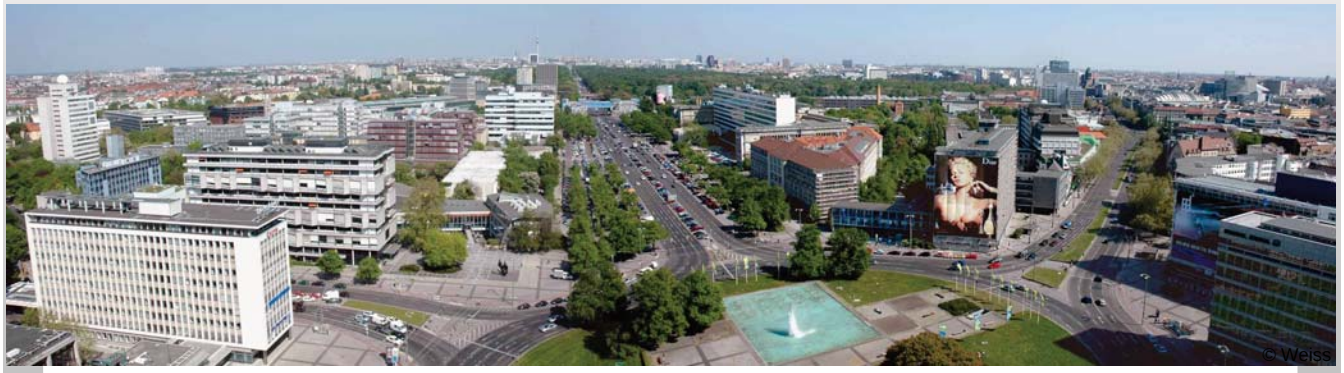


“Nach Hause telefonieren”
Wie funktioniert eigentlich Mobilfunk?

Technisches Seminar DESY, Zeuthen

Matthias Lange, 03.05.2011
mlange@sec.t-labs.tu-berlin.de

Agenda

- Geschichte des Mobilfunks
- Aufbau eines Handys
- Aufbau des Mobilfunknetzes
- Sicherheitsproblematiken

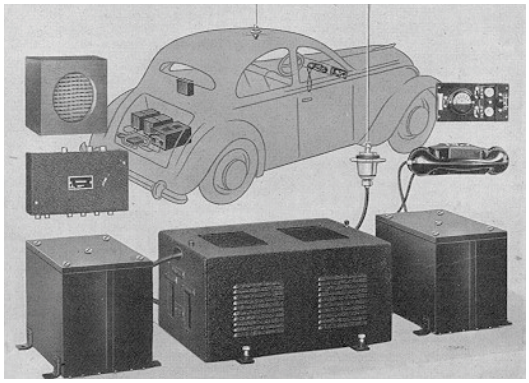
Geschichte des Mobilfunks

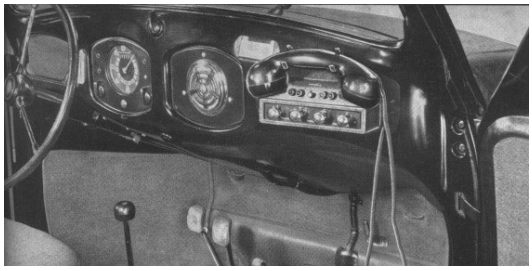
„Ein Herr, der vor ihnen auf dem Trottoir langfuhr, trat plötzlich aufs Pflaster, zog einen Telefonhörer aus der Manteltasche, sprach eine Nummer hinein und rief: ‚Gertrud, hör mal, ich komme heute eine Stunde später zum Mittagessen. Ich will vorher noch ins Laboratorium. Wiedersehen, Schatz!‘ Dann steckte er sein Taschentelefon wieder weg, trat aufs laufende Band, las in einem Buch und fuhr seiner Wege.“

– Erich Kästner (1932, Der 35. Mai)

A- und B-Netz

- A-Netz ab 1958
  - Analog
  - Handvermittelt
  - 150 MHz Band
  - 1977 eingestellt
- B-Netz
  - Analog
  - 1972 – 1994 in Betrieb
  - Selbstwählverkehr
  - Region-Vorwahl nötig
  - 150 MHz Band





C-Netz

- C-Netz
  - Ab 1985
  - Zellulares Netz
    - Weniger Sendeleistung
  - Daten- (DATEX) und Faxverbindungen möglich
  - 450 MHz Band
  - Ende 2000 eingestellt

GSM-Netze

- 1982 Gründung der Group Spéciale Mobile (GSM)
  - Digitales Netz
  - 900 MHz Band
  - Funkverfahren TDMA
- 1991 in Genf GSM-Pilotnetz
- Weltweiter Standard für mobile Telefonie
- Offizielle Einführung ab 1992 mit dem D-Netz
  - D1 (Telekom) und D2 (Mannesmann)
- Ab 1994 E-Netz im 1800 MHz Band
  - E-Plus
  - Viag Interkom (ab 1998)

UMTS & LTE

- UMTS - Universal Mobile Telecommunication System
  - Neue Funkzugriffstechnik (WCDMA)
  - Erhöhung der Datenübertragungsrate
  - Sicherheit
  - Ausbaustufen HSDPA (14,4Mbit/s) und HSUPA (5,8Mbit/s)
- LTE – Long Term Evolution
  - Für schnelle Datendienste (bis 300Mbit/s)
  - IP basiert
  - 800 MHz Band (digitale Dividende)

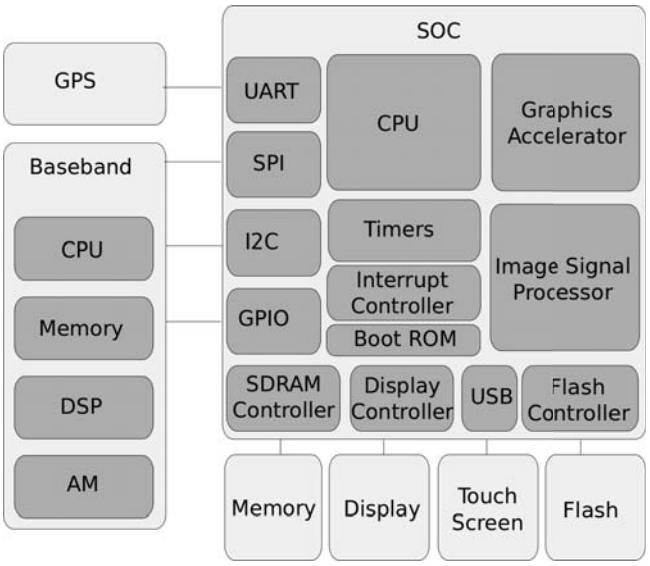
Aufbau eines Handys

Außen

- Display
- Lautsprecher
- Mikrofon
- Kamera
- Tastatur
- Antenne

Innen

- Zwei Prozessoren
  - Anwendungsprozessor
  - Basebandprozessor
- Sensoren
  - GPS
  - Beschleunigung
  - Gyroskop
- Bluetooth
- WLAN
- Flash-Speicher



Anwendungsprozessor

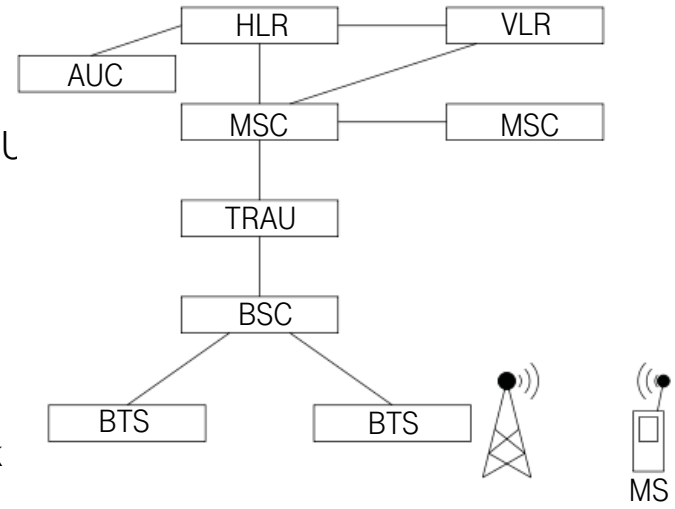
- System on a chip mit ARM-Kern
  - Inzwischen auch Mehrkernsysteme
  - Leistungsfähiger Graphikprozessor
- Plattform für das Telefonbetriebssystem
  - iOS, Android, Symbian
  - Herstellerspezifische Betriebssysteme

Baseband

- Schnittstelle zum Mobilfunknetzwerk
- ARM-Prozessor
  - Eigenes Echtzeit-Betriebssystem
- DSP
  - Sprachkodierung
  - Steuerung der Funkschnittstelle
- Häufig eigenes Mikrofon
- Nur wenige Hersteller
  - Zertifizierung von Hard- und Software zwingend
- Per serieller Schnittstelle am Anwendungsprozessor angeschlossen
  - Hayes-Kommandosatz (AT)

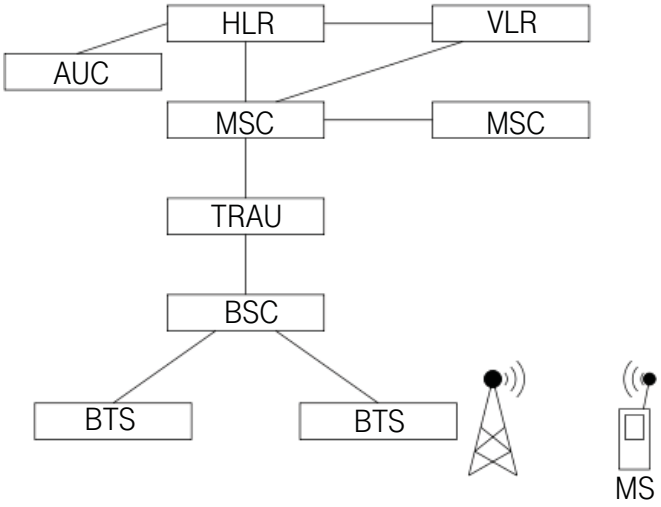
Aufbau des Mobilfunknetzes

- MS: Mobile Station
- BTS: Base Transceiver Station
  - Basisstation
- BSC: Base Station Controller
- TRAU: Transcoder Rate Adaption U
- MSC: Mobile Switching Center
  - Vermittlungsstelle
- VLR: Visitor Location Register
  - Wer ist wo?
- HLR: Home Location Register
  - Zentrale Nutzerdatenbank
- AUC: Authentication Center
  - Nutzerauthentifizierung

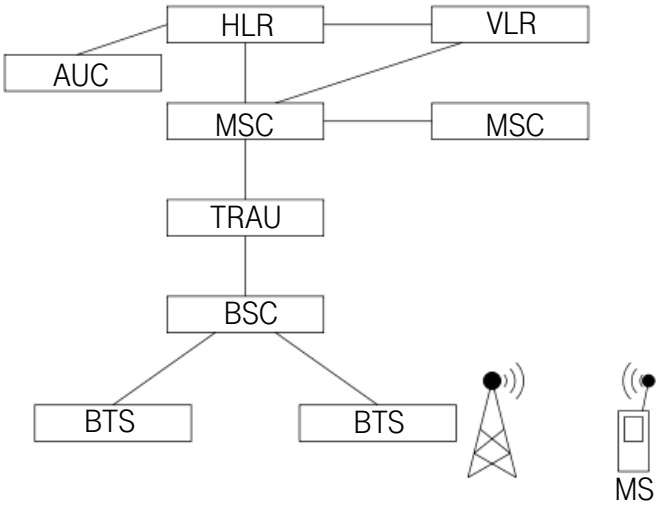


Wie wird also telefoniert?

- Handy verbindet sich mit Basisstation
  - Austausch eines Sitzungsschlüssels
  - Aufenthaltsort wird im VLR gespeichert
- Wählen der Telefonnummer
  - Wird von der Telefonanwendung eingelesen
  - “ATD 0160123456789” zum Baseband
  - Antwort “CONNECT”
  - Mikrofon wird eingeschaltet
- Baseband schickt die Anfrage an das Mobilfunknetzwerk



- MSC fragt beim HLR nach, ob der Angerufene existiert
- MSC fragt beim VLR nach der Zelle des Angerufenen
  - Verbindungsaufbau
- Angerufene bekommt Anruf signalisiert
  - Telefonanwendung schickt an das Baseband “ATA”
  - Antwort “CONNECT”
  - Mikrofon wird eingeschaltet
- “Gertrud, hör mal, ich komme heute eine Stunde später zum Mittagessen.”



Sicherheitsproblematiken

Sicherheitsuntersuchungen

- GSM Spezifikationen nicht öffentlich zugänglich
  - "Security by obscurity"
  - Durch Patente geschützt
- Bislang teure Spezialhardware für Untersuchungen nötig
- Patente laufen aus
- Open-Source-Projekte machen Untersuchungen möglich
  - OpenBTS
  - OpenBSC
  - OsmocomBB

SMS of Death

- Billige sog. “Feature Phones”
  - Proprietäre Betriebssysteme
  - Selten oder keine Aktualisierungen
- “Abschießen” des Telefons mit einer speziell aufbereiteten SMS
  - Unterschiedlich starke Effekte
  - Alle Hersteller betroffen
- Auch Smartphones betroffen
  - iPhone SMS Bug 2009
- Schutz nur durch Updates der Software möglich
  - Netzbetreiber könnte SMS-Nachrichten automatisch filtern

Abhören von Gesprächen

- Mit teurer Spezialausrüstung wohl schon lange möglich
- Verschlüsselung zwischen Handy und Basisstation
  - A5/0 – keine Verschlüsselung
  - A5/1 – geknackt, Dekodierung in Echtzeit mit Hilfe sog. “Rainbow Tables”
  - A5/2 – schwächere A5/1 Variante für Export, geknackt, seit 2007 “verboten”
  - A5/3 – nicht geknackt, aber zahlreiche Schwachpunkte bekannt

“Man in the middle”-Angriff

- Basisstation authentifiziert sich nicht gegenüber dem Handy
- “böse” Basisstation fängt den Verbindungsaufbau ab und stiehlt den Sitzungsschlüssel
- Angreifer hat alle Möglichkeiten die das Opfer hat
  - Mitlauschen ein- und ausgehender Anrufe
  - Anrufe auf Kosten des Opfers
  - Transparente Modifikation von z.B. SMS
  - Empfang von SMS (mTAN)

Fragen?

Danke!