Sicherheit mobiler Kommunikation

Hendrik Tews

Institut für Theoretische Informatik, TU Dresden

http://wwwtcs.inf.tu-dresden.de/∼tews/

Teilnehmer sind mobil

- mobiles telefonieren $\surd$
- mobiles Internet (mobile IP)
- ad hoc Netzwerke

I. mehrseitige Sicherheit

II. GSM — mobil telefonieren in der Gegenwart
(global system for mobile communications)
- Geschichte
- Funktionsweise
- Bedrohungen
- bekannte Angriffe

III. UMTS — die Zukunft
(universal mobile telecommunications system)

IV. Literatur / Ausklang

Schutz / Bedrohung	Inhalt	Kommunikationsumstände
Zugriff auf Informationen	Vertraulichkeit (confidentiality) Unsichtbarkeit (hiding)	Anonymität/Pseudonymität Unbeobachtbarkeit Unverkettbarkeit (unlinkability)
Modifikation	Integrität	Zurechenbarkeit (accountability)
Beeinträchtigung der Funktionalität	Erreichbarkeit / Verfügbarkeit	rechtliche Bindung

(nach Pfitzmann, Wolf, Federrath)

Einem Angreifer/Kommunikationspartner bleibt verborgen

Vertraulichkeit
der Inhalt der Kommunikation

Unsichtbarkeit
dass eine Kommunikation stattfindet

Anonymität
die Identität der Kommunikationspartner

Pseudonymität
die Identität der Kommunikationspartner,
es können jedoch Rechnungen erstellt werden

Unbeobachtbarkeit
die Aufenthaltsorte der Kommunikationspartner
dass Kommunikationsgeräte benutzt werden

Unverkettbarkeit
welche Aktionen vom gleichen Teilnehmer stammen

Integrität

Integrität
die Nachricht kann nicht modifiziert werden,
bzw. Modifikationen werden erkannt
Verdopplungen der Nachricht werden erkannt

Zurechenbarkeit
Kommunikation ist beweisbar
weder Sender noch Empfänger können abstreiten
an der Kommunikation teilgenommen zu haben

Verfügbarkeit

rechtliche Bindung
Betrügen unmöglich

Erreichbarkeit
Teilnehmer sind erreichbar, wenn sie das wollen

Verfügbarkeit
Ressourcen stehen ausreichend zur Verfügung

Abhängigkeiten

$$
\begin{tikzcd}
\text{Vertraulichkeit} & \text{Anonymität} \\
\text{Unsichtbarkeit} \arrow[u] & \text{Unbeobachtbarkeit} \arrow[l] \arrow[u] \\
\text{Integrität} & \text{Zurechenbarkeit} \arrow[l] \\
\text{Verfügbarkeit} \arrow[u] & \text{rechtliche Bindung} \arrow[u]
\end{tikzcd}
$$

Unterscheidung nach Partnern/Gegnern

Sicherheit ist immer mehrseitige Sicherheit

- Teilnehmer können Schutzziele formulieren
- und aushandeln (gegebenenfalls abbrechen)

kryptographische Methoden

Vertraulichkeit	Verschlüsselung
Unsichtbarkeit	Steganographie
Anonymität	implizite Adressierung, Mixe
Integrität	Authentisierung *Challenge–Response* assymetrische Kryptosysteme
Zurechenbarkeit	digitale Signaturen

Geschichte

1958 A–Netz, erstes Mobilfunknetz in Deutschland

- 160 MHz, analog, handvermittelt
- keine Anrufe aus dem Festnetz, keine Verbindungsübergabe
- bis 1971 80% Flächendeckung und 11.000 Kunden

1972 B–Netz

- ebenfalls 160 MHz
- Anrufe aus dem Festnetz, wenn Aufenthaltsort bekannt
- nur mit Auto mobil
- 1979 13.000 Kunden

- ähnliche Entwicklungen in anderen Ländern führten zu mehreren inkompatiblen Systemen

1982 Gründung von GSM (Groupe Spéciale Mobile), Ziele:

- europäischer Standard
- digital
- Roaming (Netzwechsel)

1986 C–Netz

- 450 MHz, Sprache analog, Signalisierung digital auf einem Kanal
- etwa 500.000 Kunden
- automatische Lokalisierung, Verbindungsübergabe, erste Sicherheitsfunktionen
- 2001 abgeschaltet

1992 D-Netze

Angriffspunkte

- Endgeräte
  - Sicherheit
  - Fälschung
- Luftschnittstelle
- erste Basisstation
- ortsfestes Netzwerk
  - Vermittlungsrechner, Datenbanken
  - Leitungen
  - Richtfunk

Besonderheiten im Mobilfunk

- Endgeräte klein, Massenmarkt
  $\longrightarrow$ Diebstahl

- Kunde & Netz kennen sich nicht
  $\longrightarrow$ Authentisierung

- Lokalisierungsdaten

SIM (subscriber identity module), Chipkarte, speichert persönliche Daten
permanente Daten:

IMSI (International mobile subscriber identity) $\approx$ internationale Telefonnummer
$\boldsymbol{Ki}$ teilnehmerspezifischer Schlüssel
A3/A8 Algorithmen zur Authentifizierung/Verschlüsselung
PIN (personal identification number)

temporäre Daten:

TMSI (temporary mobile subscriber identity), zeitweilige Identifikationsnummer
$\boldsymbol{Kc}$ Chiffrierschlüssel Kc,
LAI (location area identification) $\approx$ Aufenthaltsort

MS (mobile station) Mobiltelefon (unpersönlich)

BSS (base station subsystem) $\approx$ Basisstation mit Sender
BSC – base station controller
BST – base transceiver station

HLR/VLR/AuC (home location register / visitor location register / authentification centre)
Datenbanken:

- Teilnehmernummer (IMSI)
- letzter Aufenthaltsort (LAI)
- teilnehmerspezifischer Schlüssel Ki
- persönliche Daten, Bankverbindung, Dienstprofil, ...
- Gebührendaten

Funktion

Probleme

- Identitäten (IMSI/TMSI) werden ab und zu im Klartext übertragen
- Standard schreibt nur die Verschlüsselung der Funkstrecke vor
- Betreibernetz (BSS/VLR) authentisiert sich nicht
- Ende–zu–Ende Sprachverschlüsselung nicht vorgesehen
  (aber TopSec GSM)
- Ende–zu–Ende Authentikation nicht vorgesehen
- keine anonyme Netzbenutzung
- nur symmetrische Verschlüsselung
- Aufenthaltsorte werden mehrfach abgespeichert
- Algorithmen A3/A8 sind betreiberspezifisch und nicht öffentlich (gewesen)
  A5 ist standardisiert, aber gemein (gewesen)
- Verschlüsselung mit A5 ist abgeschwächt
  (10 Bit des Schlüssels werden auf 0 gesetzt)
- Abrechnung vollständig durch Betreiber
- Abrechnung erfolgt erst nach Ende der Verbindung

Bedrohungen

- falsche Rechnungen können nicht wirksam angefochten werden
- Insider können SIM-Karten fälschen
- Erstellung von Bewegungsprofilen
  (theoretisch bis auf wenige Meter genau)
- viele Abhörmöglichkeiten
- telefonieren auf fremde Rechnung

IMSI–Catcher [And01]

- „Man–in–the–middle–attack“
- kann Identitäten aller Mobilfunkteilnehmer einer Funkzelle ermitteln
- und Gespräche mithören
- angeblich bei Rohde & Schwarz als „GA 090“ erhältlich
- vom Bundestag legalisiert

SRES abfangen [And01]

- auf Kosten anderer telefonieren (ortsbegrenzt)

SIM Karte fälschen

- Schnittstelle der SIM-Karte ist standardisiert
- eine bekannte A3/A8 Implementierung *COMP128* ist schwach
- mehrere Angriffe dokumentiert:

narrow pipe (David Wagner)
mit etwa 150.000 Anfragen kann der Schlüssel Ki ermittelt werden
geschätzte Dauer: 8–12 Stunden

Energieaufnahme [RRTS02]
adaptiver Angriff mit 8 Anfragen

A5 brechen [BSW00]

- 2 Minuten mithören, 2 Sekunden rechnen *oder*
- zwei Sekunden mithören, mehrere Minuten rechnen (2000)

überlange Telefonkonferenzen [And01]

- Mobiltelefon stehlen
- (alternativ: Vorbezahlte SIM–Karte mit gestohlener Kreditkartennummer für „roaming“ freischalten)
- Telefonkonferenz über fremdes Netzwerk aufsetzen
- Gespräche über die Telefonkonferenz vermitteln,
  —Konferenz nicht beenden—
- Rechnung kommt *nie*

Sicherheit in GSM ist mit Festnetz vergleichbar

- keinerlei Schutz vor Insidern
- keine Vertraulichkeit gegenüber professionellen Angreifern
- keine Anonymität (aber vorausbezahlte SIM-Karten)
- keine Integrität, Zurechenbarkeit

ABER: Sicherheitskonzept insgesamt erfolgreich

Lehren

- Verletzung des Kerckhoff-Prinzips:

  Sicherheit soll auf geheimen Schlüssel beruhen,
  nicht auf geheimen Algorithmus.

- Angriffe aus Kryptokonferenzen sind nicht wirklich relevant
- relevant sind Probleme im Design des gesamten Systems

Mehr Sicherheit

- Signalspreizverfahren auf der Luftschnittstelle
- HLR authentisiert sich gegenüber der MS
- Nachrichtenintegrität durch Signaturen gesichert
- im Servicenetzwerk wird verschlüsselt
- bekannte, gut untersuchte Algorithmen
- Abhörschnittstellen für Polizei

[And01] R. J. Anderson. *Security Engineering — A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001.

[BSW00] A. Biryukov, A. Shamir, and D. Wagner. Real time cryptanalysis of A5/1 on a PC. In B. Schneier, editor, *Fast Software Encryption, 7th International Workshop*, volume 1978, pages 1–18, 2000.

[Fed99] H. Federrath. *Sicherheit mobiler Kommunikation*. DuD–Fachbeiträge. Vieweg, 1999.

[Pfi] A. Pfitzmann. Sicherheit in Rechnernetzen. Vorlesungsskript.

[Pfi01] A. Pfitzmann. Multilateral security: Enabling technologies and their evaluation. In R. Wilhelm, editor, *Informatics: 10 Years Back, 10 Years Ahead*, volume 2000 of *Lecture Notes in Computer Science*, pages 50–62. Springer–Verlag, 2001.

[PSM01] S. Pütz, R. Schmitz, and T. Martin. On the security of the UMTS system. In D. Fox, M. Köhntopp, and A. Pfitzmann, editors, *Verlässliche IT-Systeme 2001 - Sicherheit in komplexen IT-Infrastrukturen*, pages 87–106. Vieweg, 2001.

[RRTS02] J. R. Rao, P. R., S. Tinguely, and H. Scherzer. Partitioning attacks: Or how to rapidly clone some GSM cards. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 31–41, Oakland, CA, May 2002. IEEE Computer Society Press.

[Sch00] J. Schiller. *Mobilkommunikation: Techniken für das allgegenwärtige Internet*. Addison–Wesley, 2000.

[WP00] G. Wolf and A. Pfitzmann. Properties of protection goals and their integration into a user interface. *Computer Networks*, 32(6):685–699, May 2000.

Mobilfunk als Teilgebiet der Abkürzungswissenschaften

- LAI MS BSS BSC BST HLR VLR AuC GSM UMTS SIM IMSI PIN TMSI
- DBA's überwiegen

Sicherheit im Mobilfunk

- klassische Versuch–und–Irrtum Methode
- Systemgestaltung $\longleftrightarrow$ kryptographische Schwachpunkte
- komerziell $\longleftrightarrow$ universitär
  - Standards sind gigantisch
  - wiss. Artikel sind oft unklar, manchmal widersprüchlich
    Was kann das Protokol?
    Wer authentisiert?
    Wird verschlüsselt oder nicht?
  - Wissenschaft findet *langsam* ihren Weg