Sicherheitsaspekte drahtloser Datenübertragungsverfahren WLAN, Bluetooth, GSM, DECT

48. Weinheimer UKW-Tagung 2003, Weinheim

Dipl-Ing Erich H. Franke
DK6II
Königsbach-Stein
erich.franke@afusoft.de
http://www.afusoft.de

‚Treiber' der Digitalisierung

- Schutz der übertragenen Information
  - Vor unbefugtem Zugriff
    - Verschüsselung einfacher zu realisieren als analog
    - Dto. „Digitales Rechte-Management"
  - Vor unbefugter Verfälschung
- Mehrfach-Dienste-Fähigkeit
  - Sprache + Bilder + Daten (‚Multi-Media')
  - Mehrere Informationsströme verschachtelt
- Theoretisch gleichbleibende Qualität
  - Solange, bis die Verbindung eben abreißt…

Szenarien und Angriffe

- Abhören
  - Inhaltsauswertung
  - Standortbestimmung und Bewegungsprofile
- Täuschen und Sabotage
  - Vortäuschen einer Identität
  - Unbefugte Nutzung
  - Stören, ‚Denial-of-Service‘
- Sonstige
  - Abhören von Raumgesprächen

Zielsetzungen von Angreifern

- Direkt
  - Nutzung des Übertragungsdienstes
    - Z.B.: Phone Phreaking, Cable Pirating, Deferred access
    - Z.B.: ‚Wir surfen auf des Nachbars Kosten...‘
  - Unterbrechung des Dienstes
    - ‚illegal‘: z.B. kriminell/terroristisch
    - ‚legal‘: z.B. Strafvereitelung

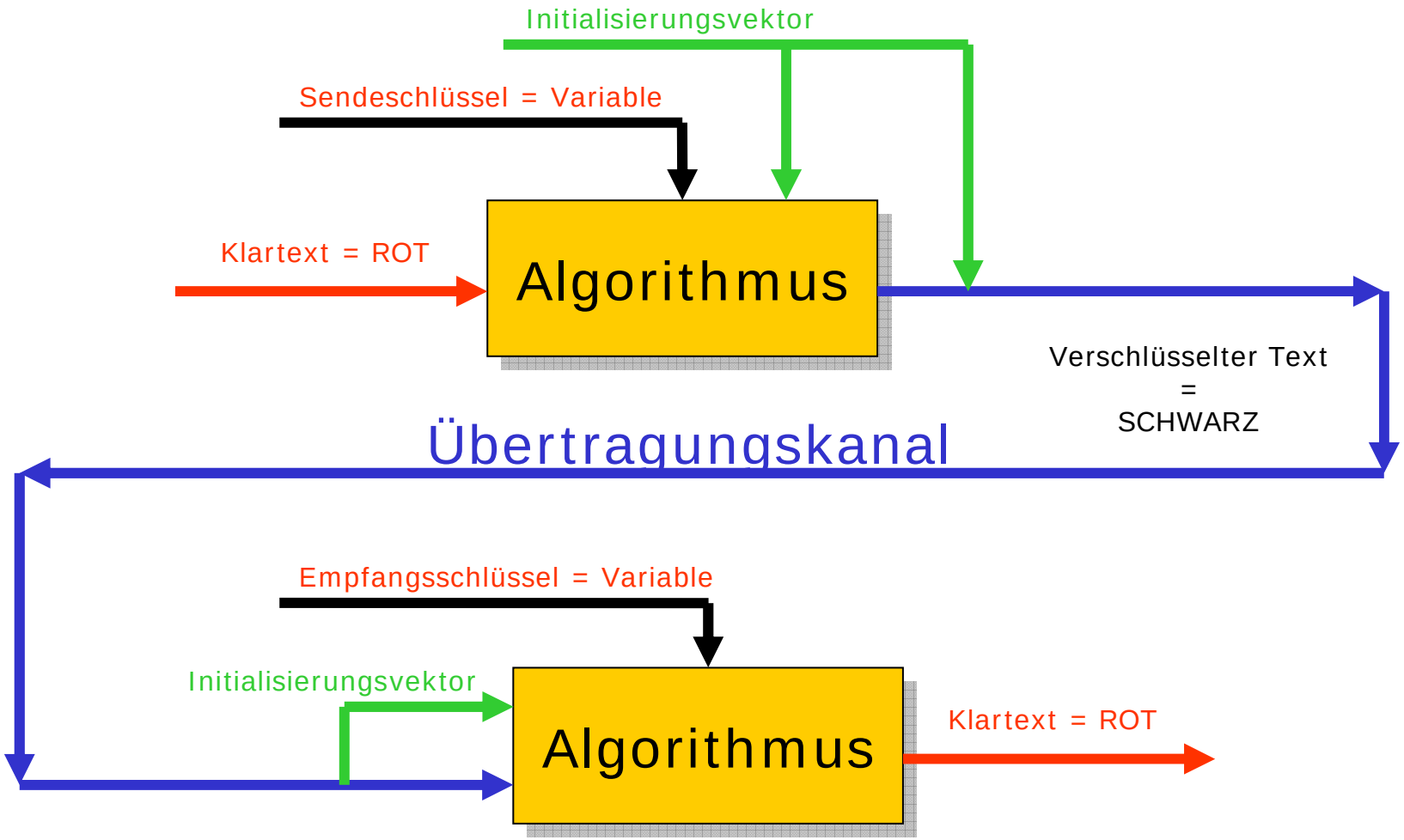
- Indirekt
  - Als ‚Eintrittskarte‘ in Rechnernetze
    - Z.B.: WLAN ‚War Driving‘

Maßnahmen

- Authentisierung
  - Schutz der Zugangsberechtigung
- Verschlüsselung
  - Schutz des Nachrichteninhaltes vor Ausspähung
- Signatur
  - Schutz des Nachrichteninhaltes vor Verfälschung

...Basis hierfür sind kryptologische Verfahren

Grundlage (fast aller) Verfahren



Definitionen (1)

- Variable (Schlüssel)
  - Ist geheim zu halten
  - Muss ausreichend viele Variationen erlauben
  - Muss ausreichend oft gewechselt werden
  - Darf nicht ‚erratbar' sein

- Initialisierungsvektor (IV)
  - Ist als offen zu betrachten
  - Soll ausreichend viele Variationen sicherstellen
  - Darf nicht vorhersehbar sein

Definitionen (2)

- Algorithmus
  - Muss als offen angesehen werden, d.h. Geheimhaltung darf keine Schutznotwendigkeit sein (Kerkhoff et. al.)
  - Darf Schlüssel auch dann nicht kompromittieren, wenn man Klartext und zugehörenden verschlüsselten Text besitzt
  - Bits der Variablen und des IV müssen möglichst ‚große' Auswirkungen auf die Verschlüsselung besitzen

Risiken und Nebenwirkungen

- Brute Force-Angriff auf den Schlüssel
  - Blindes ‚Durchprobieren' aller Kombinationen
- Modified Brute Force (‚Chosen Challenge')
  - Bei bekannten Schwachstellen, z.B. wenn Änderungen an der Variablen ‚leicht vorhersehbare' Änderungen der Verschlüsselung bewirken
- Back Door Access
  - Algorithmus ist Teil des ‚Geheimnis' ist und wurde kompromittiert
  - Verschlüsselung wurde umgangen

Varianten der Verschlüsselung

- Symmetrische Verfahren
  - Variable zum Ver- und Entschlüsseln sind identisch.
  - Sie müssen zu Sender und Empfänger verteilt werden
  - Einfach zu implementieren

- Asymmetrische Verfahren
  - Die Variablen sind abhängig aber nicht umrechenbar
  - Eine Hälfte der Variablen kann ‚veröffentlicht' werden
  - Auch sehr gut zur Authentisierung geeignet (Signatur)

Varianten der Authentisierung

Verifier	Claimant
Erzeugt eine zufällige Anfrage (Challenge)	
Verarbeitet seine eigene Anfrage mit dem ihm selbst bekannten ‚Geheimnis‘	Verarbeitet die Anfrage mit dem ihm bekannten ‚Geheimnis‘ (Response)
Vergleicht die ‚verarbeitete‘ Antwort des Claimants mit dem selbst erarbeiteten Ergebnis	

Praktische Beispiele: GSM

Eckdaten

- Teilnehmerkennung IMSI (15 Ziffern)
- Gerätekennung IMEI (15 Ziffern)
- Geheimer Schlüssel K_i (128 Bit, auf SIM-Karte)
- Gegenpart im Netz: AUC (Authentification Center)
- Einseitige Authentisierung

Praktische Beispiele: GSM

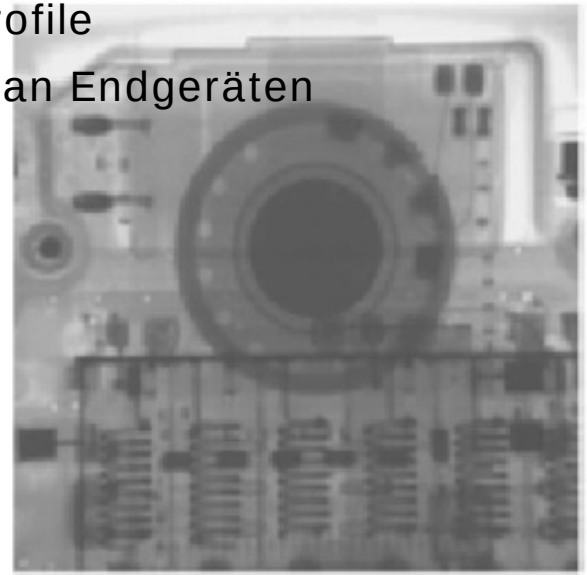
Problempunkte

- Authentisierung nur einseitig (Netz authentisiert Mobilteil)
  - Anfälligkeit gegen ‚gefälschte Netzknoten'
- Schwachstellen in den Algorithmen, kombiniert mit Schwachstellen der SIM-Karte
  - COMP-128 anfällig gegen Angriffe mit ausgewählten Texten
  - SIM-Karte erlaubt fortgesetzte Authentisierungsversuche, daher ist o.g. Schwachstelle ausbeutbar (150k Versuche, ca 8h, [DUD]). Bei UMTS durch AUTN behoben!)
  - Angriff benötigt Zugang zur SIM-Karte
- Kurze (zusätzlich künstlich verkürzte) Variablen
  - 64 Bit Nachrichtenschlüssel wird (wurde?) auf 54 Bit verkürzt

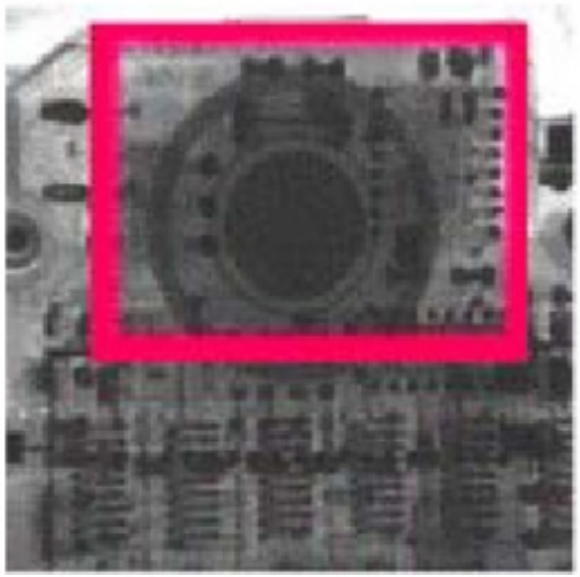
Praktische Beispiele: GSM

Weitere Problempunkte

- Funktionsvielfalt der Endgeräte erlaubt bestimmte Attacken
  - Speziell geformte ‚fehlerhafte' SMS
  - Upload von JAVA-Applets
  - Bewegungsprofile
  - Manipulation an Endgeräten
    (Quelle BSI)



Referenzröntgenbild eines Mobiltelefons (Teilansicht)



Röntgenbild eines hardware-manipulierten Mobiltelefons (Teilansicht)

Praktische Beispiele: WLAN

Eckdaten

- Variablenlängen von 104 bzw. 40 Bit (WEP 128 bzw. 64)
- MAC-Filter (Zugang nur für ‚bekannte MAC-Adressen)
- Einseitiges Authentisierungsverfahren mit 128 Bit Vektor und Challenge/Response
- IV mit 24 Bit
- Keine Verteilmechanismen für die Variablen
- SSID Broadcast

Praktische Beispiele: WLAN

Problemkreise

- Variablenlängen von 104 Bit bzw. 40 Bit zu kurz
- MAC-Filter ist nur ein schwacher Schutz
- Authentisierungsverfahren kompromittiert einen Teil der Schlüsselbitfolge
- IV mit 24 Bit viel zu kurz, d.h. häufige Wiederholungen einer Schlüsselsequenz nach ca. 4000 Paketen
- Kein Schutz gegen Wiederholungen des IV (Recorder Spoof)
- Schwäche im Algorithmus RC4 erlaubt gezielten Angriff (Fluhrer, Mantin, Shamir, 2001) t ~ 65Min

Einige Gegenmaßnahmen

- Reichweite einschränken
  - Antennenposition, Sendeleistung
- Variablen ausreichend oft wechseln
  - Möglichst in kürzeren Abständen als Angriffe möglich sind
  - RADIUS benutzen
- Kompromittierung vermeiden
  - Geeignete Wahl und Aufbewahrung von PIN und Passphrases.
- Anmeldung in hinreichend abhörsicherer Umgebung
  - Bluetooth-Pairing bzw. DECT-Anmeldung
- Firewalls verwenden wo immer möglich
- Systeme / Logs überwachen (Auditing)