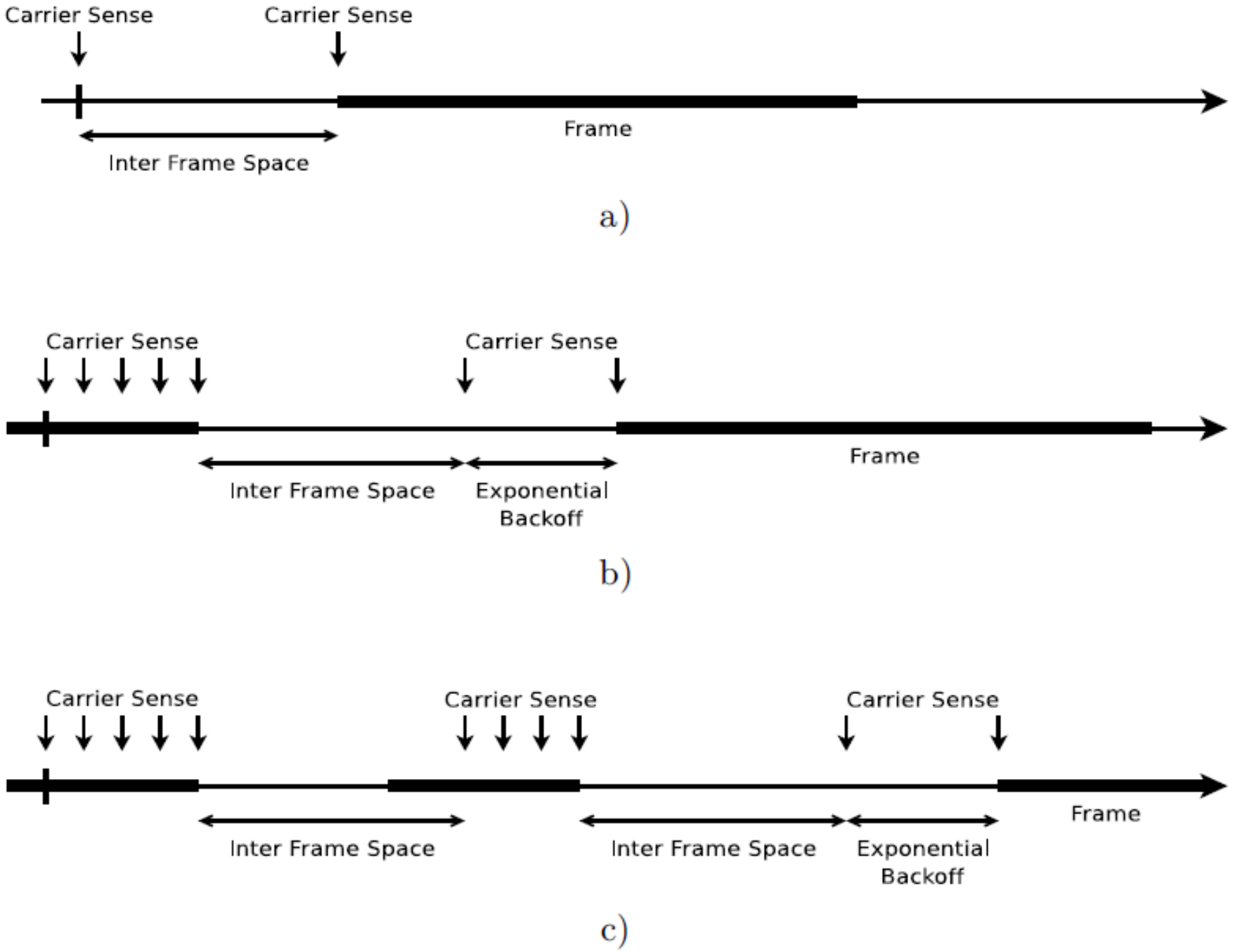

1 2.412
2 2.417
3 2.422
4 2.427
5 2.432
6 2.437
7 2.442
8 2.447
9 2.452
10 2.457
11 2.462
12 2.467
13 2.472
14 2.484
Channel
Center Frequency
(GHz)
22 MHz

802.11n

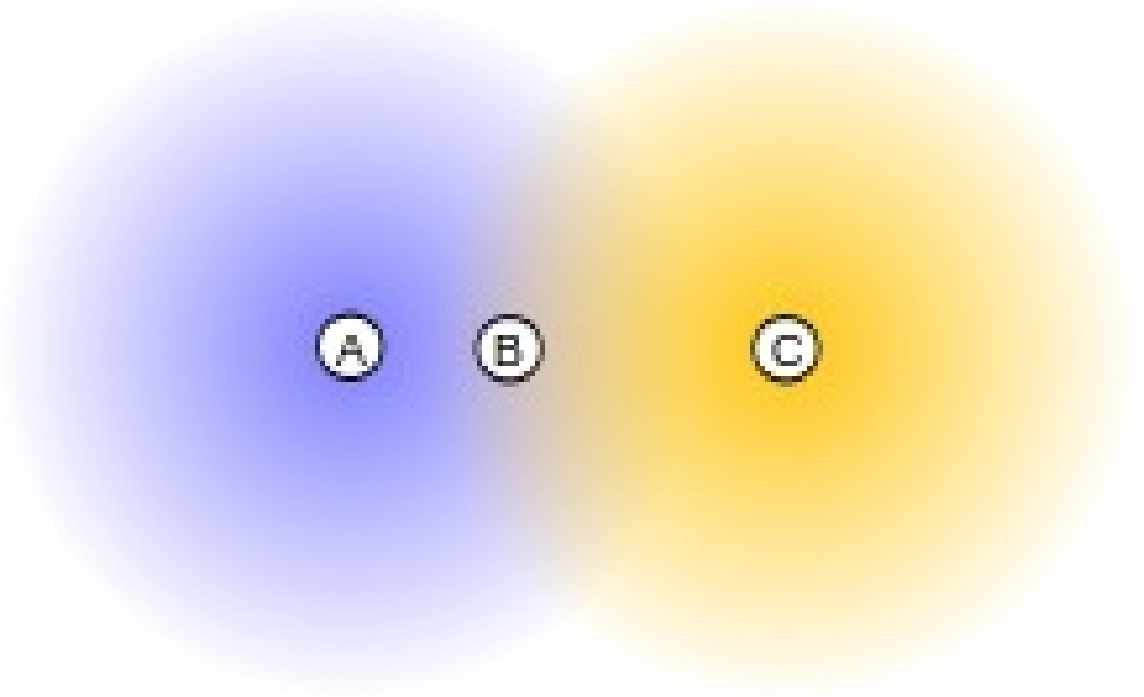
- 2,4 und 5Ghz Band
- Höhere Bandbreite
- MIMO Technologie
- Ab- und Aufwärtskompatibel
- Bis zu 600Mbit/s brutto

Carrier Sense Multiple Access/Collision Avoidance

- Kurz CSMA/CA
- CSMA/CD nicht für Funk geeignet
- CSMA: Erkennung der Kollision
- CA:
  - Verschickt alle Daten
  - Wartet auf Bestätigung


Carrier Sense
Carrier Sense
Frame
Inter Frame Space
a)
Carrier Sense
Carrier Sense
Frame
Inter Frame Space
Exponential
Backoff
b)
Carrier Sense
Carrier Sense
Carrier Sense
Frame
Inter Frame Space
Inter Frame Space
Exponential
Backoff
c)

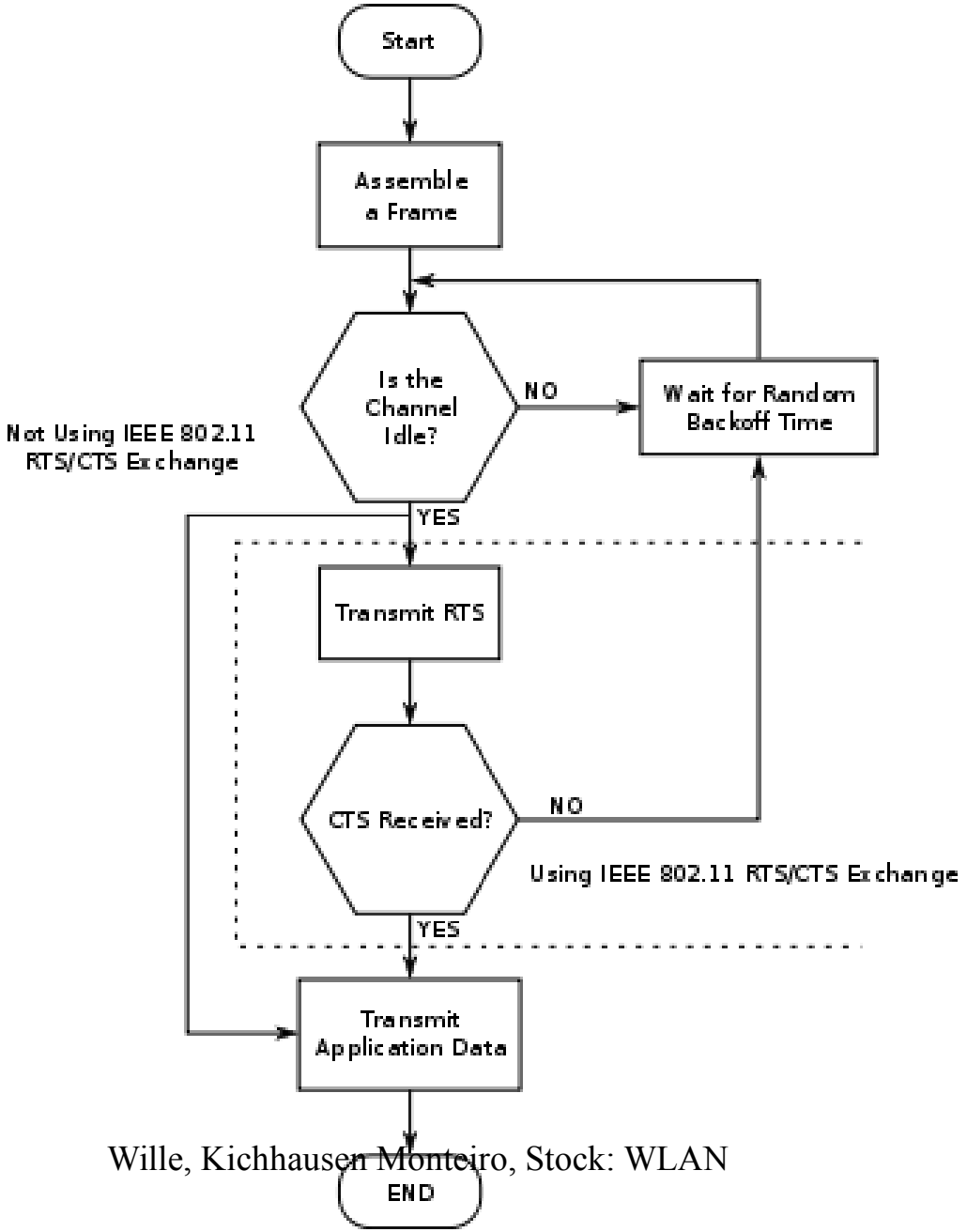
Hidden-/Exposed-Station-Problem



RTS/CTS

- Löst das Hidden-Station-Problem
- Verschickt „Request to Send“ Signal
- Schickt Daten erst bei Erhalt des „Clear to Send“ Signals

RTS/CTS


Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

Sicherheiten

- RC4
- WEP
- WPA/WPA2
- Gesundheit

RC4

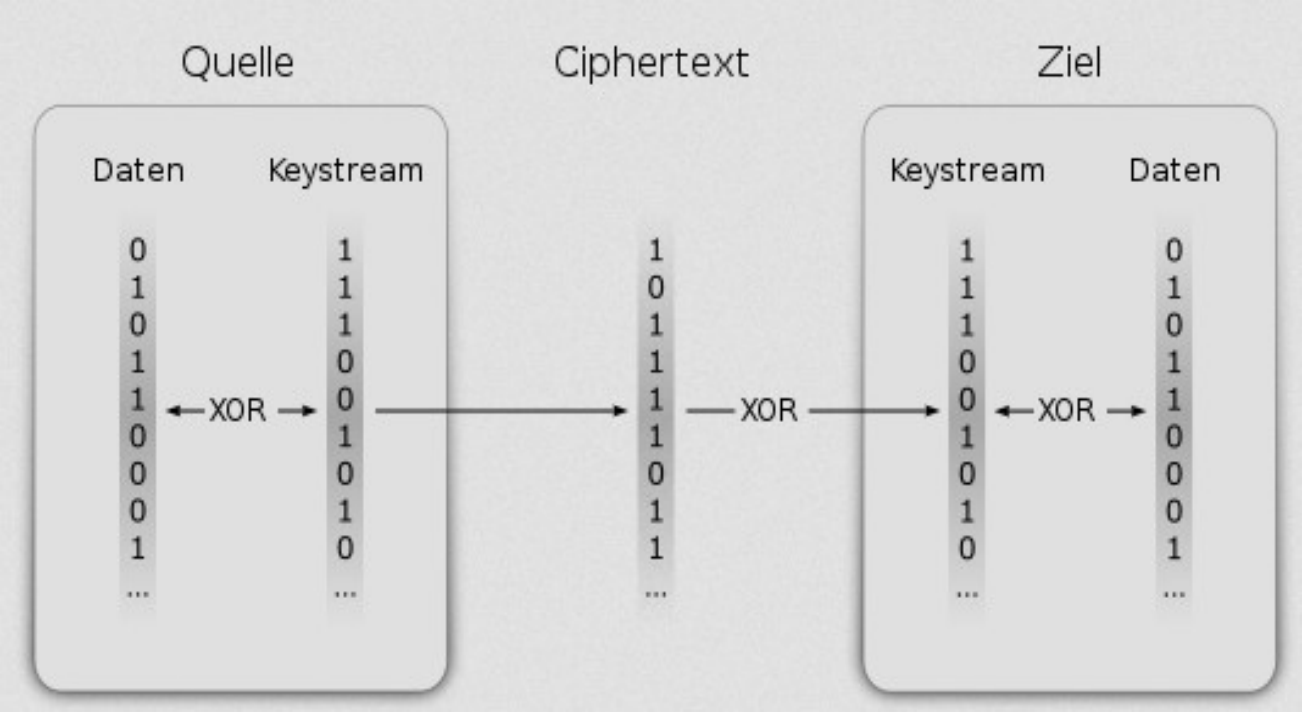
- Auch bekannt unter ARC4 / Arcfour
- Stromverschlüsselung
- Wird in HTTPS, SSH1, WEP und WPA verwendet
- Marke von RSA Security
- Veröffentlichung 1994

RC4: Funktionsweise

- Zufallsfolge wird aus einmaligem Schlüssel erzeugt
- Klartext anschließend Bit für Bit XOR-verknüpft
- Verwendung höchstwahrscheinlich unsicher

WEP

- Keystream = Schlüssel + Initialisierungsvektor IV
- Für jede Nachricht neuer IV



WEP Datenpakete

- Nutzdaten + 32-Bit Prüfsumme („Integrity Value Check“)

- Datenpaket: 32-Bit Prüffolge (mittels IV-WEP-Schlüsselkombination + Initialisierungsvektor) + verschlüsselte Daten

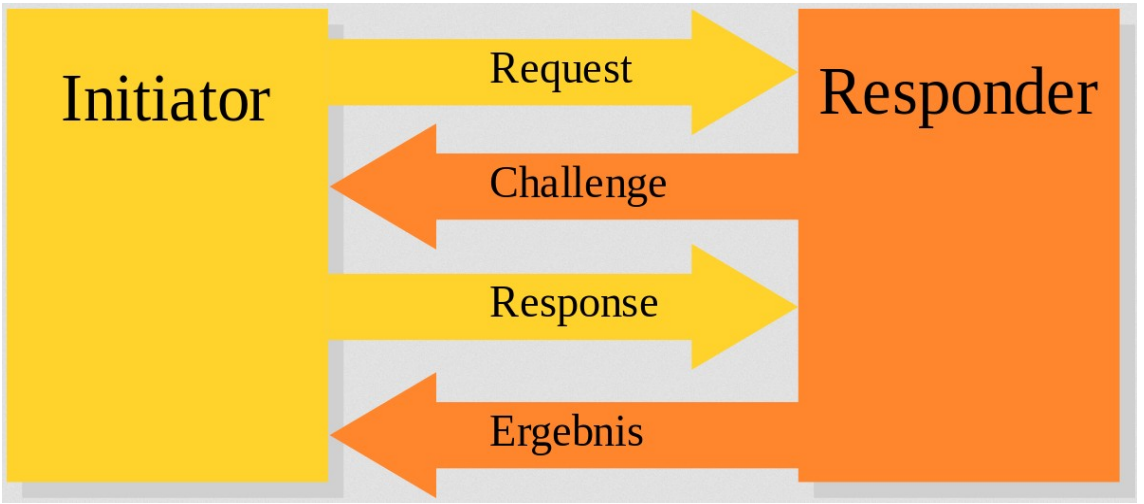
WEP - Angriffsmöglichkeiten

- Aktive Teilnehmer erleichtern den Angriff
- Mitlauschen des Gesamtverkehrs
- Daraus lässt sich unverschlüsselter IV ablesen

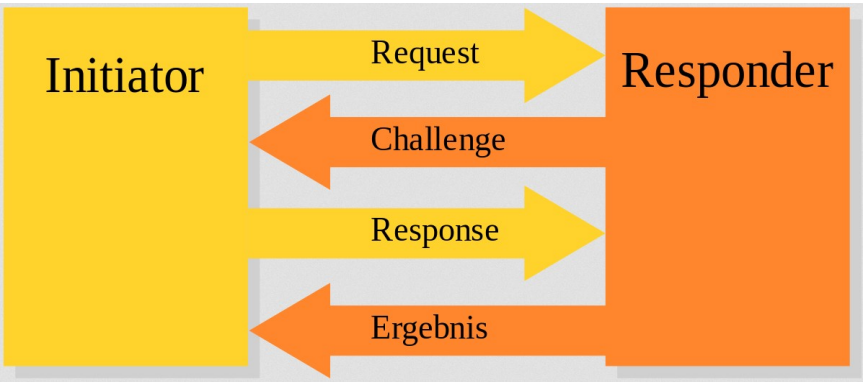
WEP - Angriffsmöglichkeiten

- Bei Shared Key Authentification:
- „Challenge Response System“
  - Server schickt Challenge
  - Client verschlüsselt und antwortet mit

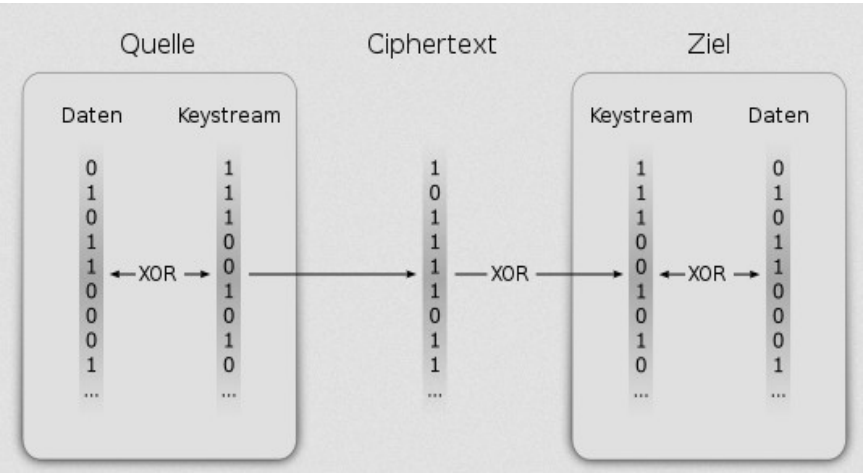
    IV1 + Ciphertext



WEP - Angriff



- Angreiferin Trudy
  - Hat Challenge1, IV1 und Ciphertext1 mitgelauscht
  - Errechnet sich mittels XOR den Keystream



  - Challenge2 beantwortet sie selbst:
  - Ciphertext2 = Challenge2 XOR Keystrem
  - Erfolgreiche Authentifizierung

Wi-Fi Protected Access (WPA)

- Pseudostandard, statt IEEE 802.11i
- Seit 2003
- Architektur von WEP + Temporal Key Integrity Protocol (TKIP)

WPA

- Durch TKIP: per-packet-key
  - dynamisch pro Paket ein 128-bit-Key

- Außerdem: Message Integrity Check

WPA2

- Implementiert IEEE 802.11i und
- integriert AES
  - Erweiterung von RC4
  - Blockchiffre
  - Einzelne Blöcke werden mit verschiedenen Teilen des Originalschlüssel verschlüsselt
- Authentifizierung: Hauptsächlich als PSK (Pre Shared Key)
  - „personal“

WPA2 Schwachstellen

- Unsichere Passwörter
  - Durch Brute-Force-Attacken zu knacken

- Sichere Passwörter:
  - Groß-/Kleinbuchstaben, Sonderzeichen, „sinnlos“
  - Size matters!! (Je länger, desto sicherer)
  - z.B. RM1gIJSNzivJ9uQB3MP

Gesundheit

- Von Anfang an Bedenken
  - Angeblich Schlaflosigkeit, Schwindel, Kopfschmerzen,...
- Langzeitstudien kaum möglich: zu junge Technologie
- Bisher keine einschlägigen, sich nicht widersprechende Studien

Zusammenfassung/Aussicht

- WLAN hat längst den Weg in unseren Alltag gefunden
  - Kaum noch wegzudenken
  - Relevanz und Verbreitung steigt weiter
  - Hardware wird immer günstiger

- Zukunft: Auch HDMI, USB, SATA über WLAN?
  - 802.11ad in Entwicklung

Vorführung

Quellen

- www.iept.tu-clausthal.de/fileadmin/homes/it-team/vortraege/WLAN.pdf
- IEEE Tabelle: http://electronicdesign.com/site-files/electronicdesign.com/files/archive/electronicdesign.com/content/content/74186/74186_table1.gif
- http://en.wikipedia.org/wiki/IEEE
- http://en.wikipedia.org/wiki/IEEE_802
- http://de.wikipedia.org/wiki/OSI-Modell
- DKR-Skript
- http://www.pcwelt.de/
- http://de.wikipedia.org/wiki/802.11n
- http://upload.wikimedia.org/wikipedia/de/b/b7/WEP-DPaket.PNG
- http://upload.wikimedia.org/wikipedia/de/5/53/WEP-Paket.PNG
- http://upload.wikimedia.org/wikipedia/commons/thumb/e/ed/WEP.svg/400px-WEP.svg.png