

WiFi

Basics & Security

Matthias Vallentin

vallentin@net.in.tum.de

Vorlesung “Internetprotokolle” SS06

Prof. Anja Feldmann, Ph.D.

Outline

- ▶ 802.11 (“WiFi”) Basics
 - ▶ Standards: 802.11{a,b,g,h,i}
 - ▶ CSMA/CA
- ▶ WiFi Security
 - ▶ WEP
 - ▶ 802.11i
 - ▶ DoS

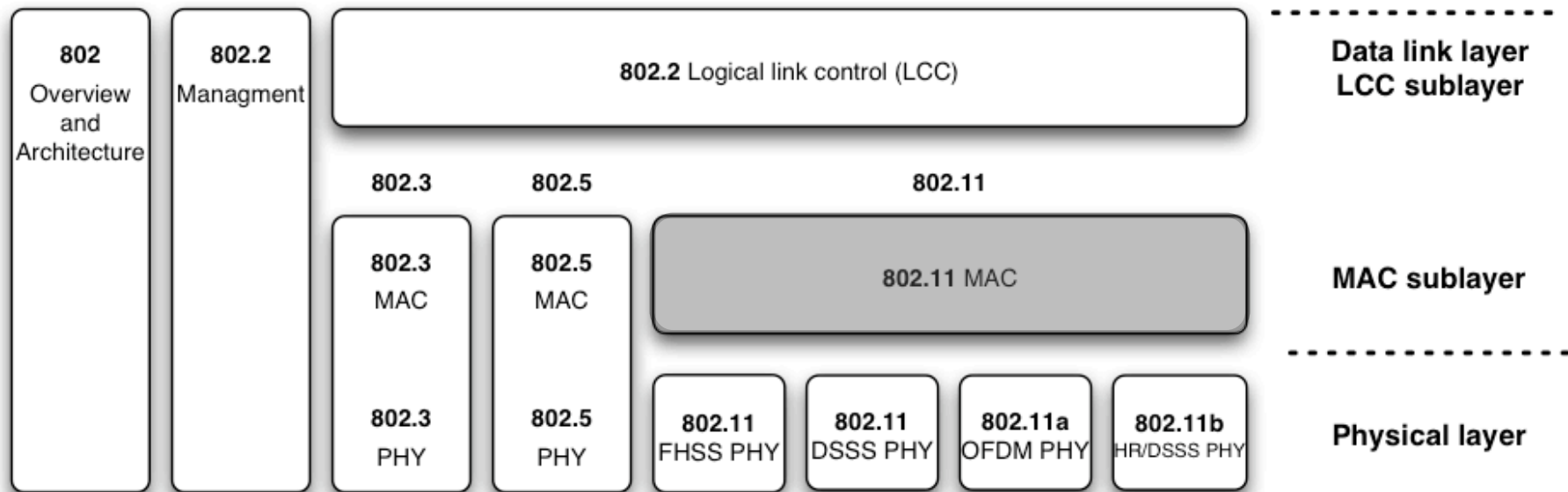
Outline

I. 802.11 Basics
I.1. Standards
I.2. CSMA/CA

- ▶ 802.11 (“WiFi”) Basics
 - ▶ Standards: 802.11{a,b,g,h,i}
 - ▶ CSMA/CA
- ▶ WiFi Security
 - ▶ WEP
 - ▶ 802.11i
 - ▶ DoS

IEEE 802 Family

I. 802.11 Basics
I.1. Standards
I.2. CSMA/CA



802.11 Standards

	802.11	802.11b	802.11a/h	802.11g	802.11n
Entstehungsjahr	1997	1999	1999/2002	2003	vorauss. Ende 2006
Frequenzband	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	5 GHz
Bruttotransfer	2 MBit/s	11 MBit/s	54 MBit/s	54 MBit/s	~600 MBit/s
Akzeptanz	veraltet	stark verbreitet	gering	verbreitet	-
Sicherheit	-	WEP	WEP	WEP, WPA	

802.11i ist ein **Amendment** (Erweiterung / Nachtrag)

802.11 Betriebsmodi

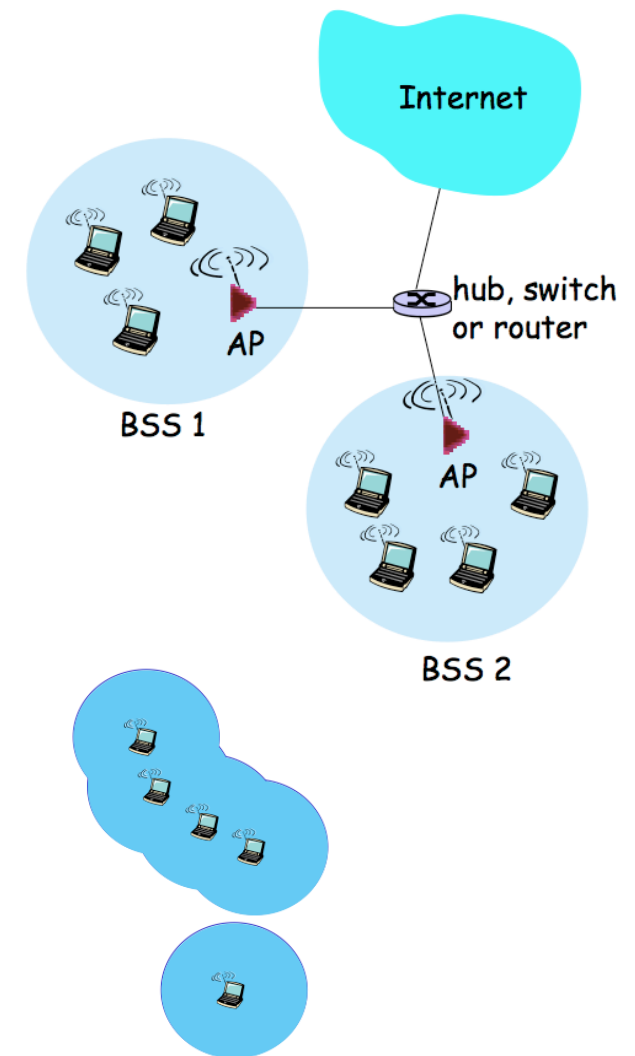
I. 802.11 Basics
I.1. Standards
I.2. CSMA/CA

Infrastructure mode

- ▶ *Access Point (AP)* stellt Schnittstelle zum Kabel-Netzwerk dar
- ▶ *Basic Service Set (BSS)* enthält
 - ▶ wireless Hosts
 - ▶ *Access Point (ad hoc mode: nur Hosts)*

Ad hoc mode

- ▶ keine *Access Points*, Devices können nur mit Devices in gleicher Reichweite kommunizieren



Unterschiede des Mediums...

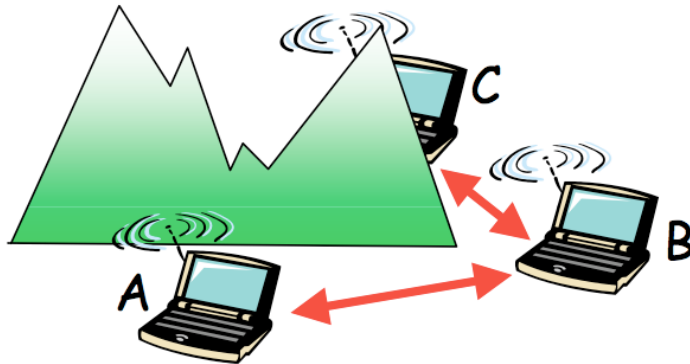
- ▶ **geringere Signalstärke:** Radio Signal verflüchtigt sich während der Ausbreitung (*path loss*)
- ▶ **Interferenz** von anderen Quellen: 2,4 GHz ISM Band wird auch von anderen Geräten verwendet (Bluetooth, ...).
- ▶ **Multipath Propagation:** Radio Signal reflektiert an Objekten (Wände, Boden) und trifft beim Ziel u.U. mehrmals ein.

...machen die Kommunikation (sogar *point-to-point*) erheblich komplizierter.

Wireless Network Characteristics

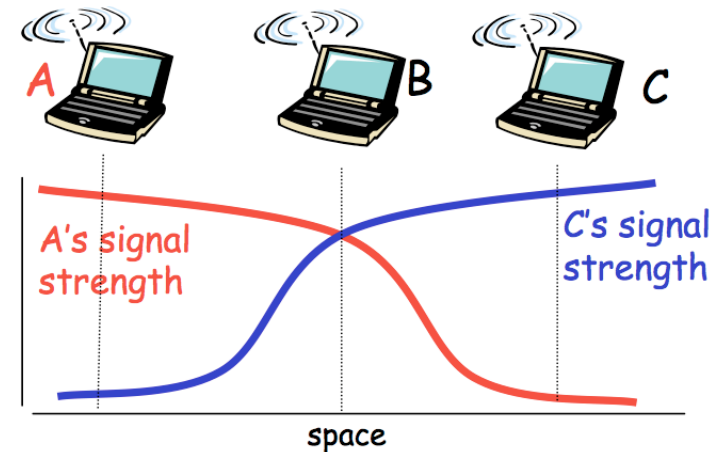
I. 802.11 Basics
I.1. Standards
I.2. CSMA/CA

- ▶ Mehrere drahtlose Sender und Empfänger schaffen weitere Probleme (zusätzlich zu CSMA)



hidden terminal/node

- ▶ A und B hören sich
- ▶ B und C hören sich
- ▶ A hört nicht C
- ➔ Interferenz bei B



signal fading

- ▶ A und B hören sich
- ▶ B und C hören sich
- ▶ A hört nicht C
- ➔ Interferenz bei B

IEEE 802.11 Multiple Access

- ▶ 802.11 **C**arrier **S**ense **M**ultiple **A**ccess - vor dem Senden “lauschen”
 - ▶ um nicht mit aktiven Übertragungen zu kollidieren
- ▶ 802.11: keine *Collision Detection (CD)*!
 - ▶ Erkennung von Kollisionen erfordert gleichzeitiges Senden (eigene Daten) und Empfangen (*sensing collisions*) → teuer!
 - ▶ Alle Kollisionen können sowieso nicht erkannt werden → *hidden node, signal fading*
- ▶ **Ziel**: Kollisionen vermeiden:
 - ▶ **CSMA/C**(ollision)**A**(voidance)

802.11 MAC Protocol: CSMA/CA

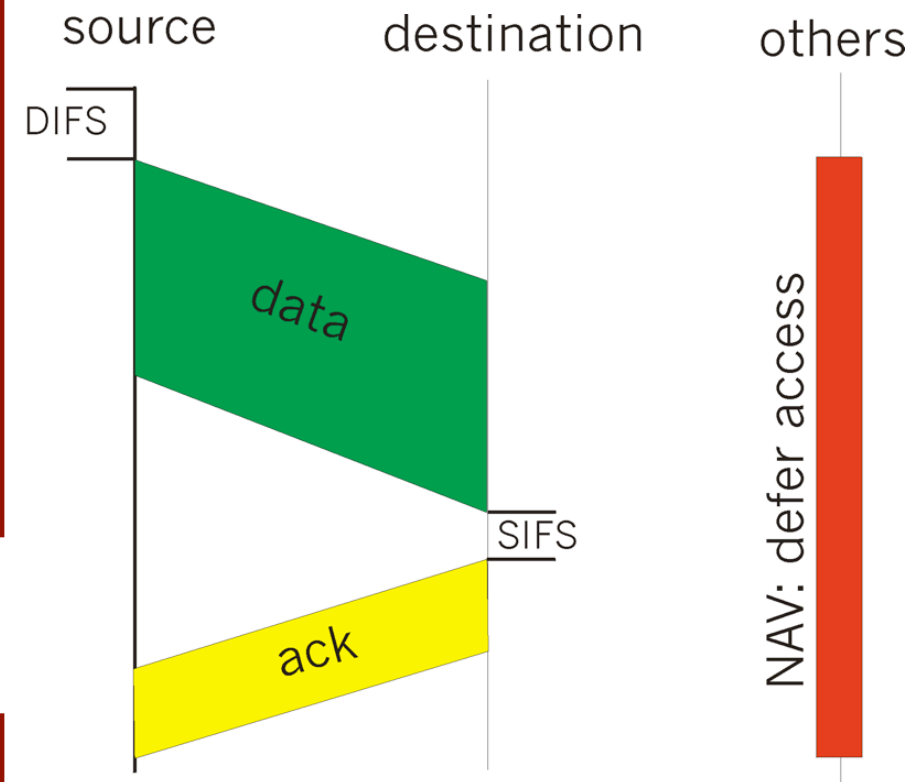
802.11 Sender

```
1 if (sense channel idle for DIFS)  
  transmit entire frame (no CD)  
2 if (sense channel busy) {  
  start random backoff timer  
  timer counts down while channel idle  
  transmit when timer expires  
  if (no ACK) {  
    increase random backoff interval  
    repeat 2  
  }  
}
```

802.11 Empfänger

```
if (frame received OK)  
  return ACK after SIFS
```

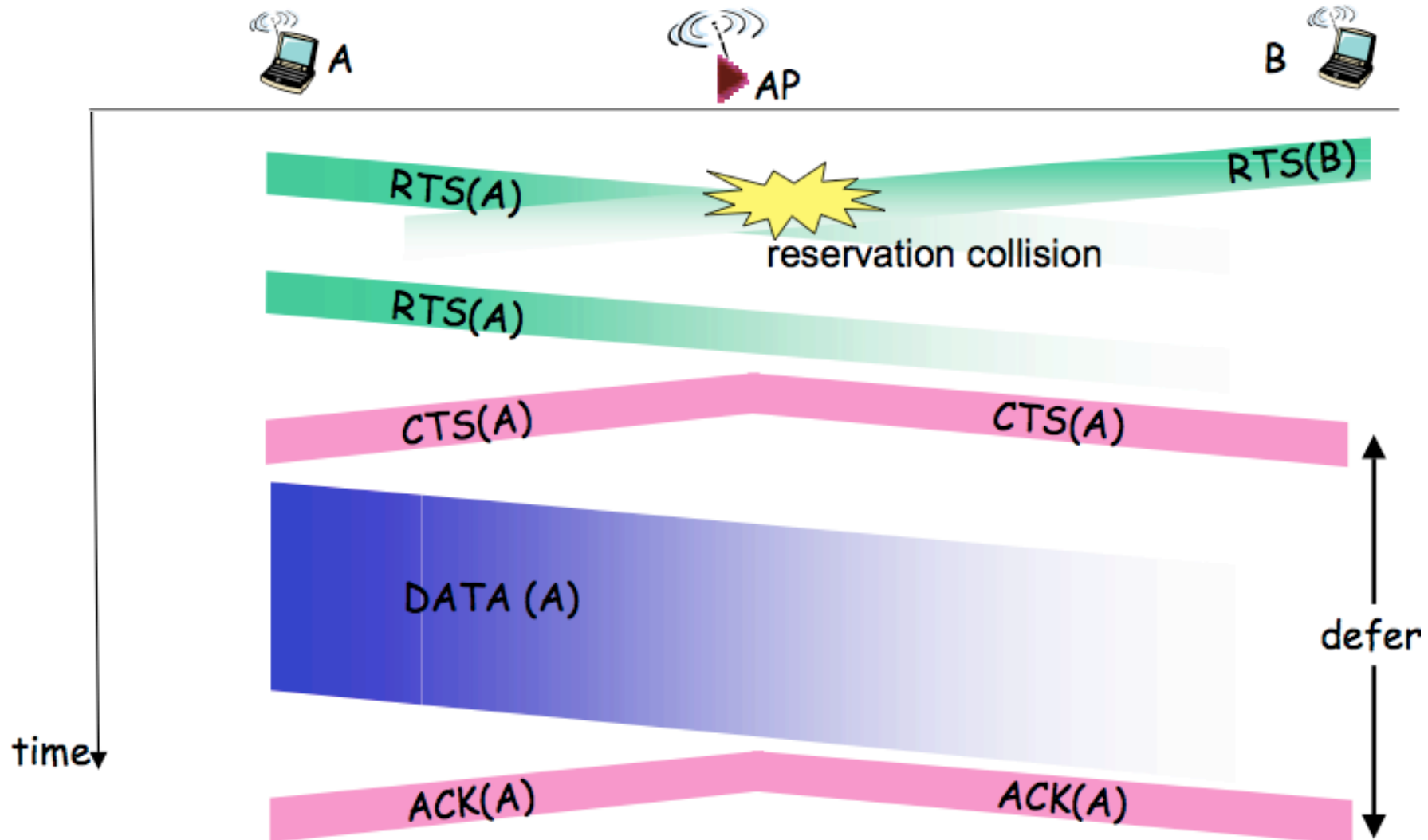
ACK wird wegen *hidden terminal* Problem benötigt



Kollisionen vermeiden

- ▶ **Idee:** dem Sender erlauben, den Kanal zu “reservieren” anstatt randomisierten Zugang zu Medium zu gewähren
- ▶ Sender schickt *kleine* **Request-To-Send** (RTS) Pakete zum AP mit CSMA
 - ▶ RTS können noch immer kollidieren (sind aber klein!)
- ▶ AP schickt einen broadcast **Clear-To-Send** (CTS) als Antwort auf RTS
- ▶ RTS/CTS wird von allen Devices gehört
 - ▶ Sender überträgt Data Frame
 - ▶ alle anderen Devices warten mit ihren Übertragungen bis der Kanal wieder frei ist
- ➔ **Data Frame Kollisionen durch kleine Reservierungspakete vollständig vermeiden!**

CSMA/CA: RTS-CTS exchange



Outline

2.WiFi Security

2.1.WEP

2.2.802.11i

2.3.DoS

-
- ▶ 802.11 (“WiFi”) Basics
 - ▶ Standards: 802.11{a,b,g,h,i}
 - ▶ CSMA/CA
 - ▶ **WiFi Security**
 - ▶ WEP
 - ▶ 802.11i
 - ▶ DoS

-
- ▶ Aspekte von *wireless Security*
 - ▶ Vertraulichkeit (*Confidentiality*)
 - ▶ Authentizität (*Authenticity*)
 - ▶ Integrität (*Integrity*)
 - ▶ **Verfügbarkeit** (*Availability*)

 - ▶ Adressieren die existierenden Sicherheits-Protokolle (WEP,WPA,WPA2) diese Aspekte?

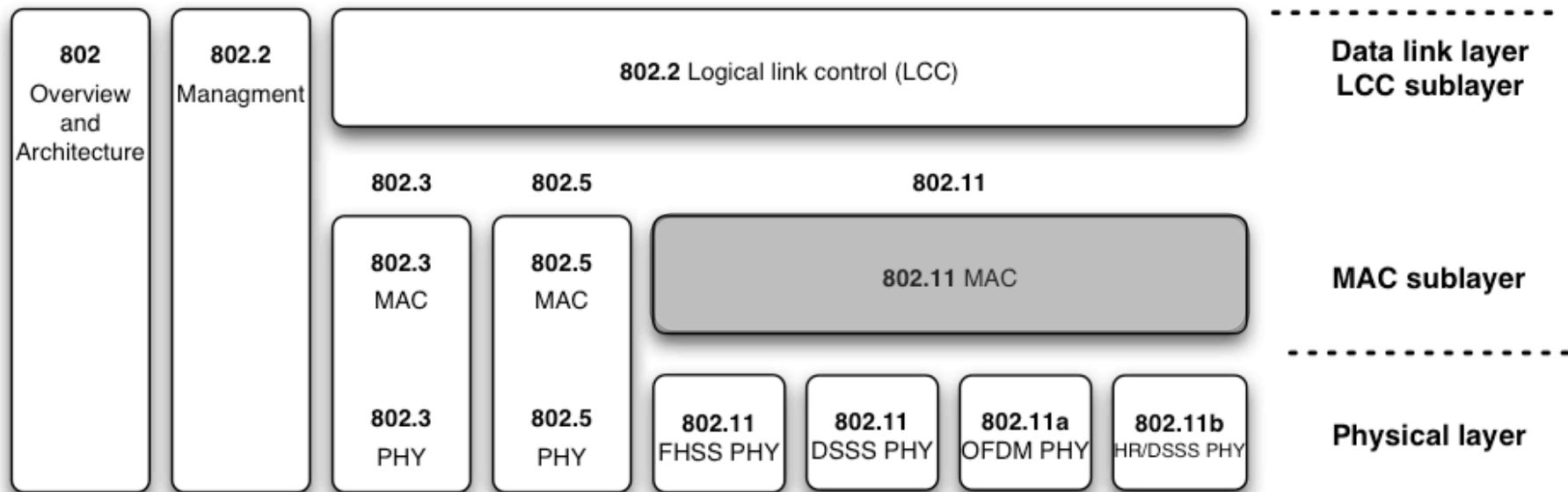
IEEE 802 Familie

2.WiFi Security

2.1.WEP

2.2.802.11i

2.3.DoS



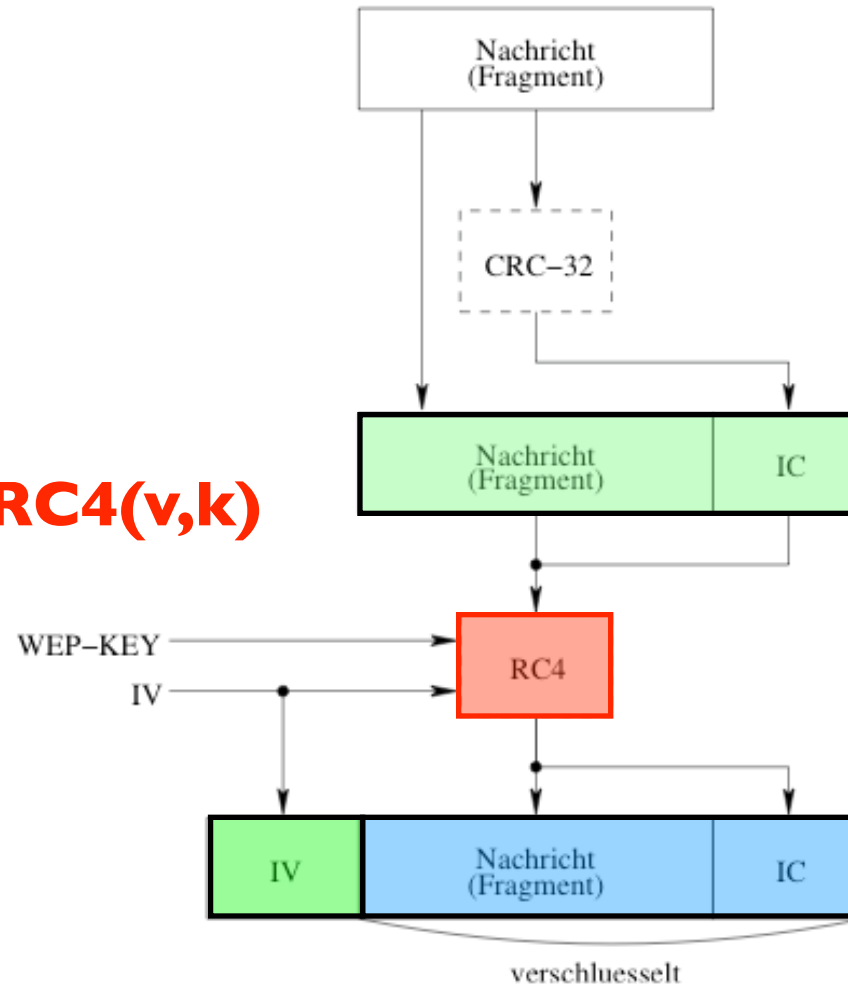
Wired Equivalent Privacy (WEP)

- ▶ Protokoll aus dem 802.11 Standard
 - ▶ **Aufgabe**: den MAC Layer schützen
- ▶ 3 Designziele:
 - ▶ **Confidentiality**: Vertraulichkeit durch Verschlüsselung
 - ▶ **Access Control**: Zugangskontrolle zur Netzwerk-Infrastruktur
 - ▶ **Data Integrity**: Schutz der Integrität durch eine Checksumme (CRC32)
- ▶ *Stream Cipher* generieren einen *pseudozufälligen Keystream*, der mit dem Klartext/Plaintext via XOR (i.Z. \oplus) verknüpft wird
 - ▶ WEP verwendet **RC4** (“arcfour”) als Streamcipher
 - ▶ Input-Parameter: Initialisierungsvektor **v** und geheimer Schlüssel **k**
 - ▶ **RC4(v,k)** ist der Keystream (**v** wird auch als *seed* bezeichnet)

$$\begin{array}{r} 100 \\ \oplus \\ 010 \\ = \\ 110 \end{array}$$

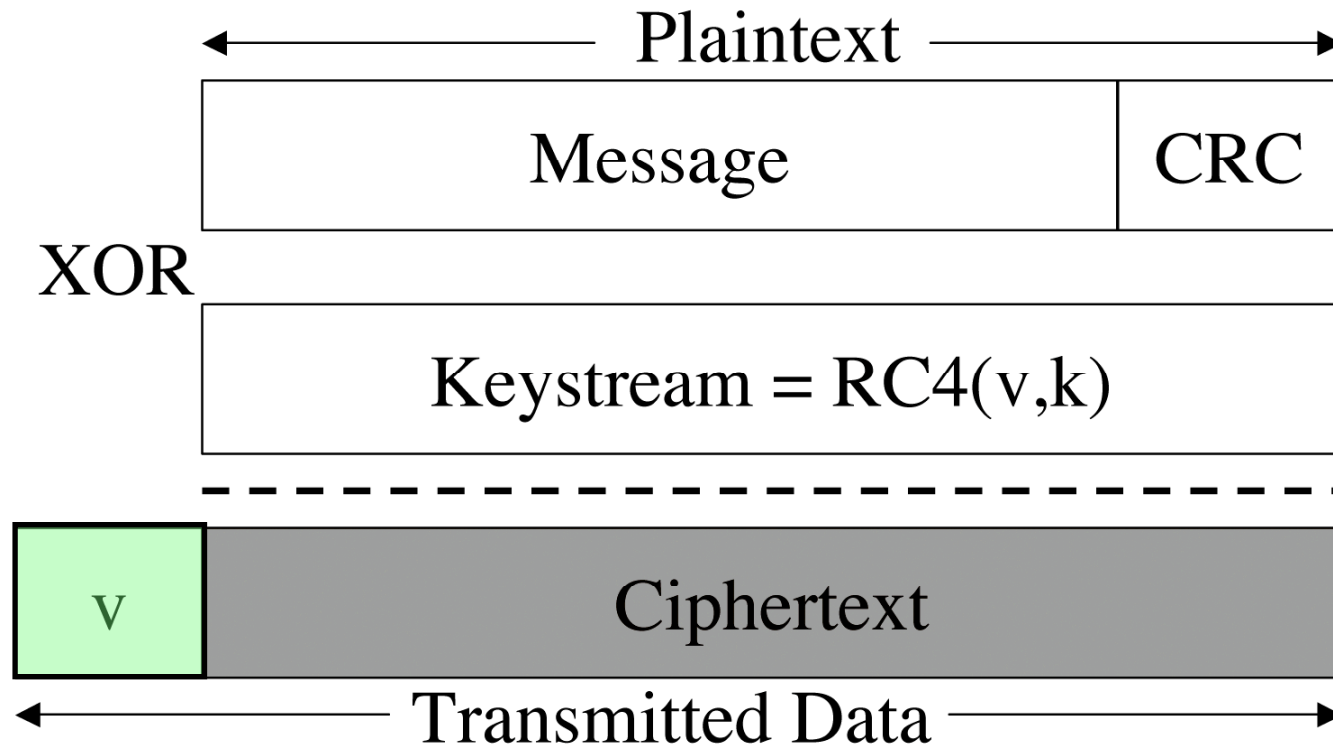
WEP

Keystream **RC4(v,k)**



----- Plaintext
----- Keystream
----- Ciphertext

WEP



v = IV = Initialization Vector (Klartext)

Angriffe auf WEP

- ▶ Bruteforce
- ▶ Keystream Reuse
 - ▶ IV Dictionary
- ▶ Weak IVs
- ▶ Frame Injection
- ▶ Fragmentation Attack

Keystream Reuse

- ▶ Wiederverwendung eines bereits benutzten Keystreams $RC4(v,k)$
- ▶ Keystream Space: **24 bit = 2^{24} IVs**
- ▶ Angreifer kann Pakete mit gleichem Keystream entschlüsseln
- ▶ mit nur *einem* validen Keystream kann ein Angreifer beliebige Frames in das Netz senden
 - ▶ 802.11b bietet keinen Schutz gegen *Replay* Angriffe

$$RC4(v,k) \oplus \text{Plaintext} = \text{Ciphertext}$$

Keystream Reuse (cont'd)

- ▶ **IV Dictionary:** Speichern aller IVs zusammen mit jeweiligem Keystream
- ▶ mit einem vollständigem Dictionary kann ein Angreifer den *gesamten* Verkehr entschlüsseln
- ▶ Wie bekommt man gültige Keystreams?
 - ▶ *Shared Key Authentication* (deprecated)
 - ▶ *Known-Plaintext*
 - ▶ *Fragmentation Attack*
 - ▶ Relaying Broadcast Frames
 - ▶ *Chop-Chop* (Keystream “raten”)

$$\text{RC4}(v,k) = \mathbf{P} \oplus \mathbf{C}$$


Weak IVs

- ▶ Der geheime Schlüssel ***k*** kann errechnet werden
 - ▶ RC4 Schwachstelle war bereits **4 Jahre** (!) vor der Veröffentlichung von WEP bekannt
 - ▶ **“schwache” IVs**: offenbaren zu 5% ein korrektes Byte vom Schlüssel ***k***
- ▶ Hardware Patches von Herstellern: Filtern von schwachen IVs
 - ▶ Problem nur noch schlimmer: Reduzierung des Keystream Space: $< 2^{24}$
 - ▶ Legacy Host kann gesamtes Netzwerk kompromittieren

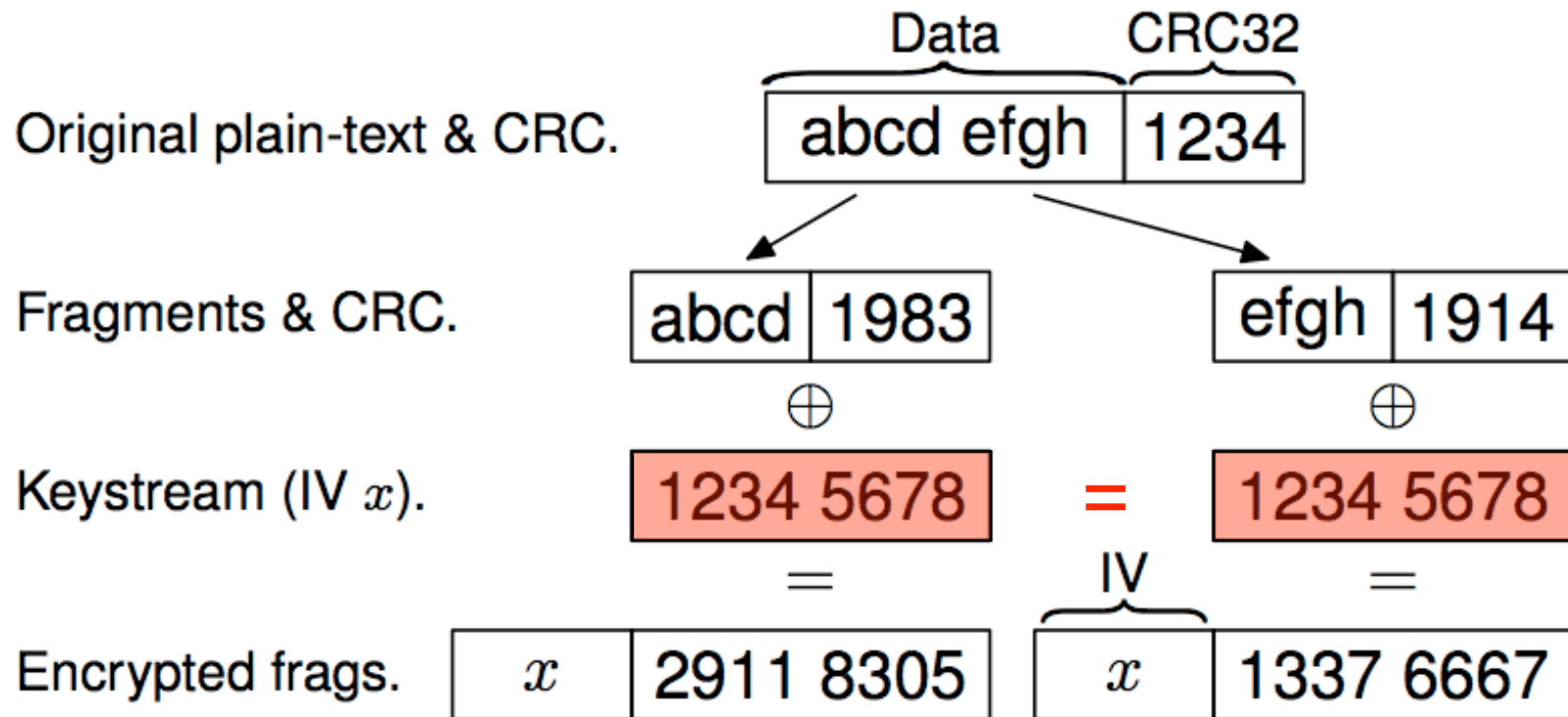
Frame Injection

- ▶ Weitere Klassen von schwachen IVs wurden veröffentlicht
 - ▶ zu 13% korrektes Byte des Schlüssels
- ▶ Hersteller integrieren keine weiteren IV-Filter
 - ▶ immer noch $\approx 500.000 - 1.000.000$ Pakete benötigt
 - ▶ lange Wartezeiten für erfolgreichen Angriff
- ▶ **Beschleunigen** der Angriffe durch *replaying* von WEP Frames
 - ▶ nur Frames, die eine Antwort im Netzwerk erzeugen
 - ▶ z.B. ARP-Request (an fester Länge erkennbar)
- ▶ Gegenmaßnahme der Hersteller: *EAP*-basierte Lösungen, die schnelles *re-keying* implementieren
 - ▶ *EAP = Extensible Authentication Protocol*
 - ▶ Authentication Framework, kein spezieller Authentifizierungs-Mechanismus
 - ▶ enthält ca. 40 Methoden: EAP-MD5, EAP-OTP, EAP-GTP, ... , EAP-TLS, ...

Fragmentation Attack

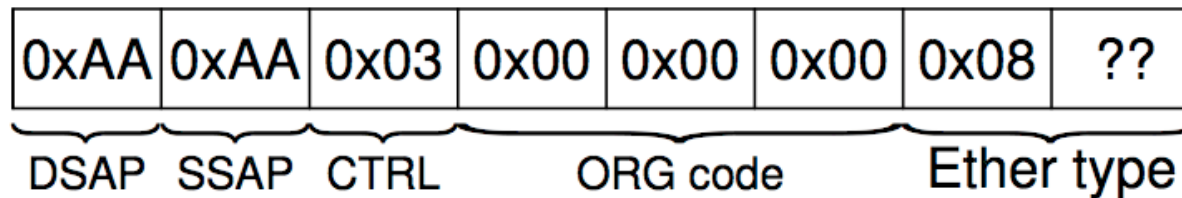
- ▶ Neue Attacke, robust gegen häufiges re-keying, da in *real-time*
 - ▶ Daten in ein WEP Netzwerk senden
 - ▶ Entschlüsseln von WEP Daten
- ▶ **Ansatz:** 802.11 kann gegen WEP verwendet werden 
 - ▶ 802.11 spezifiziert **Fragmentierung** auf dem MAC Layer
 - ▶ jedes Fragment ist einzeln verschlüsselt
 - ▶ mehrere Fragmente können mit dem gleichen Keystream gesendet werden
 - ▶ max. 16 Fragmente, da 4 bit Feld für *Frag No* im Header

802.11 Fragmentation



Fragmentation Attack

- ▶ **8** bytes known plaintext in jedem Frame*
- ▶ 802.11 Frames sind **LLC/SNAP** enkapsuliert (konstanter Header)



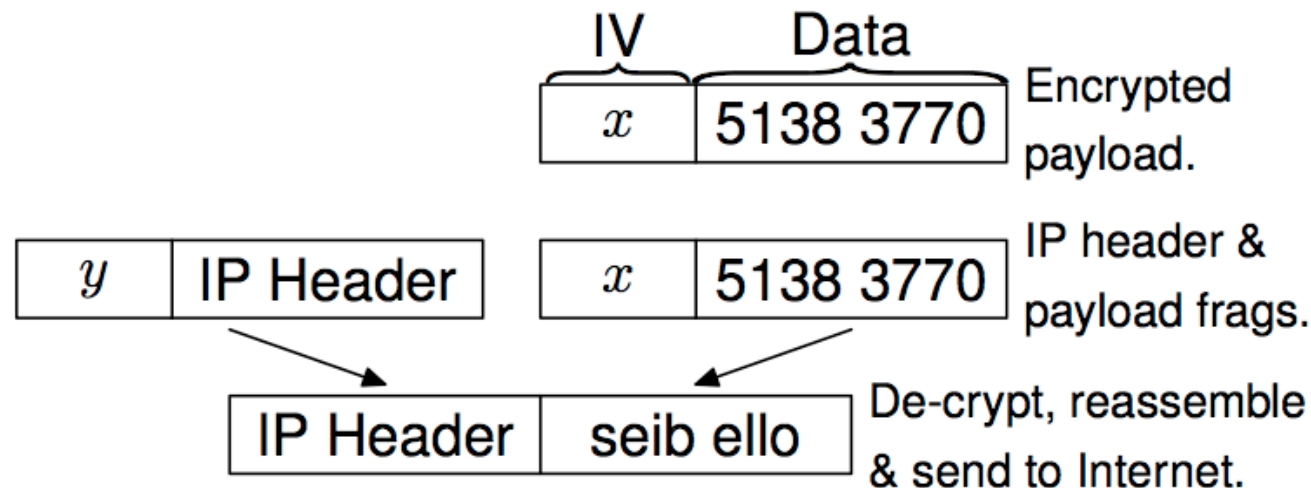
- ▶ Ether type = IP oder ARP
- ▶ implizit auch 8 bytes vom Keystream bekannt
 - ▶ $\mathbf{P} \oplus \mathbf{C} = \text{RC4}(v,k)$
- ▶ $(8 - 4) \times 16 = 64$ bytes Daten können mit Hilfe von Fragmentierung sofort injiziert werden
 - ▶ 4 bytes für CRC (daher 8 - 4)

Fragmentation Attack

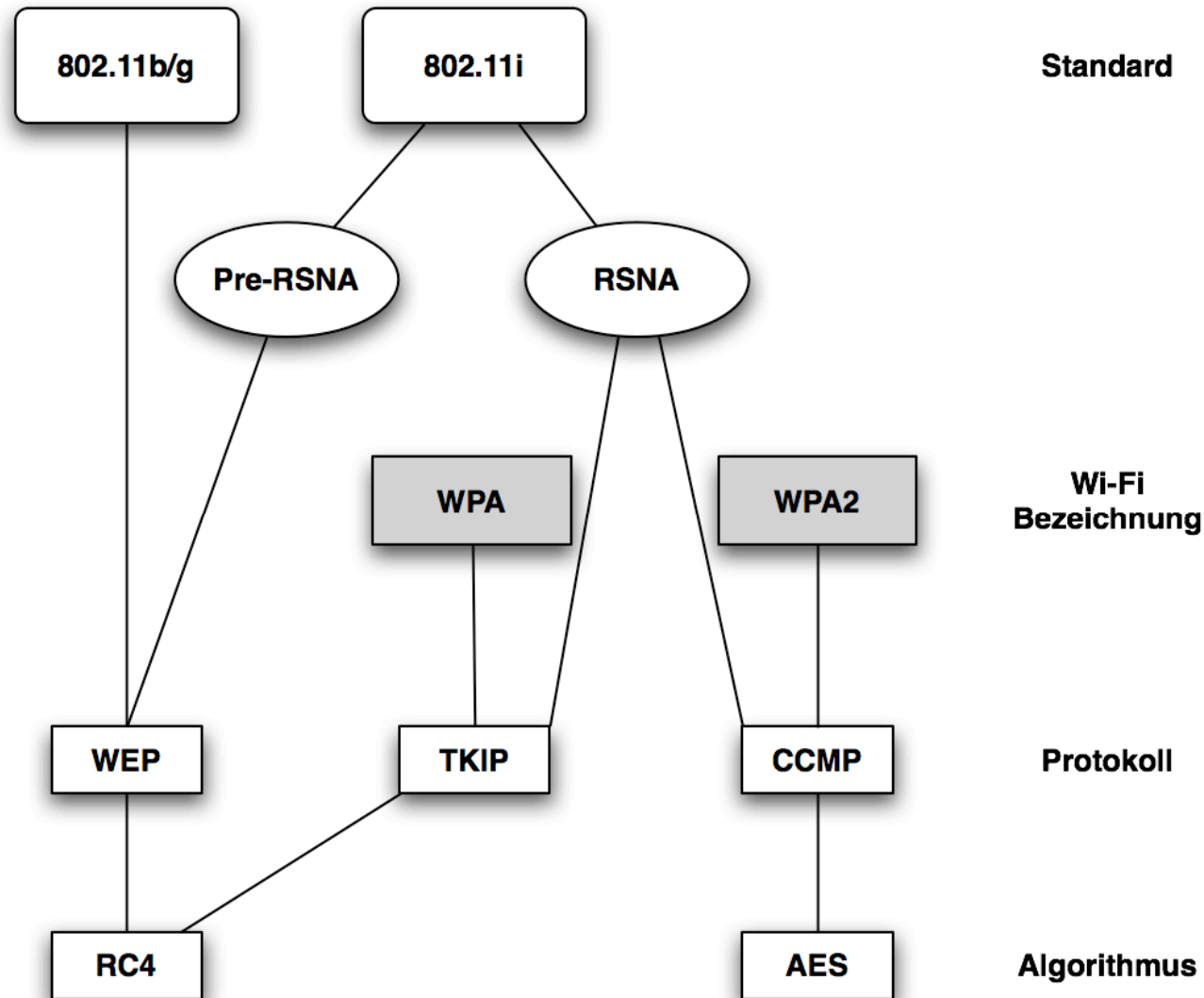
- ▶ Was können wir damit erreichen?
 - ▶ andere Angriffe beschleunigen (*Weak IV*)
 - ▶ Keystream Angriffe
 1. **8 bytes** vom Keystream bestimmen
 2. **Keystream erweitern**: lange *Broadcast Frames* in mehreren Fragmenten schicken und Antwort vom AP entschlüsseln ($\mathbf{C} \oplus \mathbf{P} = \text{RC4}(v,k)$). Solange wiederholen, bis 1500 bytes (MTU) vom Keystream bekannt sind
 3. **IV Dictionary**:
 - 3.1. Senden von 1500 byte Broadcasts
 - 3.2. AP wird das Paket (wahrscheinlich) weiterleiten
 - 3.3. Keystream für das Paket bestimmen und auf diese Weise alle weiteren Keystreams bestimmen
 4. **Entschlüsseln** von Paketen, deren Keystream bekannt ist
 - ▶ Entschlüsseln von Paketen in *real-time*...

Fragmentation Attack

- ▶ Entschlüsselung von Paketen in *real-time*
 - ▶ **Voraussetzung:** Internet Connectivity
 - ▶ Angreifer kann den AP zum Entschlüsseln verwenden ☠
 - ▶ Mit Hilfe von 802.11 Fragmentierung kann ein **zusätzlicher IP-Header** vor das ursprüngliche Paket eingefügt werden
 - ▶ Das ursprüngliche Paket wird als letztes Fragment angefügt
 - ▶ AP reassembliert, entschlüsselt und schickt das Paket an die “gespoofte” IP Adresse



802.11 Terminii



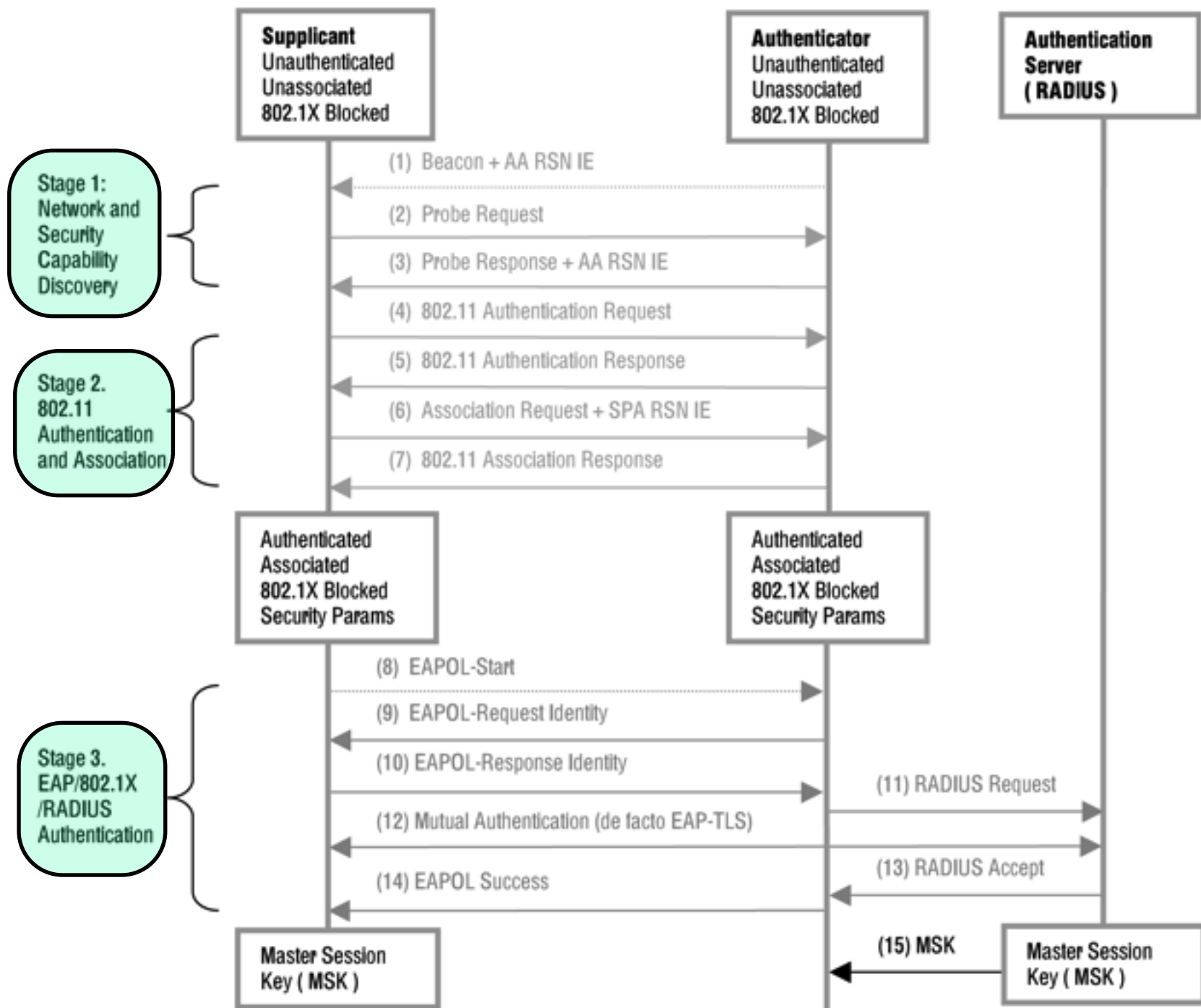
802.11 Sicherheit

	WEP	WPA	WPA2
Algorithmus	RC4	RC4	AES-CTR
Schlüssellänge	64/128 bit	128 bit	128 bit
IV-Länge	24 bit	48 bit	48 bit
Datenintegrität	CRC-32	Michael	CBC-MAC
Headerintegrität	-	Michael	CBC-MAC
Authentifizierung	Shared Key	802.1X	802.1X
Key-Management	-	802.1X	802.1X
Replay-Attacken Schutz	-	IV-Sequenz	IV-Sequenz

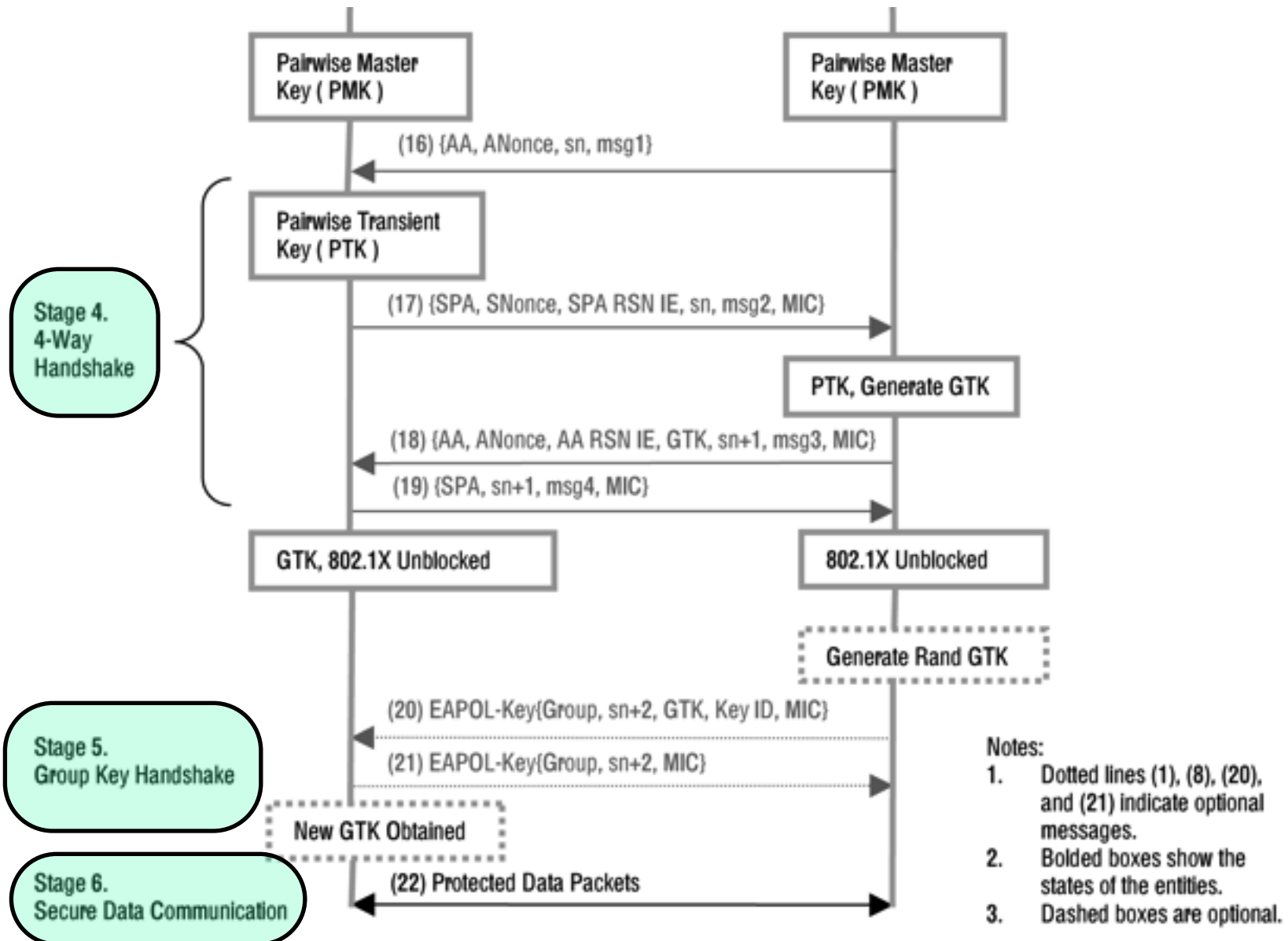
802.11i - RSNA Overview

- ▶ 3 Entitäten bei der *Robust Security Network Association (RSNA)* beteiligt
 - ▶ *Supplicant* (WLAN Client)
 - ▶ *Authenticator* (Access Point)
 - ▶ *Authentication Server* (fast immer RADIUS Server)
- ▶ 6 Verbindungsphasen bis zum Datenaustausch
 - ▶ Phase 1: *Network and Security Capability Discovery*
 - ▶ Phase 2: *802.11 Authentication and Association*
 - ▶ Phase 3: *EAP/802.1X/RADIUS Authentication*
 - ▶ Phase 4: *4-Way Handshake*
 - ▶ Phase 5: *Group Key Handshake*
 - ▶ Phase 6: *Secure Data Communication*

➔ komplexer als WEP (zum Glück auch sicherer :)



RSNA (cont'd)



802.11i Schwachstellen

- ▶ PSK Dictionary Brute-force Attack
- ▶ Security Level Rollback Attack
- ▶ Reflection Attack

802.11i PSK Brute Force

PSK = PMK = PBKDF2(*passphrase*, SSID, SSIDlength, 4096, 256)

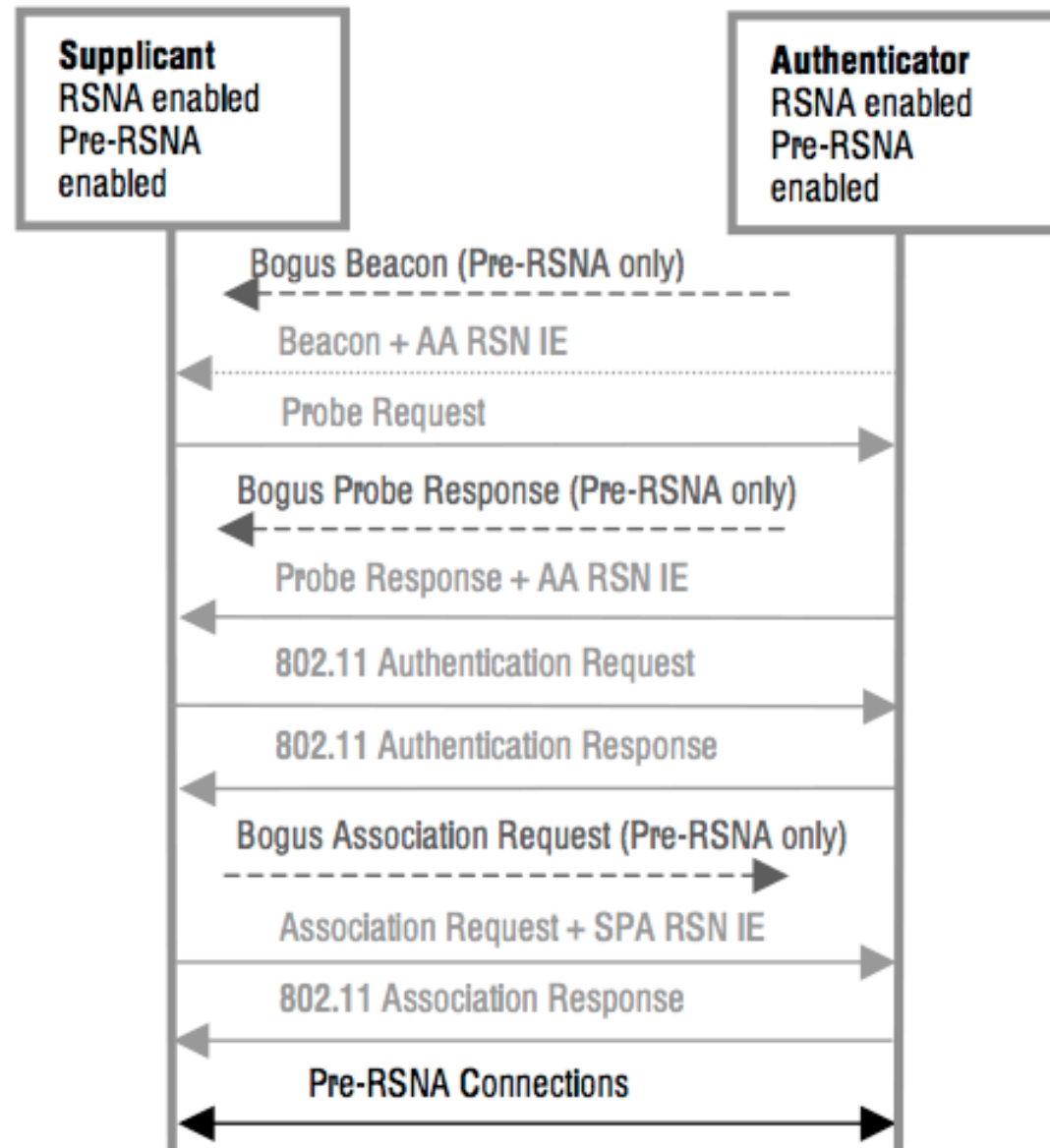
- ▶ *PSK* = Pre-Shared Key
- ▶ *PMK* = Pairwise Master Key
- ▶ *PBKDF2* = Verfahren aus PKCS#5 v2.0
- ▶ *SSID* = Service Set Identity
- ▶ *SSIDlength* = Länge der SSID
- ▶ *4096* = Anzahl der Hashdurchläufe
- ▶ *256* = Länge der Ausgabe

Security Level Rollback Attack

- ▶ *Transient Security Network (TSN)* als Kompatibilitätsmodus in heterogenen Umgebungen
 - ▶ für sanfte Migration auf WPA2 gedacht
 - ▶ erlaubt Pre-RSNA und RSNA Verbindungen
- ▶ Angreifer simuliert Pre-RSNA **Authenticator**
 - ▶ Senden von gespooften Probe-Requests / Beacons
 - ▶ Sicherheit schrumpft auf schwächste Komponente
 - ▶ Fallback to WEP :(

Security Level Rollback Attack

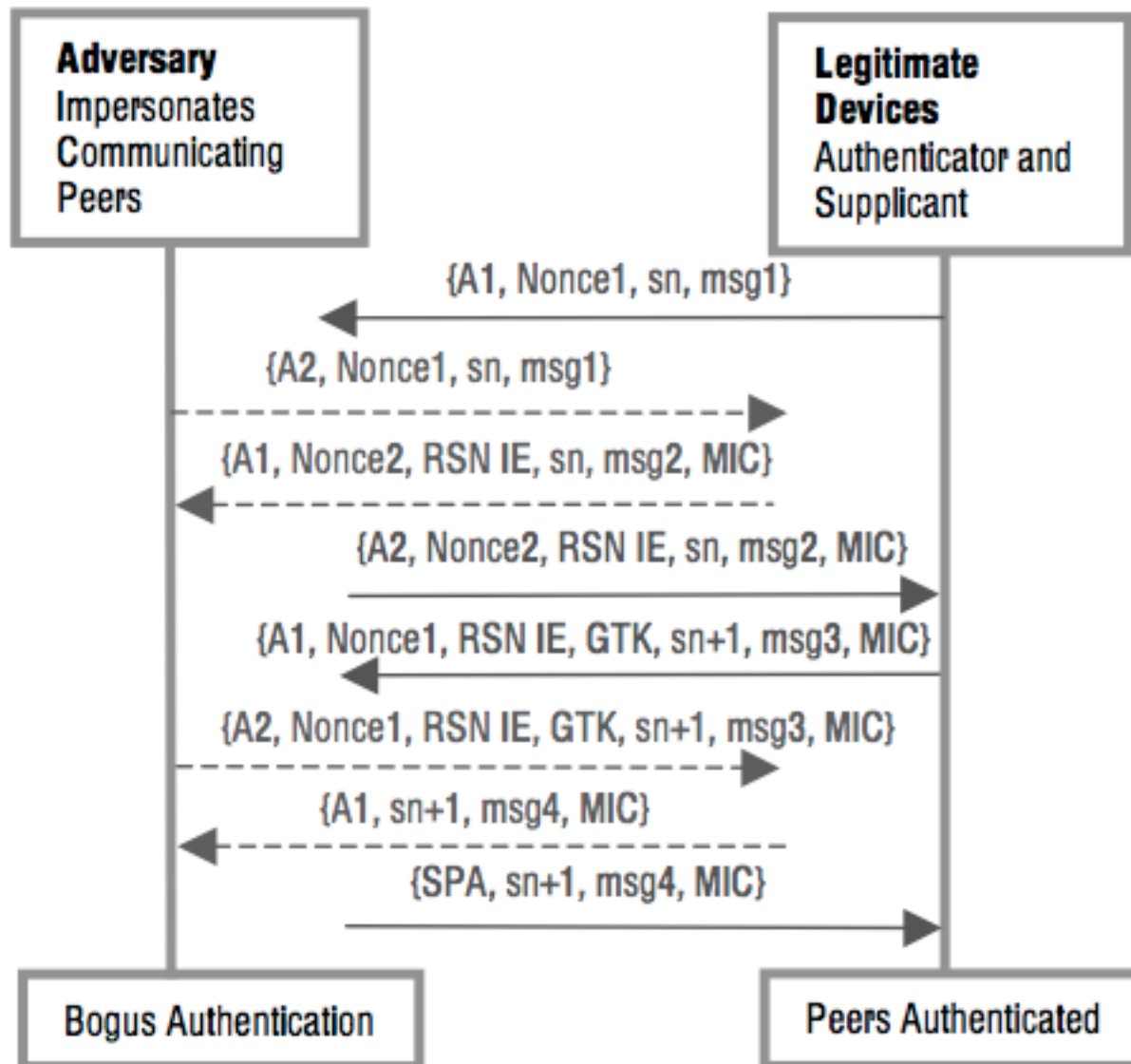
2.WiFi Security
2.1.WEP
2.2.802.11i
2.3.DoS



Reflection Attack

- ▶ Attacke funktioniert nur im *Ad hoc* mode
 - ▶ im *Infrastrucutre* mode sind *Supplicant* und *Authenticator* immer unterschiedliche Devices
- ▶ Angreifer verkörpert *Supplicant* und *Authenticator* in einem Device
 1. *4-Way-Handshake (4WH)* als *Authenticator*
 2. *4WH* als *Supplicant* mit gleichem Parametern
- ▶ Antworten vom zweiten *4WH* können als gültige Daten für den ersten *4WH* verwendet werden
 - ▶ mutual authentication durchbrochen
 - ▶ Verschlüsselte Daten können gespeichert werden (offline Analyse)

Reflection Attack



Denial-of-Service (DoS)

- ▶ Frequency Jamming (PHY)
- ▶ Deauthentication / Disassociation Frame Spoofing
- ▶ CMCA/CA - keine geschützten Management Frames
 - ▶ Standard ignorieren: kein “backoff”
 - ▶ virtual carrier-sensing (RTS mit hohem NAV)
- ▶ ARP-Cache Poisoning
- ▶ 802.1X
 - ▶ EAP-*{Start, Logoff, Failure}* Spoofing
 - ▶ EAP Identifier nur 8 bit: mehr als 255 Authentication Request gleichzeitig senden
- ➔ DoS zu einfach (nicht von 802.11i adressiert!)
- ➔ DoS Angriffe können weitere *Attacks vereinfachen (Session-Hijacking, MitM)*

Fazit

- ▶ WiFi wird ubiquitär / *pervasive*
- ▶ kontinuierliche Weiterentwicklung der Standards
- ▶ Sicherheitsaspekte
 - ▶ Shared Medium (!)
 - ▶ WEP liegt nun endgültig im Sarg
 - ▶ Verwendung sicherer Protokolle (SSH, IMAPS, HTTPS) über WLAN
 - ▶ sichere WPA/WPA2 Passphrase p wählen ($p \notin$ Wörterbuch)
 - ▶ DoS (noch) zu einfach
 - ▶ Kabel verwenden, wenn es drauf ankommt :)

FIN

Fragen ?

vallentin@net.in.tum.de