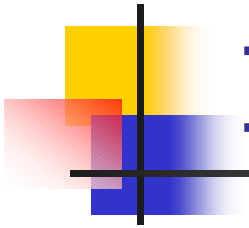
Sicherheit in mobilen Netzwerken

Seminar Mobile Computing

5.Juni 2001

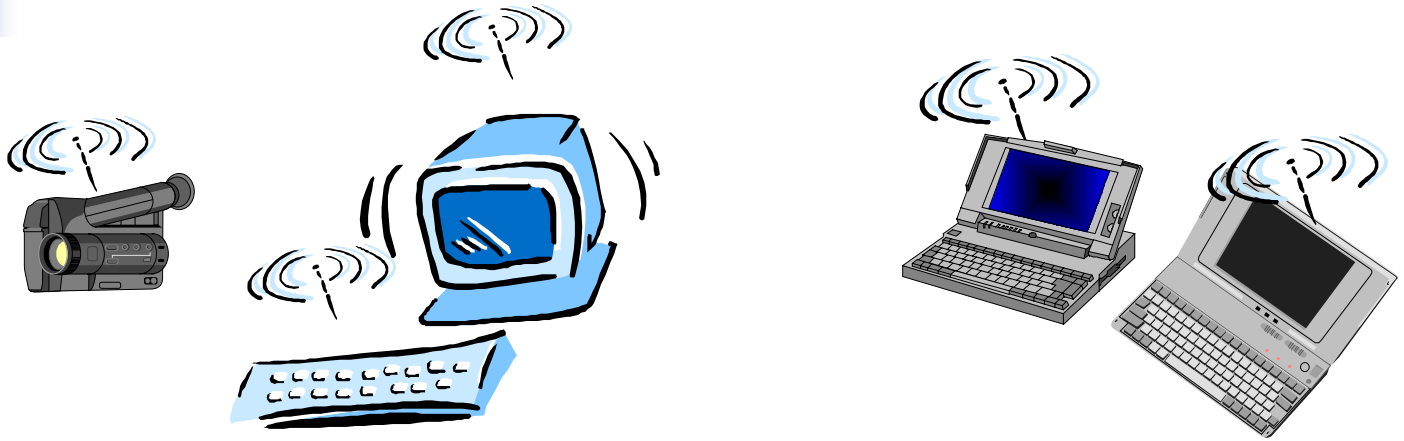
Sabine Keuser



Inhalt

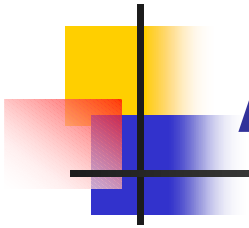
- Probleme mobiler Netzwerke
- Sicherheit in Bluetooth
- Sicherheit in Wireless LANs (IEEE 802.11)
- Zusammenfassung

Probleme mobiler Netzwerke



- Keine physikalisch sicheren Verbindungen
- Teilnehmer "kennen sich nicht"
- Unterschiedliche Sicherheitsstandards

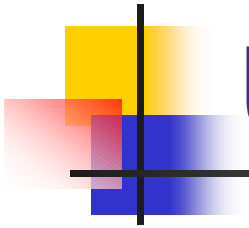
} Ad hoc Netzwerke



Attacken

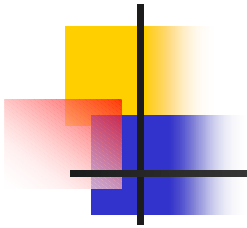
- Lauschen
- Nachrichten modifizieren / einspeisen
  - Impersonating
- Schlüssel brechen
- Location Attack
- (Denial of Service)

Mobilität



Übersicht

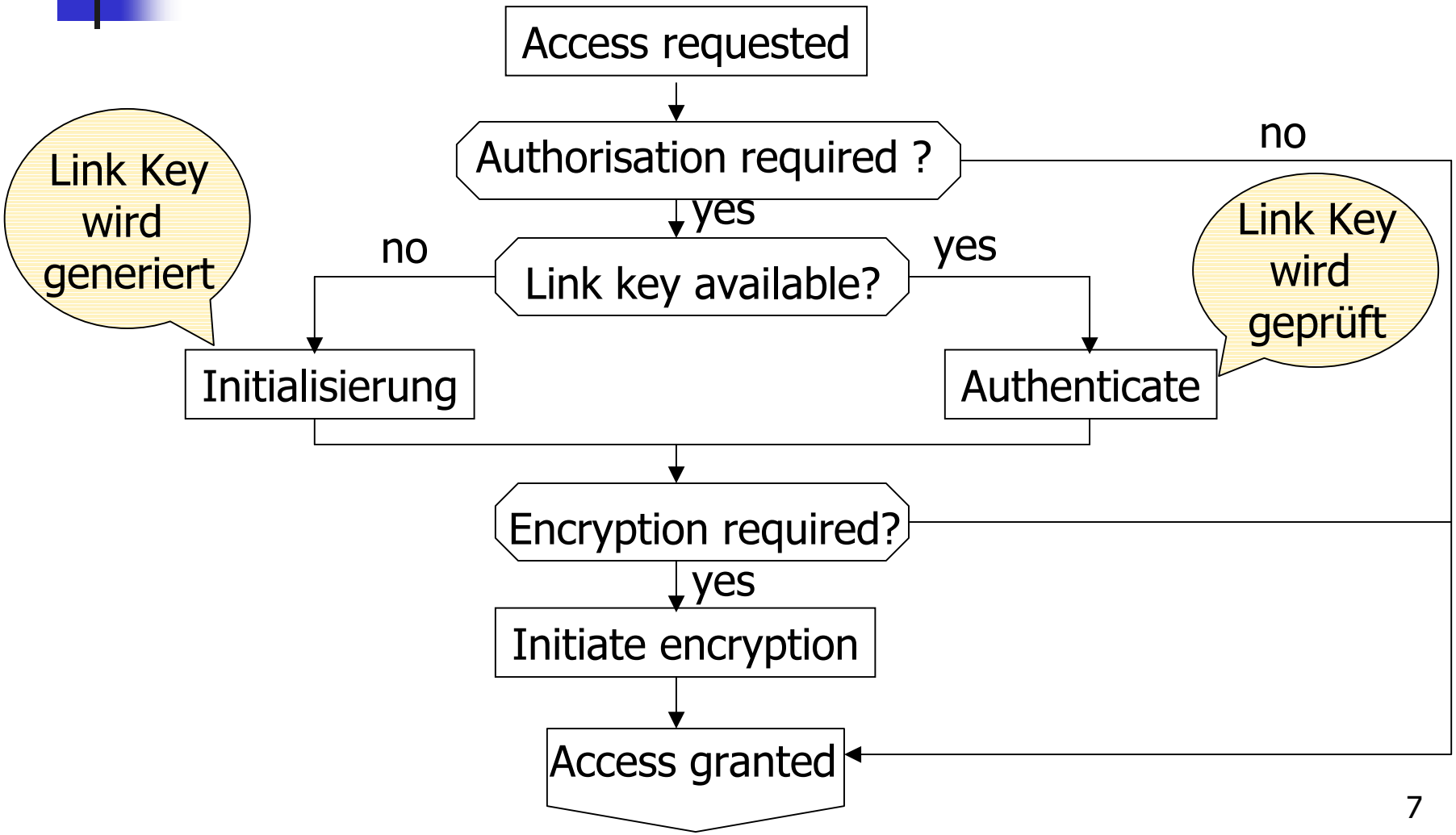
- Probleme mobiler Netzwerke
- **Sicherheit in Bluetooth**
  - **Sicherheitsmechanismen**
  - **Attacken**
  - **Gegenmassnahmen**
- Sicherheit in Wireless LANs (IEEE 802.11)
- Zusammenfassung



Bluetooth: Security Features

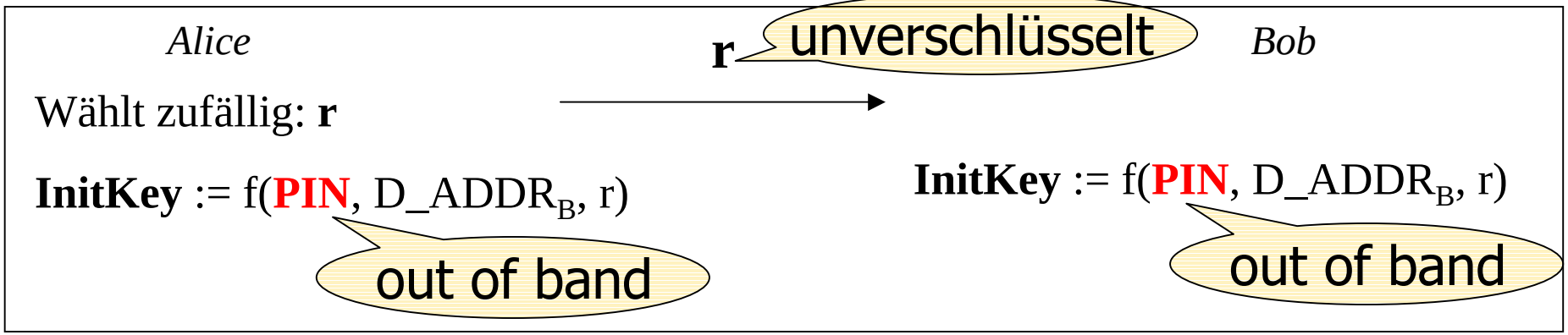
- Authentisierung (Device)
  - Einseitig
  - Gegenseitig
- Verschlüsselung
  - Gemeinsamer Secret Key
  - Schlüsselmanagement

Bluetooth: Access Procedure

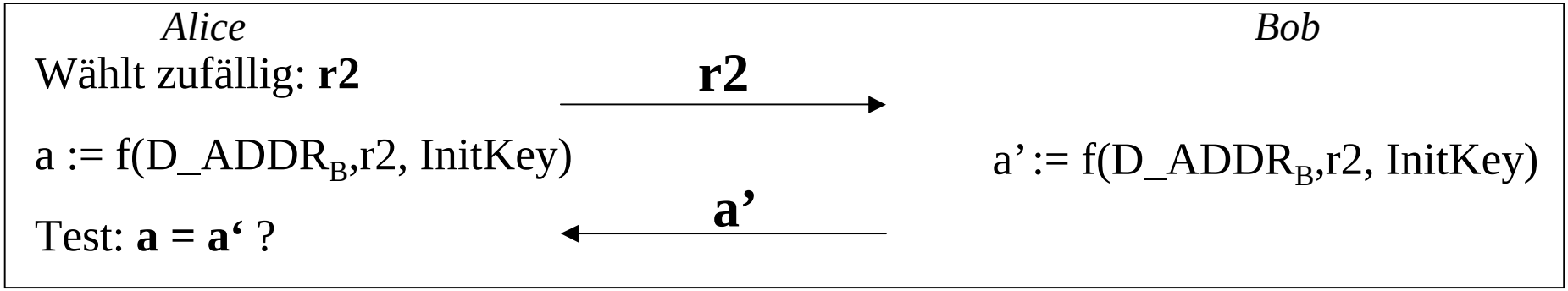


Bluetooth: Initialisierung

- Initialization Key Generierung

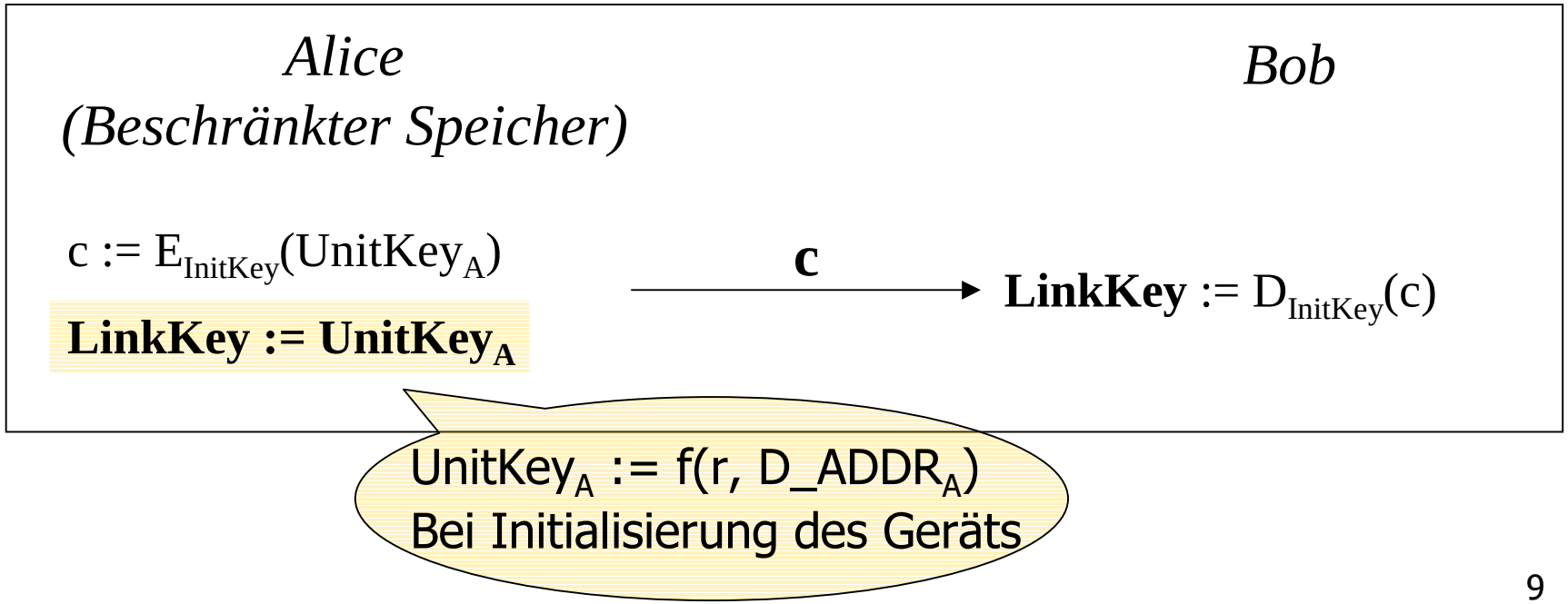


- Initialization Key Überprüfung



Bluetooth: Initialisierung

- Link Key Generierung
  - Mindestens ein Teilnehmer hat beschränkte Speicherressourcen

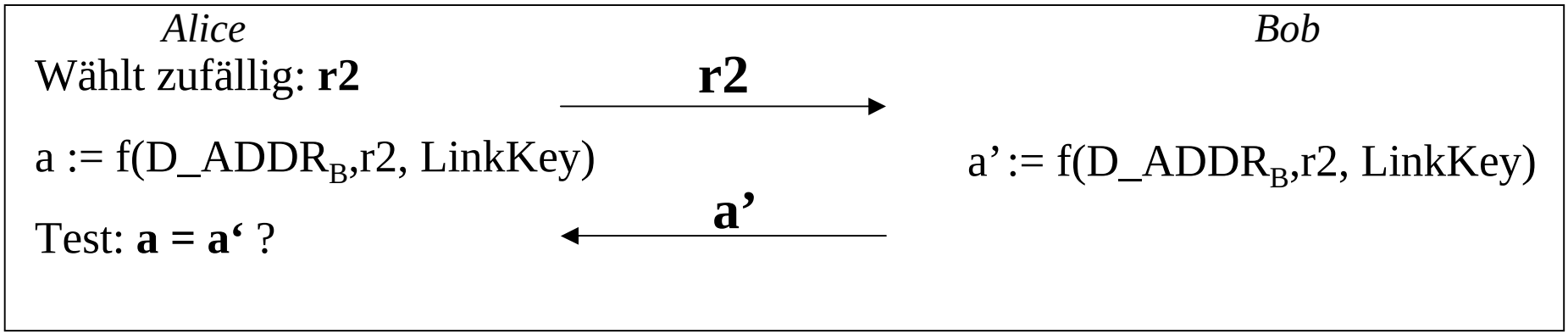


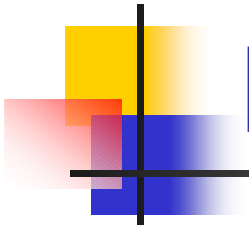
Bluetooth:Initialisierung

- Alle haben genügend Speicher

Alice		*Bob*
Wählt zufällig $\mathbf{r_A}$		Wählt zufällig $\mathbf{r_B}$
$\mathbf{LK\_K_A} := f(r_A, D\_ADDR_A)$		$\mathbf{LK\_K_B} := f(r_B, D\_ADDR_B)$
$c_A := E_{InitKey}(r_A)$	$c_A \rightarrow$	$c_A := E_{InitKey}(r_B)$
$r_{B :=} D_{InitKey}(c_B)$	$\leftarrow c_B$	$r_{A :=} D_{InitKey}(c_A)$
$\mathbf{LK\_K_B} := f(r_B, D\_ADDR_B)$		$\mathbf{LK\_K_A} := f(r_A, D\_ADDR_A)$
$\mathbf{LinkKey} := LK\_K_A \oplus LK\_K_B$		$\mathbf{LinkKey} := LK\_K_B \oplus LK\_K_A$

Bluetooth: Authentisierung



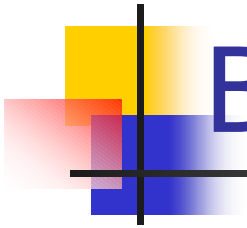


Bluetooth: Attacken

- Hopping along
- Schlüssel brechen
- Location Attacks

Bluetooth: Hopping Along

- 23-79 Kanäle
- Pseudozufällig mit clock und device address als seed.
- Antwort auf Inquiry verrät die device addresse und clock
- Master sendet clock und Adresse beim pageing
- Attacke:
  - Scanne die inquiry Frequenzen und belausche die response messages



Bluetooth:Schlüssel brechen

Brute Force Attacke auf kurzen oder schwachen PIN

- Passiv
  - Belauschen der Initialization (Klartext)
  - PIN raten
  - Überprüfen (offline)
  - Alle Kommunikation kann belauscht werden, Nachrichten können eingespeist werden

Bluetooth:Schlüssel brechen

- Aktiv
  - Kommunikation initiieren
  - 1. Challenge senden
  - PIN raten
  - Überprüfen (offline)
  - Nachrichten können eingespeist werden

Bluetooth: Location Attacks

- Ist ein Device im *discoverable* Mode antwortet es auf *Inquiries* mit seiner Device Adresse
- Attacken:
  - Netzwerk von Services (machen inquiries)
  - Bringe victim device dazu nach anderen Devices zu scannen
  - Channel Acces Code kann von jeder Message bestimmt werden

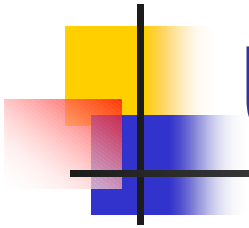
Bluetooth: Gegenmassnahmen

- Sichere PIN wählen
- Sicherheit im Application Layer
- Physikalischer Schutz
- Unit Keys geheimhalten
- Pseudoyme

Location Attack

Benutzer

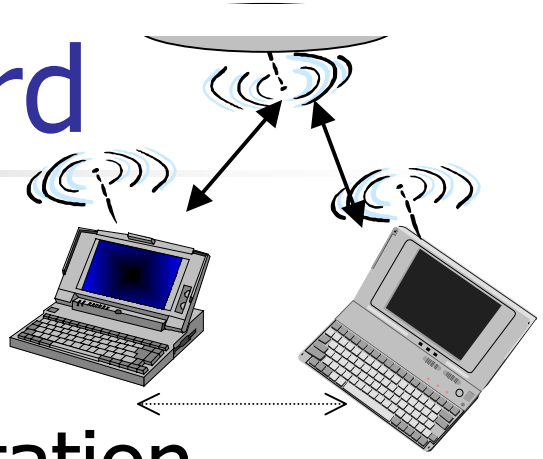
Bluetooth standard



Übersicht

- Probleme moblier Netzwerke
- Sicherheit in Bluetooth
- **Sicherheit in Wireless LANs (IEEE 802.11)**
  - **Sicherheits Mechanismen**
  - **Attacken**
  - **Gegenmassnahmen**
  - **WLAN an der ETH**
- Zusammenfassung

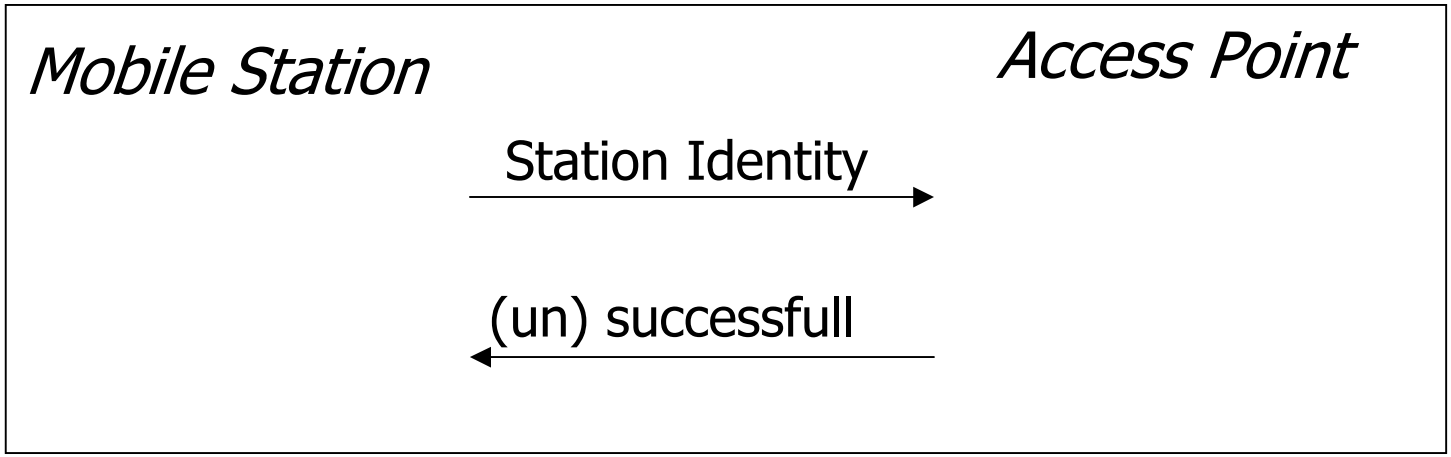
IEEE 802.11: Standard



- Kommunikation zwischen Access Point und Mobile Station
- Authentisierung
- Verschlüsselung: Wired Equivalent Privacy (WEP)
  - Kein Schlüsselmanagement

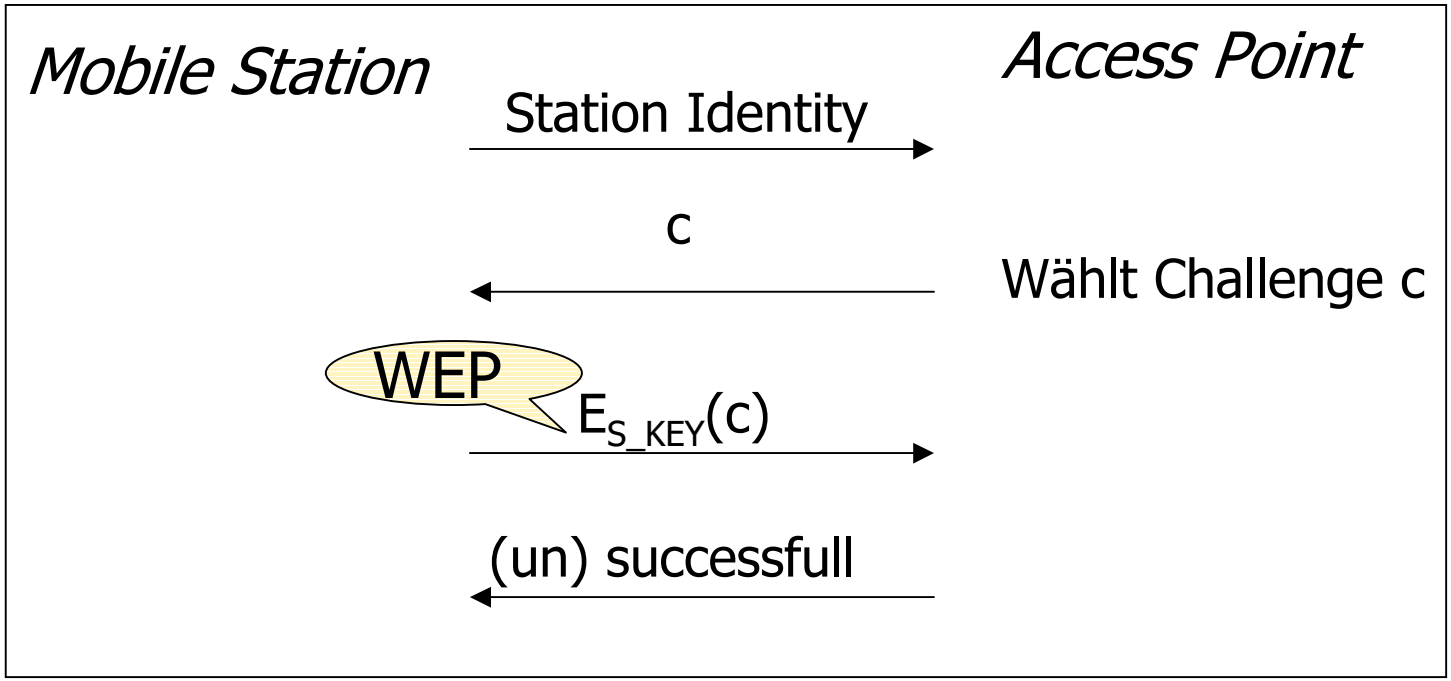
IEEE 802.11: Authentisierung

- Open System



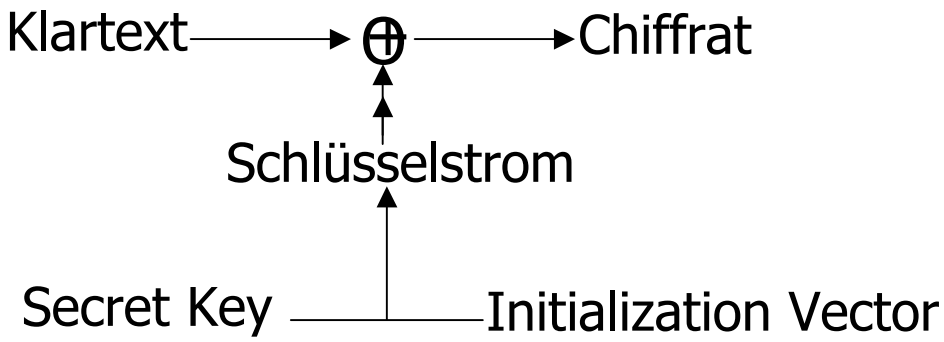
IEEE 802.11: Authentisierung

- Shared Key authentication
  - Voraussetzung: Wired Equivalent Privacy



IEEE 802.11: Verschlüsselung

- Integrity Check Field (CRC-32, 32 Bit))
- Verschlüsselung: Stream Cipher (RC4)
- Gemeinsamer Secret Key (40 Bit)
- Initialization Vector (24 bit)



IEEE 802.11: Verschlüsselung

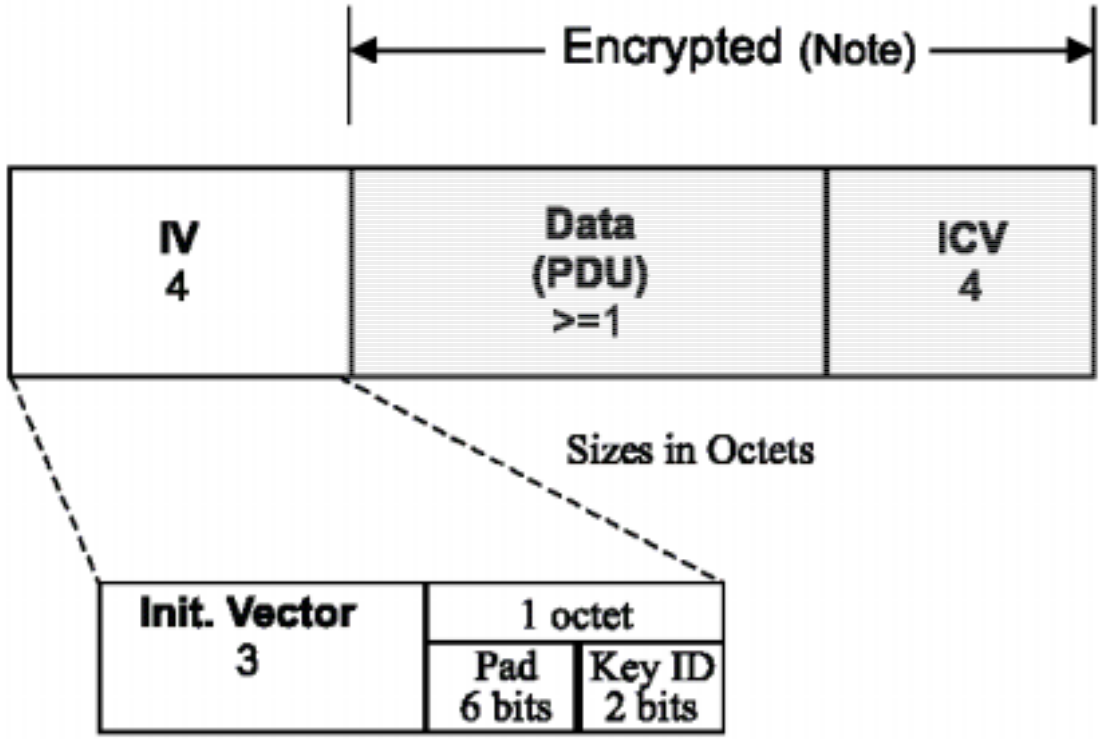


Figure 46 - Construction of expanden WEP Frame Body

IEEE 802.11: Verschlüsselung

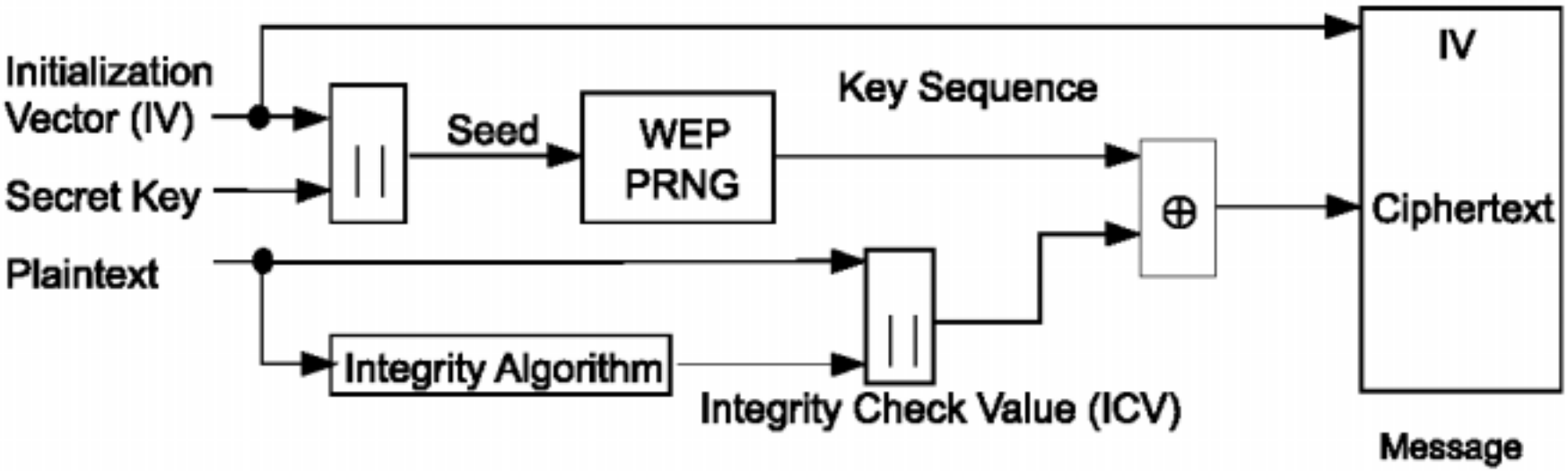


Figure 44—WEP encipherment block diagram

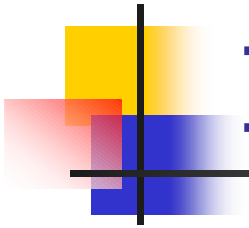
ANSI/IEEE Std 802.11, 1999 Edition

IEEE 802.11: Security Features

- Gemäss IEEE 802.11:
  - It is reasonably strong 
  - It is self-synchronizing
  - It is efficient
  - It may be exportable
  - It is optional

IEEE 802.11: Schwachstellen

- Initialization Vector (IV) wiederholt sich
  - Bei 1500 Byte Paketen bei 11Mbps nach ~5 Stunden
- Verschlüsselungsalgorithmus:
  - Gegeben: 2 Pakete mit gleichem IV und Secret Key -> RC4(X) xor RC4(Y) = X xor Y
- Checksum CRC-32
  - Nachricht ist Modifizierbar (ohne Schlüssel)



IEEE 802.11: Attacken

- Lauschen
- Nachrichten einspeisen
- Nachrichten modifizieren

IEEE 802.11: Lauschen

2 Pakete mit gleichem IV und Secret Key abfangen
-> RC4(X) xor RC4(Y) = X xor Y

- Statistische Analysen
  - Sprache
  - IP Verkehr
- Sende Nachrichten an eine Mobile Station
- Ist ein Klartext-Chiffrat Paar bekannt sind alle Pakete mit diesem IV entschlüsselbar

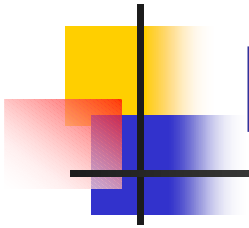
IEEE 802.11: Lauschen

- Entschlüsselungstabelle aufbauen:
  - (IV, Key stream) Paare
  - Grösse ~15 GB
  - Alle Pakete können entschlüsselt werden

IEEE 802.11: Nachrichten einspeisen

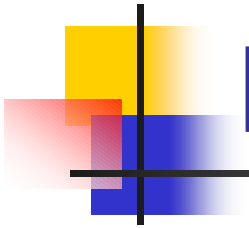
- Voraussetzung:
  Ein Klartext-Chiffrat Paar bekannt
  (X, RC4(X))
- Konstruiere neue Nachricht Y inkl. checksum
- RC4(X) xor X xor Y = RC4(Y)
- Ist ein Klartext-Chiffrat Paar bekannt, können beliebige Pakete mit diesem IV eingespeist werden.

IEEE 802.11: Nachrichten modifizieren



- Voraussetzung:
  Ein Klartext-Chiffrat Paar teilweise bekannt (zB Headerstruktur)
- Modifiziere Paket so, dass der CRC-32 trotzdem stimmt.
- Ist die Struktur der Pakete bekannt, kann der Inhalt sinnvoll modifiziert werden.

IEEE 802.11: Nachrichten modifizieren



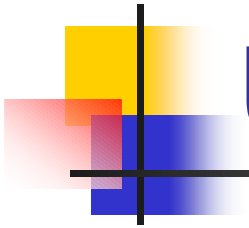
- Anwendung: Access Point überlisten
  - Voraussetzungen:
    - Position der IP Ziel Adresse im Paket bekannt.
    - Vermutungen über den Inhalt der IP Ziel Adresse
  - Modifiziere Paket so, dass die IP Adresse geändert wird, damit das Paket an einen eigenen Host geschickt wird.

IEEE 802.11: Gegenmassnahmen

- Verschlüsselung auf Application Layer (zB ssh) — Benutzer
- WEP trotzdem verwenden: — Sys Admin
  - Immerhin ein Hindernis
  - Möglichkeit juristisch vorzugehen
- Sichere Checksumme verwenden — IEEE
- Grösseren IV Raum oder anderen Verschlüsselungsalgorithmus — IEEE

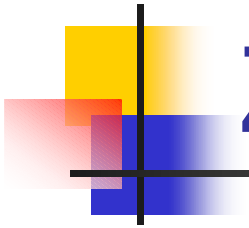
IEEE 802.11: An der ETH

- Keine Authentisierung
- Keine Verschlüsselung



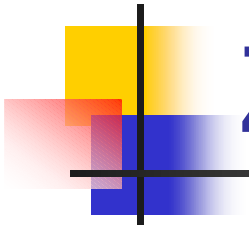
Übersicht

- Probleme mobiler Netzwerke
- Sicherheit in Bluetooth
- Sicherheit in Wireless Lans (IEEE 802.11)
- **Zusammenfassung**



Zusamenfassung

- Wann wurde die Sicherheitsspezifikation zuletzt geändert?
  - IEEE 802.11: 1999
  - Bluetooth: 1999



Zusammenfassung

	Bluetooth	IEEE 802.11
Lauschen	Ja (bei schlechter PIN)	Ja
Nachrichten einspeisen/modifizieren	Ja (bei schlechter PIN)	Ja
Schlüssel brechen	Ja (bei schlechter PIN)	
Location Attacks	Ja	Uninteressant