Drahtlose Netzwerke
Grundlagen und Einsatzfelder

Sicherheit im WLAN

Sicherheit - Ziele

- **Integrität (integrity)**
  - Es kommt das an, was abgesendet wurde.
- **Vertraulichkeit (privacy)**
  - Es können nur berechtigte Empfänger lesen.
- **Authentifikation (authentication)**
  - Sender und Empfänger wissen, mit wem sie kommunizieren.
- **Autorisierung (authorization, access control)**
  - Darf derjenige das, was er tun will?
- **Unabstreitbarkeit (non-repudiation)**
  - Es kann nachgewiesen werden, dass jemand etwas gesendet hat.
- **Verfügbarkeit (availability)**

- **Potentiell unabhängige Anforderungen!**

Angriffsformen

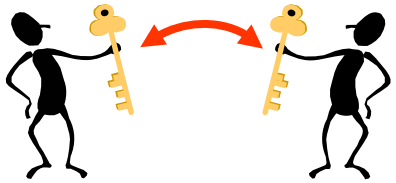
- **Passive Angriffe**
  - Lauschangriff (eavesdropping)
- **Aktive Angriffe:**
  - Maskerade (masquerading)
    - Ein Teilnehmer täuscht eine falsche Identität vor
  - Intrigieren (tampering)
    - Nachrichten werden im Lauf der Übertragung unbemerkt verfälscht
  - Wiederholen (replay)
    - Nachrichten werden gespeichert und später (unverändert) erneut abgeschickt
  - Dienstverweigerung (denial of service)
    - Dienstleistung für berechtigte Benutzer wird verhindert, z.B. durch Überlastung oder Störsender

Sicherheitsmechanismen

- **Überwiegend kryptographische Mechanismen:**
  - **Authentisierung**
    - von Datenpaketen (data origin authentication)
    - von Systemen/Benutzern (entity authentication)
  - **Integritätssicherung** (integrity protection)
    - häufig kombiniert mit Daten-Authentisierung
  - **Verschlüsselung** (encryption)
  - **Schlüsselaustausch** (key exchange)
- **Ohne kryptographische Mechanismen:**
  - **Zugriffskontrolle** (access control)
  - **Einbruchserkennung** (intrusion detection; hier nicht behandelt)

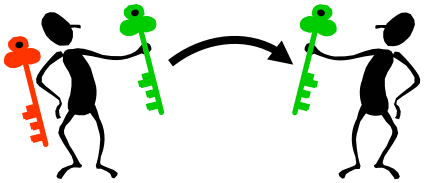
Kryptographieverfahren

Symmetrische Kryptographie



- **Instanzen besitzen gemeinsamen geheimen Schlüssel.**
- Vorteile:
  - geringer Rechenaufwand
  - kurze Schlüssel
- Nachteile:
  - Schlüsselaustausch schwierig
  - keine Verbindlichkeit

Asymmetrische Kryptographie (Public-Key-Kryptographie)



- **Schlüsselpaar aus privatem und öffentlichem Schlüssel**
- Vorteile:
  - öffentliche Schlüssel sind relativ leicht verteilbar
  - Verbindlichkeit möglich
- Nachteile:
  - hoher Rechenaufwand
  - längere Schlüssel

Sicherheitsprobleme im WLAN (1)

- **Störsender**
  - WLAN-Devices oder andere ISM-Band Geräte (Mikrowelle)
  - DoS-Attacke („Jamming“)
- **Eindringen in WLAN**
  - Einschleusen von nicht autorisierten Stationen
  - Betrieb von nicht genehmigten APs
- **Abhören und Monitoren von Nachrichten**
  - Des WLANs (physikalisch im Umkreis immer möglich)
  - Broadcasts eines über einen Hub angeschlossenen Ethernets

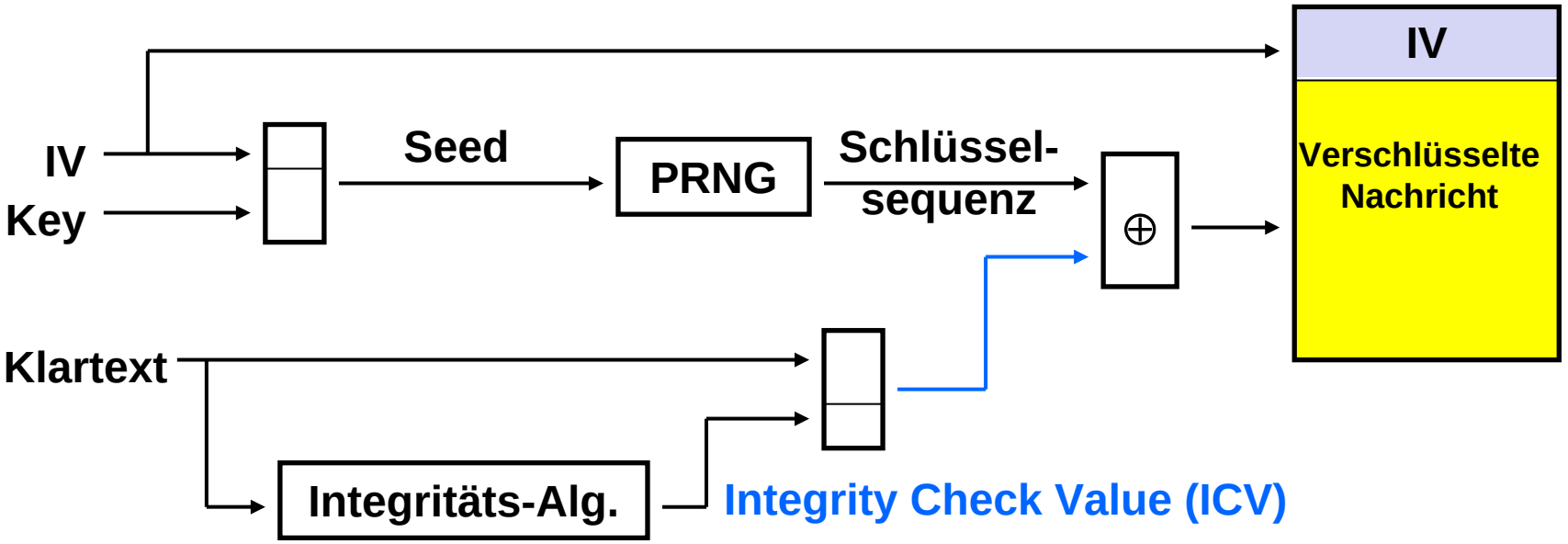
Sicherheitsprobleme im WLAN (2)

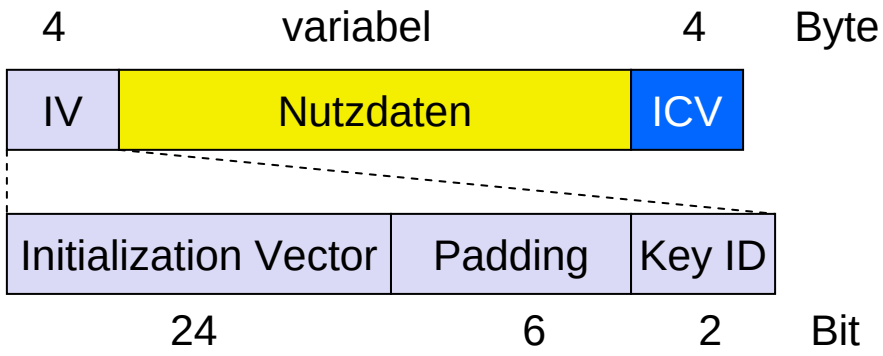
- **Angriffe gegen das WEP-Passwort**
  - Brute-Force
  - Wörterbuch
  - Social Engineering
- **Angriffe gegen den WEP-Verschlüsselungs-Algorithmus**
- **Fehlkonfigurationen**
  - Default ist meist „Keine Sicherheit“
  - Bei nicht veränderten Defaults ist das WLAN offen
    - Default SSID
    - WEP ausgeschaltet
    - Default SNMP Password
    - Default Password für Konfigurationsinterface (z.B. HTML, telnet)

WEP: Eigenschaften

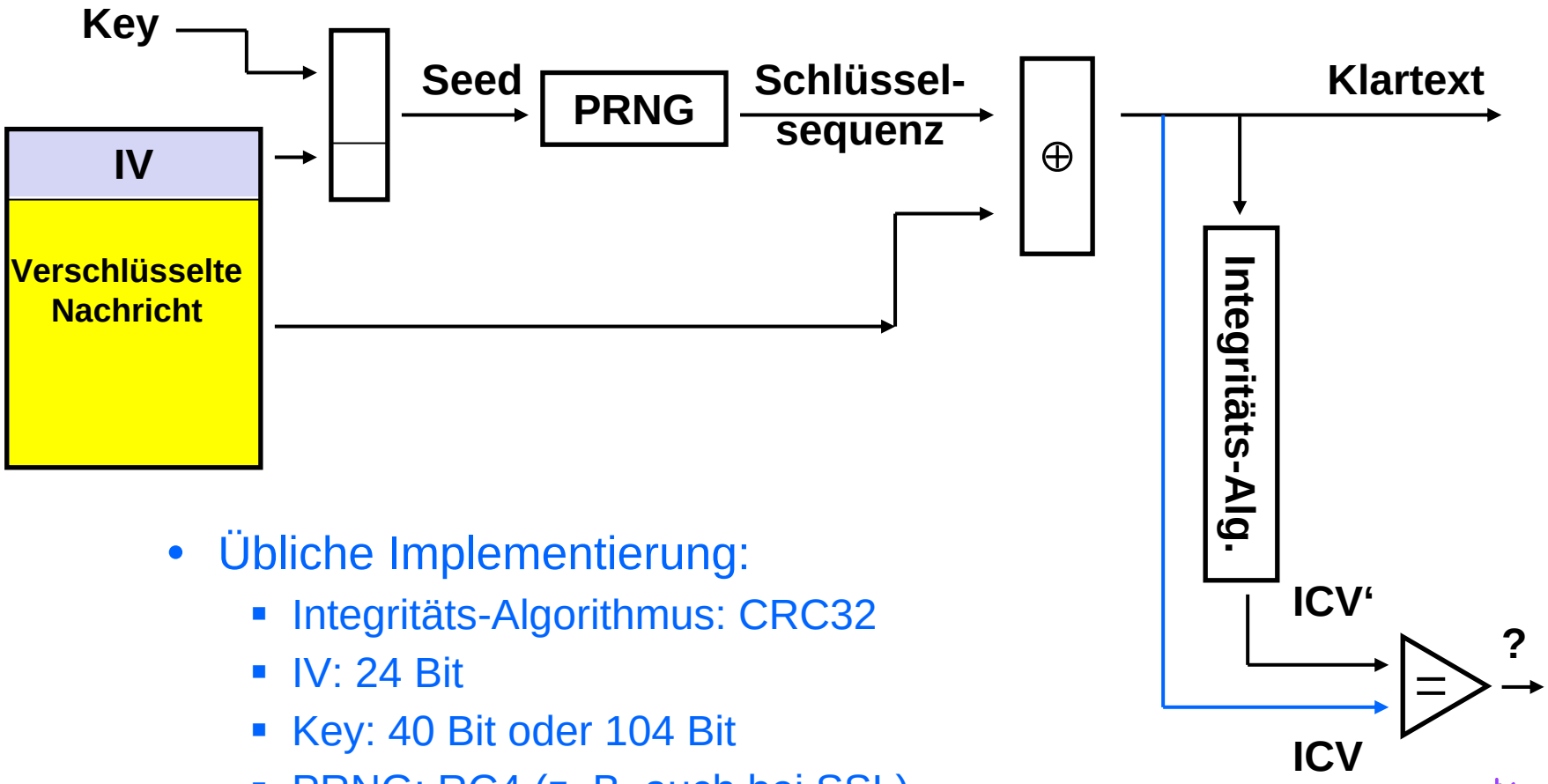
- **„Wired Equivalent Privacy“**
- **Eigenschaften (laut 802.11-1999):**
  - angemessen sicher („reasonable strong“)
    - WEP-Schlüssel schwer knackbar, auch mit Brute-Force
    - Initialisierungsvektor ständig geändert
  - selbst-synchronisierend („self-synchronizing“)
  - effizient
    - In Soft- oder Hardware implementierbar
  - exportierbar
    - nicht „so stark“, dass kein Export aus den USA erlaubt
  - optional
    - Entwickler: ob sie es implementieren wollen
    - Nutzer: ob sie es nutzen wollen

WEP-Verschlüsselung





WEP-Entschlüsselung



- Übliche Implementierung:
  - Integritäts-Algorithmus: CRC32
  - IV: 24 Bit
  - Key: 40 Bit oder 104 Bit
  - PRNG: RC4 (z. B. auch bei SSL)

Sicherheitsmechanismen im WLAN (Wiederholung)

- **Standard-Mechanismen der Sicherungsschicht**
  - Verschlüsselung (WEP)
    - symmetrisch
  - Authentifizierung
    - Aufsetzend auf Verschlüsselung
  - Zugangskontrolle
    - Über die MAC-Adressen
- **Was wird damit erreicht?**
  - Vertraulichkeit, Integrität (wenn WEP funktioniert)
  - Authentizität, Autorisierung (eingeschränkt auf eine Gruppe)
- **Schwächen von WEP**
  - Symmetrisches Verfahren mit nur einem Schlüssel
  - Keine Schlüsselverteilung
  - WEP ist keine starke Kryptographie

Angriffe auf WEP (1)

- **Idee: Ausnutzung der Wiederholung der IVs**
  - Princy C. Mehta: Wired Equivalent Privacy Vulnerability
- **Der IV hat 24 Bit:**

$$\frac{1500\ bytes}{packet} \times \frac{8\ bits}{1\ byte} \times \frac{1\ \text{sec}}{11\ Mbits} \times \frac{1\ Mbit}{10^6\ bits} \times 2^{24}\ packets \approx 18{,}300\ \text{sec} \approx 5\ hrs$$

- **Alle 5 Stunden wiederholt sich der IV auf einem ausgelasteten (11 Mbit) Netz**
- **Datenmenge: 2^{24} = 16.777.216 Frames = max. 24 GB**
- **Statistische Analyse**
  - XOR der verschlüsselten Frames entspricht XOR der unverschlüsselten Frames

➔ **Lösungsmöglichkeit: 48 Bit IV (WPA, 802.11i)**

Angriffe auf WEP (2)

- **Idee: Durch naive Wahl der IVs**
  - N. Borisov, I. Goldberg, D. Wagner: Intercepting mobile communications: The insecurity of 802.11
- **Der Standard schreibt nichts über die Erzeugung der IVs vor**
- **Einige Karten starten nach jeden Reset bei 0 und zählen aufwärts**
  - Es ist viel einfacher zwei Frames mit gleichem IV zu finden

Angriffe auf WEP (3)

- **Idee: Durch die Nutzung von schwachen IVs**
  - S. Fluhrer, I. Mantin, and A. Shamir : Weaknesses in the Key Scheduling Algorithm of RC4
  - A. Stubblefield, J. Ioannidis, A. D. Rubin: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
- **Bestimmte IVs verraten 1 Byte des Schlüssels**
- **Benötigt wenige Frames um den Schlüssel zu finden**
  - 4.000.000 – 6.000.000 = max. 8,5 GB
- **Wenn WEP-Schlüssel aus ASCII-String erzeugt werden**
  - 1.000.000 – 2.000.000 Frames = max. 2,8 GB
- **z.B. Tool „AirSnort“ für Linux**

Angriffe auf WEP (4)

- **Idee: IP-Verkehr mit viel „Known-Plaintext“**
  - z. B. ICMP, ARP, TCP ACK, ...
- **Senden aus dem Internet an die angegriffene Station**
- **➔Stück der Länge N der Pseudozufallszahlenfolge**
  - IV ist bekannt
- **Man kann Nachrichten der Länge N fälschen**
  - Durch Wiederverwendung des bekannten IV
- **Abwandlung: Partial Known-Plaintext**
  - z. B. in IP-Headern

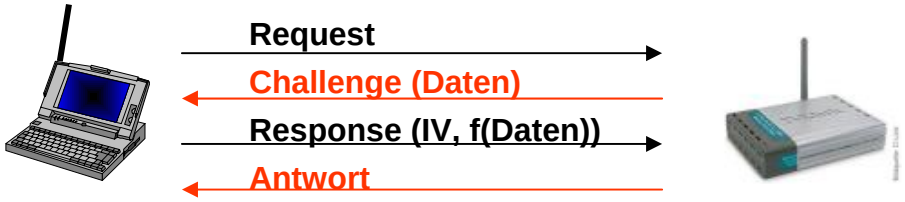
Angriffe auf WEP (5)

- **Idee: WEP ohne kryptographische Prüfsumme (ICV)**
  - Linearabbildung CRC lässt Vorhersage zu
- **Mit N-Byte Pseudozufallszahlenfolge lassen sich Authentifikation, Dis/Re/Association und Beacons senden**
- **Angriffe:**
  - Denial-of-Service durch Disassociation einer Station
  - Vortäuschung eines APs durch eigene Beacons

➔ **Kryptographische Prüfsumme notwendig!**

Angriffe auf WEP (6)

- **Authentifizierung ohne Kenntnis des WEP-Keys!**
  - Authentifizierung:



  - Dabei:
    - Daten: „Zufälliger“ Wert als „Herausforderung“ vom AP
    - f: Verschlüsselungsfunktion: f(x) = x XOR Schlüsselstrom
  - Also: Schlüsselstrom = x XOR f(x)

➔ Durch erlauschte Authentifizierung ist eine eigene Authentifizierung möglich!

➔ Aber: NOCH keine Kommunikation

WEP-Schwächen (Wdhlg.)

- **RC4-Stromverschlüsseler benötigt für jedes Datenpaket neuen Schlüssel**
  - WEP-Schlüssel + IV zu kurz, nicht zufällig genug
- **WEP-Schlüssel statisch**
  - Known-Plaintext ermöglicht ermitteln der Schlüsselströme, die zu jedem IV gehören
- **CRC32 zur Integritätssicherung (ICV)**
  - Unsicher, Manipulationen können unentdeckt bleiben

Verbesserungen

- **„Fast Packet Keying“ (FPK)**
  - Schlüssel (104 Bit) und IV (24 Bit) dynamisieren:
    - Aus (konstantem) WEP-Schlüssel, Sender-MAC + ‚Packet IV‘ gehasht

    ➔(IV, Schlüsselstrom) wiederholen sich erst nach $4 \cdot 10^{21}$ Jahren

- **„Temporal Key Integrity Protocol“ (TKIP)**
  - „erweitertes FPK“:
    - Ziel-MAC fließt mit ein
    - Vorheriges Paket fließt mit ein

    ➔ „packet ordering“ → keine „Wahl“ des IV mehr möglich
  - Checksumme: Kryptographisch sicher, kein CRC mehr

WPA

- **Wireless Protected Access (WPA)**
  - war Vorgriff auf 802.11i
  - IV mit 48 Bit Länge
  - Benutzt TKIP
  - Einsatz von IEEE 802.1x Authentifikation
  - Key 128 Bit, bei jeder Assoziation ausgehandelt
  - Key mit IEEE 802.1x periodisch gewechselt

- **802.1x:**
  - Trennung „Authentifizierungs-Kommunikation“ und „Daten“
  - Solange nicht Authentifiziert nur Kommunikation mit Auth.-Server

IEEE 802.11i (WPA2)

- **IEEE 802.11i (WPA2)**
  - Ähnlich WPA, aber:
  - AES (Blockchiffrierer), „Nachfolger“ von RC4
  - Mit Passphrase oder Zertifikaten (802.1x, RADIUS)