Netzsicherheit

Teil 2: Mobilfunk

Prof. Dr. Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Kurze Geschichte

- Erstes kommerzielles Mobilfunksystem: AT&T 1946 in St. Louis
- 1980er Jahre: Entwicklung mehrerer zueinander inkompatibler Mobilfunksysteme in Europa
- 1982: Gründung der „Groupe Spéciale Mobile“ (GSM) durch die CEPT (Conférance Européenne des Administrations des Postes et des Télécommunications)
- 1987: Unterzeichnung des MoU zum GSM-System
- 1988: GSM wird ETSI-Standard
- 1992: Offizielle Einführung von GSM-Systemen

Quelle: Einführung in GSM. Stefan Eglauf, Samuel Frempong, Hochschule Rapperswil

Kurze Geschichte

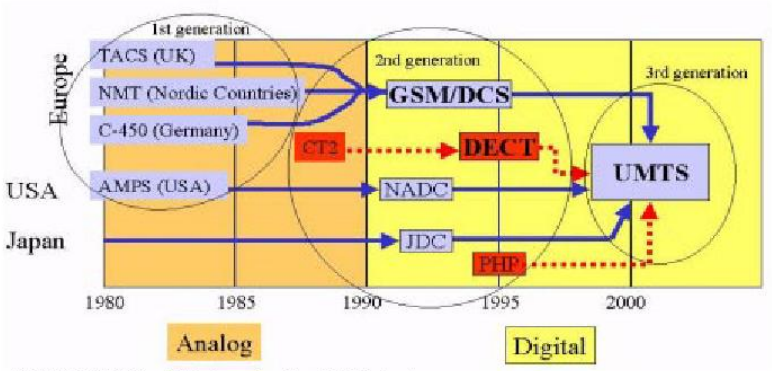


ABBILDUNG 3. Überblick der weltweiten Mobilfunknetze

Mobilfunk: Systemüberblick

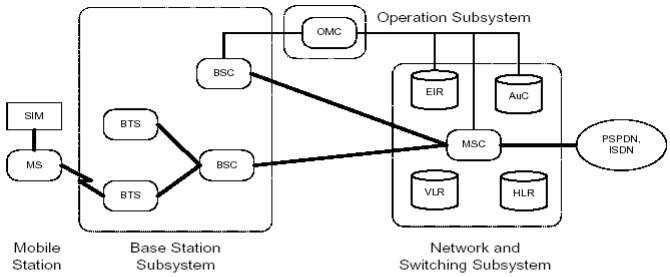


ABBILDUNG 1. GSM-Systemarchitektur

Das GSM-Netz lässt sich am besten als hierarchisch gegliedertes System verschiedener Netzelemente verstehen. Am unteren Ende steht die Mobile Station (MS), die über Funk mit der nächstgelegenen Base Tranceiver Station (BTS) kommuniziert. Zur Lenkung und Kontrolle der BTS werden sie gebietsweise von einem Base Station Controller (BSC) zusammengefasst. Das den BSC wiederum übergeordnete Netzelement, sind die Mobile Switching Centers (MSC), sie sind unter anderem für den Übergang in andere (in- oder ausländische) Telefonnetze verantwortlich.

Mobilfunk: Systemüberblick

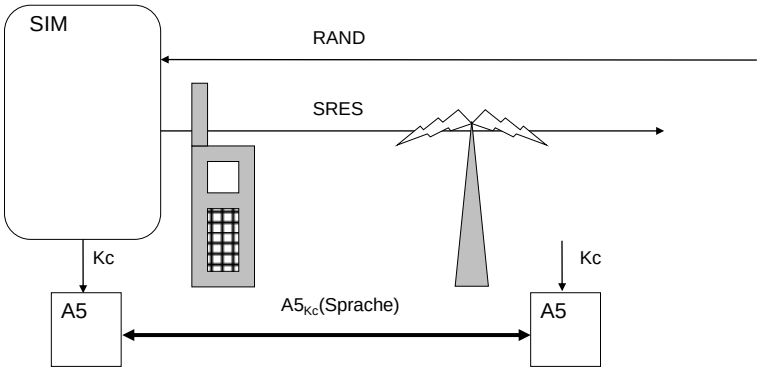
Um die anfallenden Vermittlungs- und Verwaltungsaufgaben bewältigen zu können, wird eine Reihe von Datenbanken benötigt. Diese sind meist auf der MSC-Ebene angesiedelt. Dies sind:

- Home Location Register (HLR): Hier werden die persönlichen Informationen des Benutzers wie Telefonnummer, freigeschaltete Dienste und so weiter gespeichert. Pro GSM-Netz gibt es nur ein HLR.
- Visitor Location Register (VLR). Das VLR enthält die dynamischen Teilnehmerdaten. Es handelt sich um lokale, einem Gebiet zugeordnete Datenbanken, welche Kopien der HLR-Datenbestände für die Benutzer führen, die sich momentan in ihrem Zuständigkeitsbereich befinden.
- Authentication Center (AuC). Das AuC enthält die Zugangsdaten der einzelnen Benutzer, insbesondere der persönlichen, geheimen SIM-Karten-Schlüssel, die zum Zugang ins Mobilfunknetz und anschliessend für die codierte Übertragung der Gesprächsdaten über das Netz notwendig sind.
- Equipment Identity Register (EIR). Im EIR werden die MS spezifischen Daten, insbesondere eine Liste der IMEI-Nummern, geführt.

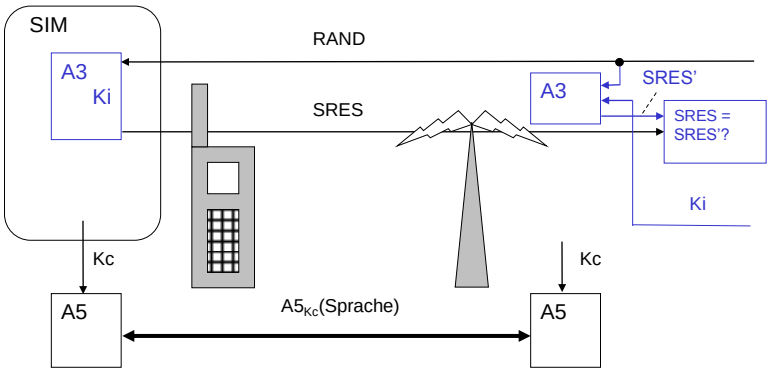
Mobilfunk: Systemüberblick

- Subscriber Identification Module (SIM, Chipkarte):
  - IMSI (International Mobile Subscriber Identity)
  - Authentifizierungsalgorithmus A3
  - Schlüsselerzeugungsalgorithmus A8
  - Schlüssel Ki
  - PIN, PUK
- Mobile Station (Handy):
  - IMEI (International Mobile Equipment Identity)
  - Verschlüsselungsalgorithmus A5 (standardisiert)
    - Stromchiffre, Initialisierung mit Kc und FN (TDMA Frame Number)

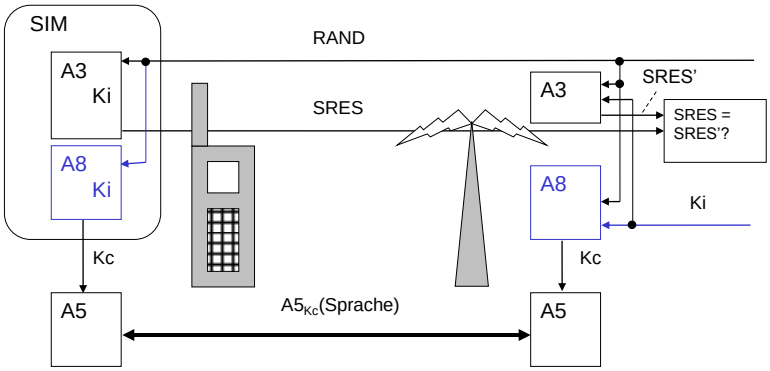
Mobilfunk: GSM-Sicherheit



Mobilfunk: GSM-Sicherheit



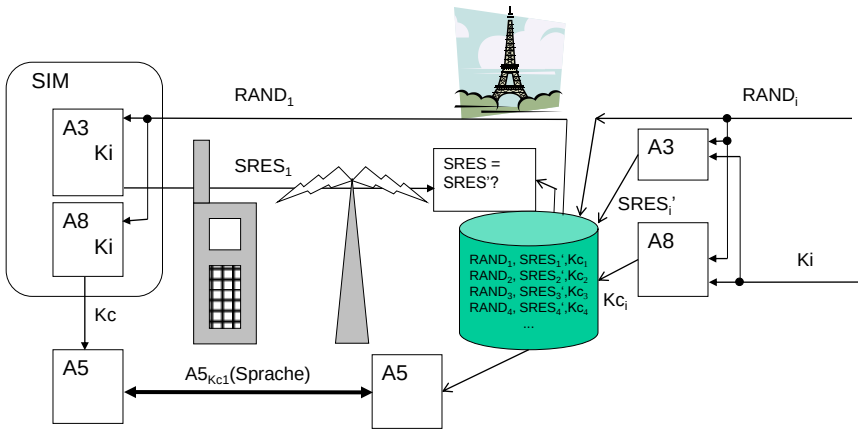
Mobilfunk: GSM-Sicherheit



Mobilfunk: Weitere Sicherheitsmechanismen

- Schutz der Teilnehmeridentität
  - IMEI soll nicht im Klartext übertragen werden
  - VLR weist der MS eine TMSI (Temporary Mobile Subscriber Identity) zu, und teilt die Zuordnung dem HLR mit
- Roaming
  - Authentifizierung im fremden Netz durch vorproduzierte Triplets (RAND, Kc, SRES)

Mobilfunk: Roaming



Mobilfunk: Sicherheitsprobleme

- IMSI-Catcher
- Zugriffsmöglichkeit auf gespeicherte Bewegungsdaten
- Schlechte Varianten von A3/A8
- A5 musste 1991 exportierbar sein!
- Bedarfsträger dürfen abhören

Mobilfunk: UMTS-Sicherheit

Die bewährten Sicherheitsfeatures von GSM sollen beibehalten werden, und die Rückwärtskompatibilität so groß wie möglich sein. Beibehalten werden also:

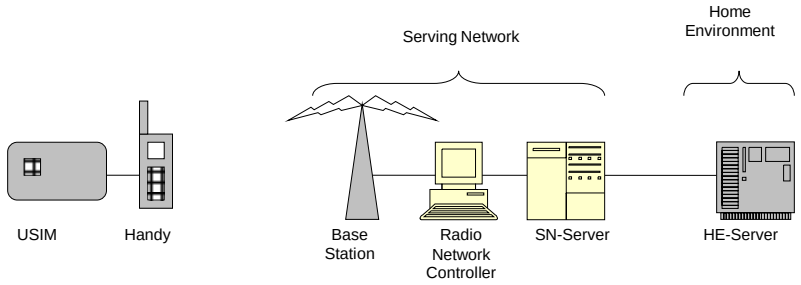
- Vertraulichkeit der Identität eines Teilnehmers (keine Erstellung von Bewegungsprofilen).
- Authentisierung des Kunden gegenüber dem Netzwerk.
- Verschlüsselung der Luftschnittstelle.
- Verwendung einer SIM als vom Handy unabhängiges Sicherheitsmodul (jetzt USIM genannt).
- Authentisierungsmöglichkeit eines Kunden gegenüber der SIM (Eingabe eines Passwortes als Schutz gegen Diebstahl).
- Für den Kunden transparente Sicherheitsmechanismen (außer der PIN-Eingabe).
- Eine Authentikation auch in fremden Netzwerken („Serving Network“ im Gegensatz zum „Home Environment“).
- Die Möglichkeit, dass jeder UMTS-Betreiber eigene Authentisierungs-verfahren einsetzt.

Mobilfunk: UMTS-Sicherheit

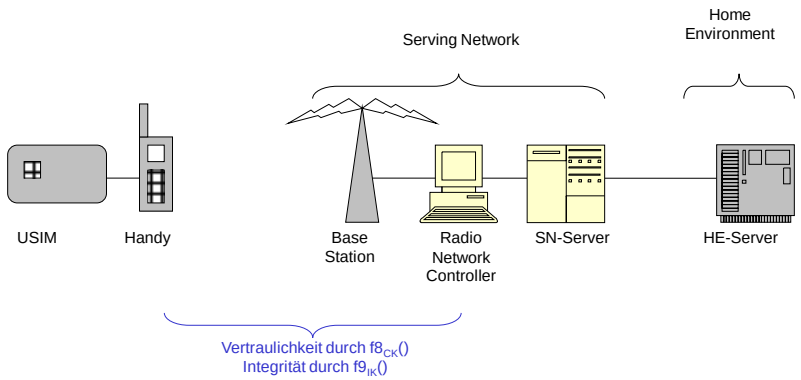
Die Sicherheitsarchitektur soll neue Gegebenheiten berücksichtigen, und die daraus resultierenden bekannten Schwächen von GSM beheben, aber auch neue Sicherheitsfeatures anbieten. Das sind:

- Authentisierung des Home Environment (HE) gegenüber der USIM.
- Ein Sequenznummermanagement, um die Wiederverwendung von alten Authentisierungsdaten zu beschränken.
- Übertragung eines „Authenticated Management Field“ (AMF), damit der Betreiber die USIM über einen sicheren Kanal steuern kann.
- Einführung eines Integritätsschlüssels, um Steuerbefehle authentisieren zu können.
- Einführung von Sicherheitsfunktionalitäten für den Signalisierungsverkehr im Festnetz (so genannte Core Network Signalling Security), so dass z.B. die besonders sensitiven Authentisierungsdaten der Teilnehmer verschlüsselt zwischen den Netzbetreibern ausgetauscht werden; dieses Feature ist jedoch z. Zt. nur optional

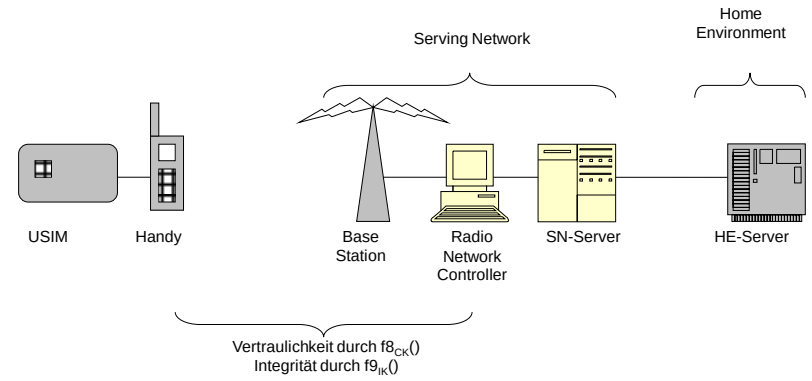
Mobilfunk: UMTS-Sicherheit



Mobilfunk: UMTS-Sicherheit



Mobilfunk: UMTS-Sicherheit

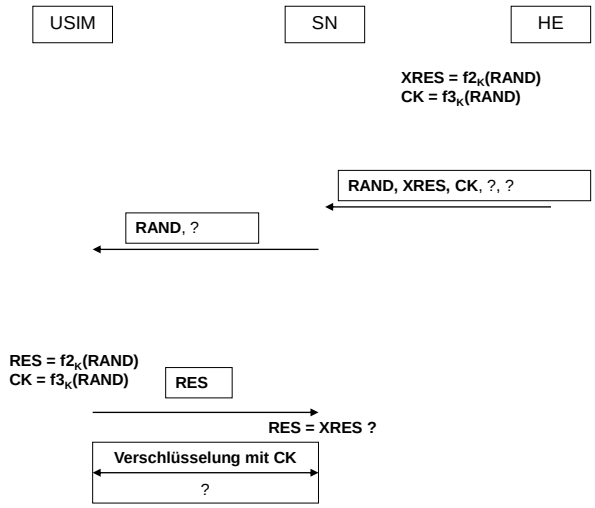


Mobilfunk: UMTS-Sicherheit

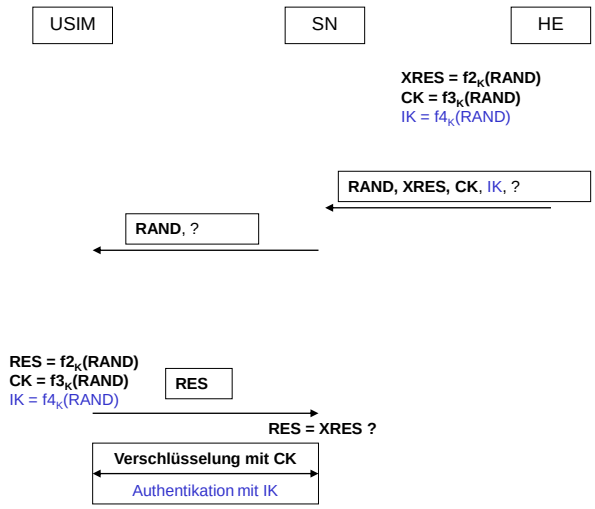
Die Sicherheitsarchitektur von 3GPP erweitert das Challenge-and-Response-Protokoll von GSM um

- einen MAC, mit dem sich das Home Environment gegenüber der USIM authentisiert,
- eine Sequenznummer SQN, die die „Frische“ der Protokolldaten garantiert,
- das USIM-Steuerfeld AMF und
- einen Integritätsschlüssel IK.

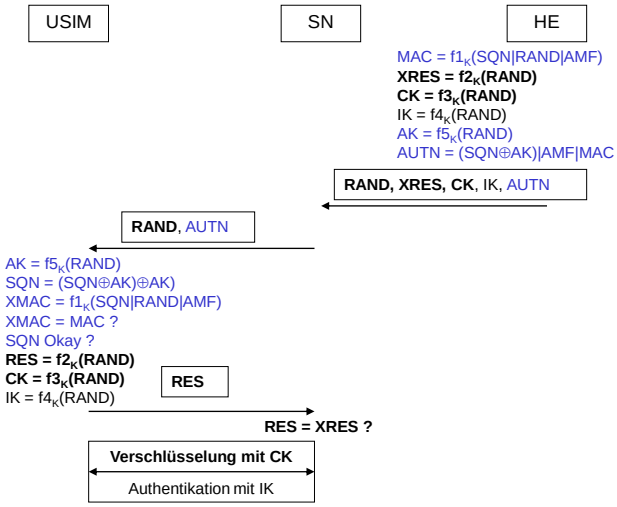
Mobilfunk: UMTS-Sicherheit



Mobilfunk: UMTS-Sicherheit



Mobilfunk: UMTS-Sicherheit



Mobilfunk: UMTS-Sicherheit

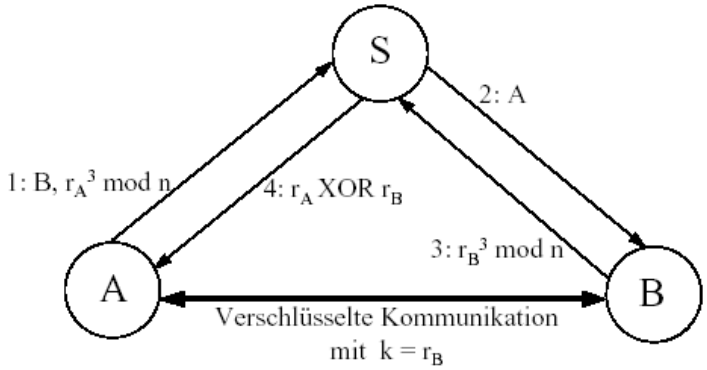


Bild 7.7: Das TMN-Protokoll

Mobilfunk: UMTS-Sicherheit

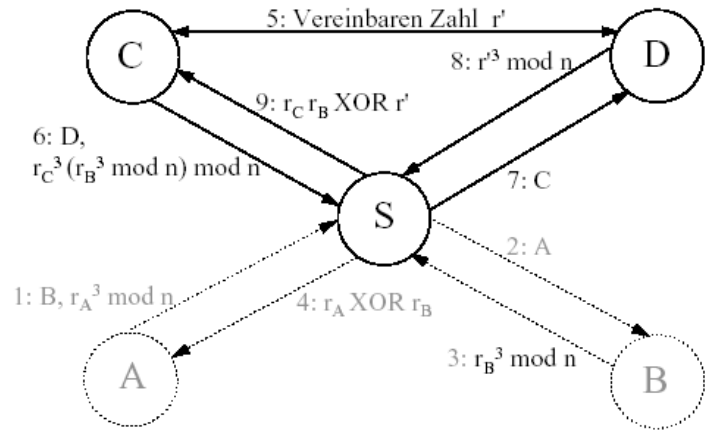


Bild 7.8: Simmons' Attacke auf das TMN-Protokoll

Mobilfunk: UMTS-Sicherheit

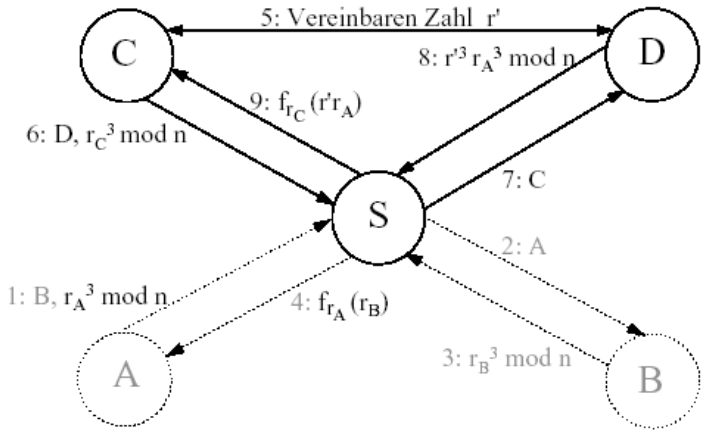


Bild 7.9: Eine Attacke auf das modifizierte TMN-Protokoll

Dolev-Yao-Modelle

Dolev, D. & Yao, A. C.-C.
On the security of public key protocols
IEEE Transactions on Information Theory, **1983***, 29*, 198-207

- Kryptographische Bausteine (Verschlüsselung, digitale Signatur, ...) werden als „Black Box“ mit idealen Sicherheitseigenschaften aufgefasst
- Angreifer darf alle Nachrichten im Netzwerk
  - lesen, löschen, umordnen, in ihre Bestandteile zerlegen,
  - selbst Nachrichten senden,
  - an andere als die intendierten Teilnehmer weiterleiten,
  - mehrere Instanzen eines Protokolls mischen, ...
- Computer-unterstützte Verifikation möglich
  - ... daher große Forschungscommunity
- Am HGI nicht vertreten
  - ... wir schauen tiefer in die „Black Box“ hinein

BAN-Logik

M. Burrows, M. Abadi, and R. M. Needham, *Authentication: A Practical Study in Belief and Action.* Proc. 2nd Conf. on Theoretical Aspects of Reasoning about Knowledge, M. Vardi (Ed.), 1987, pp 325-342.

- Erster Ansatz zur halbautomatischen (computerunterstützten) Verifikation der Korrektheit von Protokollen
- Aufdeckung von Protokolllücken in den 1990ern
- Ziele:
  - Vollautomatische Untersuchung von Protokollen, ähnlich den statistischen Analysen von Verschlüsselungsalgorithmen
  - Beweis der Sicherheit eines Protokolls
- Ziele wurden (bisher) nicht erreicht: Suchbaum ist zu groß!
- Die zur Standardisierung vorgeschlagenen UMTS-Protokolle wurden mittels BAN-Logik (manuell!) verifiziert!