ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Sicherheit in GSM, UMTS, WEP, WPA und TinySec

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Sicherheitsanforderungen Mobiltelefone

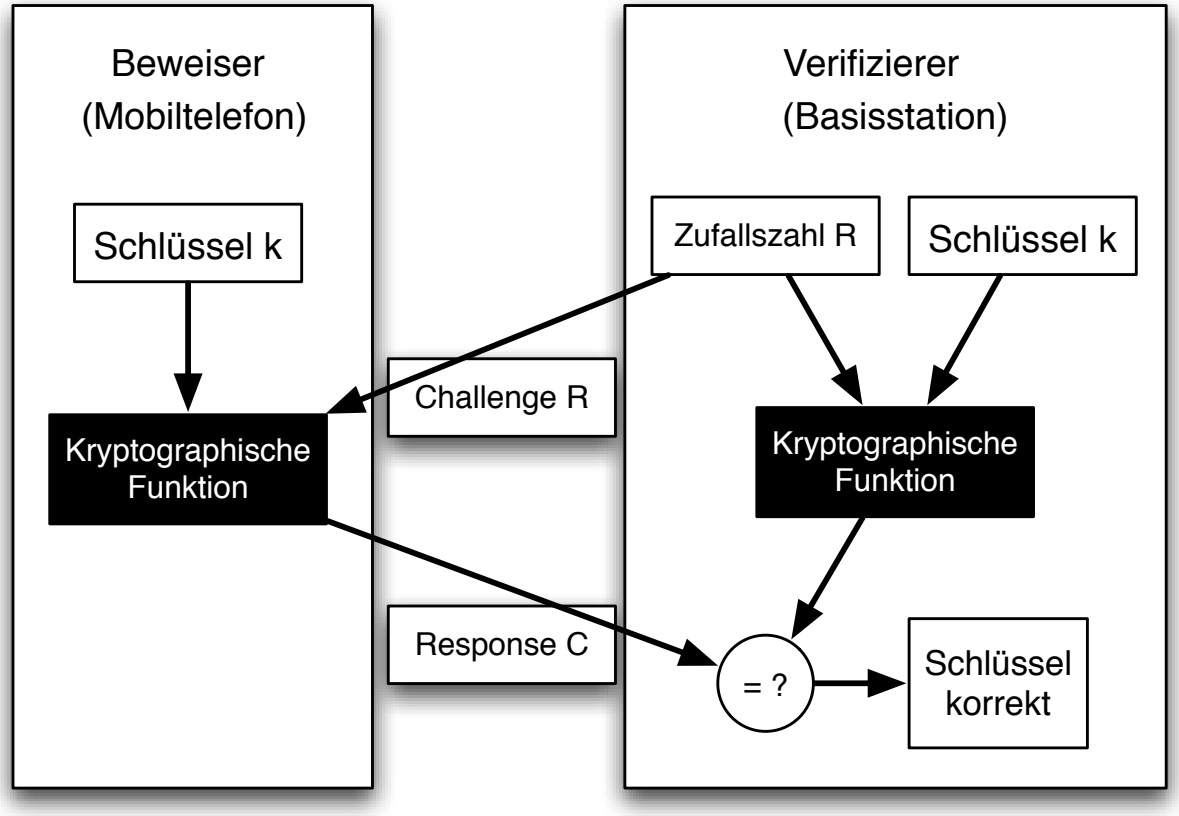
- **Netzwerkanbieter**
  - Authentifizierung des Benutzers
  - korrekte Abrechnung, kein Missbrauch
  - Effizienz (geringer Overhead)
- **Benutzersicht**
  - Vertraulichkeit
  - Keine Benutzerprofile
  - Verbindung mit der angegebenen Basisstation
  - korrekte Abrechnung

Sicherheitsalgorithmen GSM

- **SIM-Karte (Smartcard)**
  - 128-Bit-Schlüssel
  - Benutzer: PIN und PUK
- **Smartcard-basierte Authentifizierung**
  - mit nicht standardisierten Algorithmus A3
- **Anonymität**
  - Verwendung temporärer Identifikationen
- **Verschlüsselung zur Basisstation**
  - A5/3 (Kasami)-Algorithmus
  - ersetzte unsichere Vorgänger A5/1, A5/2

Challenge-Response-Authentifizierung

- **Challenge-Response**
  - Basis-Station sendet Zufallszahl R (Challenge)
  - Mobiltelefon
    - berechnet C=A3(K, R)
      - für Kartenschlüssel K
    - sendet C an Basisstation (Response)
  - Basis-Station überprüft Ergebnis
- **Motivation**
  - keine geheimen Schlüssel werden übermittelt
  - keine Replay-Attacken möglich



Verbesserungen in UMTS

- **Verschlüsselung endet nicht mehr in der Basisstation**
- **Temporäre Kommunikationsschlüssel**
  - Regelmäßige Erneuerung
    - in Abhängigkeit von Zeit und Datenmenge
  - Symmetrischer 128-Bit-Schlüssel
- **Netz authentifiziert sich gegenüber dem Benutzer**
- **UMTS verwendet verbesserte, öffentliche, symmetrische Verschlüsselung**

Sicherheitsaufgaben im WLAN

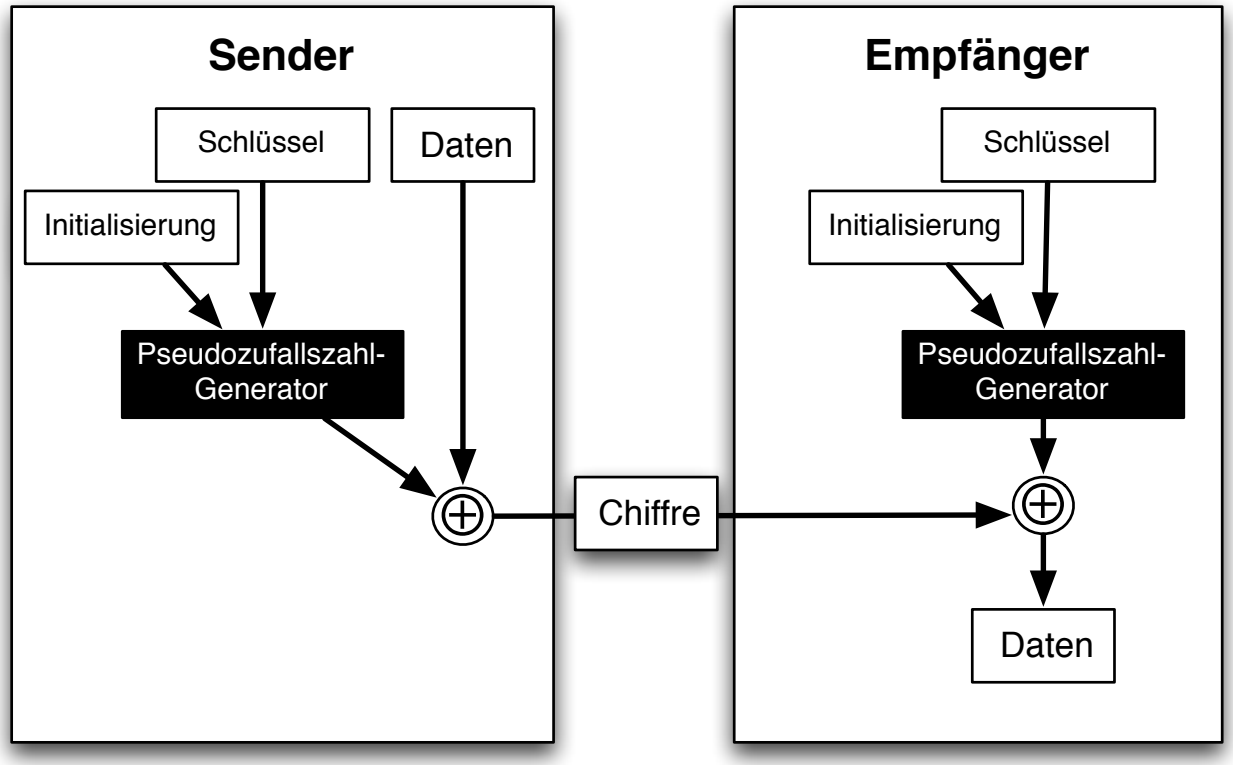
- **Authentifizierung**
  - der Nutzer oder
  - des Geräts
- **Schutz der übermittelten Daten**
  - gegen Abhören
  - und Verfälschung
- **Probleme**
  - Hacker-Software weit verbreitet
  - Geräte sind frei programmierbar und weit verbreitet

Wired Equivalent Privacy

- **Sicherheitsmechanismus für 802.11 WLAN**
  - gegen Abhören von Nachrichten
  - Seit 2001 erhebliche Schwachstellen bekannt
- **64-Bit-WEP verwendet 40-Bit-Schlüssel**
  - verwendet symmetrische Strom-Kodierung RC4
  - alternativ 128-bit WEP (104 Bit-Schlüssel)
  - mit jeweils 24 Bit für Initialisierung
- **Schwächen**
  - Keine Nachricht darf sich wiederholen
  - Auch für große Schlüssel unsicher
  - kein Schlüsselmanagement

Strom-Kodierung

- **Verschlüsselungs-Algorithmus**
  - Eingabe als Byte-Strom (Folge von Bytes)
  - Bitweises Xor mit Pseudozufallsfolge
- **Entschlüsselung**
  - Bitweises Xor mit selber Pseudozufallsfolge
- **Wichtig:**
  - Austausch der Initialisierung des Zufallsgenerators
  - Synchrones Arbeiten
- **Beispiel:**
  - Rivest Code 4 (RC-4)



WPA

- **WPA: Wi-Fi Protected Access**
  - Sichere Verbesserung gegenüber WEP
  - Verwendet Authentifizierungsserver
    - Extensible Authenticiation Protocol (EAP)
  - oder pre-shared key mode (PSK) für kleinere Netze
- **Verwendet RC4-Stromkodierung mit 128 bit keys**
  - Dynamischer Schlüsselwechsel mittels Temporal Key Integrity Protocol (TKIP)
- **Statt CRC bessere Datenintegrität durch Message Integrity Code (MIC)**
- **Frame-Zähler verhindert Replay-Angriffe**

Weitere Maßnahmen in 802.11

- **Abschottung des unsicheren WLAN von drahtgebundenen Intranet-LAN**
- **Weitere Sicherheitsschichten in höheren Schichten**
  - IPSec oder SSL oder SSH
- **Zusätzliche Authentifizierung**
  - z.B. VPN (Virtual Private Network)
- **Zulassung nur von registrierten MAC-Adressen**
- **Unterdrückung des Netzwerknames**
- **In Zukunft:**
  - Verwendung von AES statt RC4

Sicherheitsrisiken in Drahtlosen Sensornetzen

- **Abhören von Nachrichten**
  - Bruch der Vertraulichkeit
- **Verfälschen und Einfügen falscher Pakete**
  - Zugriffskontrolle
  - Integrität
- **Störung der Kommunikation**
  - Wiedervorspielen von alten Nachrichten (Replay-Attacke)
  - Denial of Service

TinySec

- **Karlof, Sastr, Wagner**
  - TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, SenSys 2004
- **Sicherheitsschicht für drahtlose Sensornetze**
- **Ziele**
  - Zugriffskontrolle
  - Integrität von Nachrichten
  - Vertraulichkeit
  - Transparenz für Anwendungen und Programmierer

TinySec-Design

- **Ein gemeinsamer globaler symmetrischer kryptographischer Schlüssel**
- **Verschlüsselung in der Verbindungsschicht (Link layer)**
  - Verschlüsselung und Schutz der Integrität
  - Transparenz für Anwendungen
- **Verwendung von symmetrischen blockweisen Verschlüsselungen**
  - **wahlweise DES, AES, Skipjack, RC5**
  - **erzeugt auch Nachrichtenunterschriften**
    - Message Authentification Codes (MAC)

Diskussion TinySec

- **TinySec ermöglicht**
  - Zugriffskontrolle
  - Integrität der Nachrichten
  - Vertraulichkeit
- **TinySec verhindert nicht**
  - Störung
  - Kompromittierung eines Knoten oder Schlüssels
  - Replay-Attacke
  - Denial of service

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer