IMSI Catcher

Daehyun Strobel

daehyun.strobel@rub.de

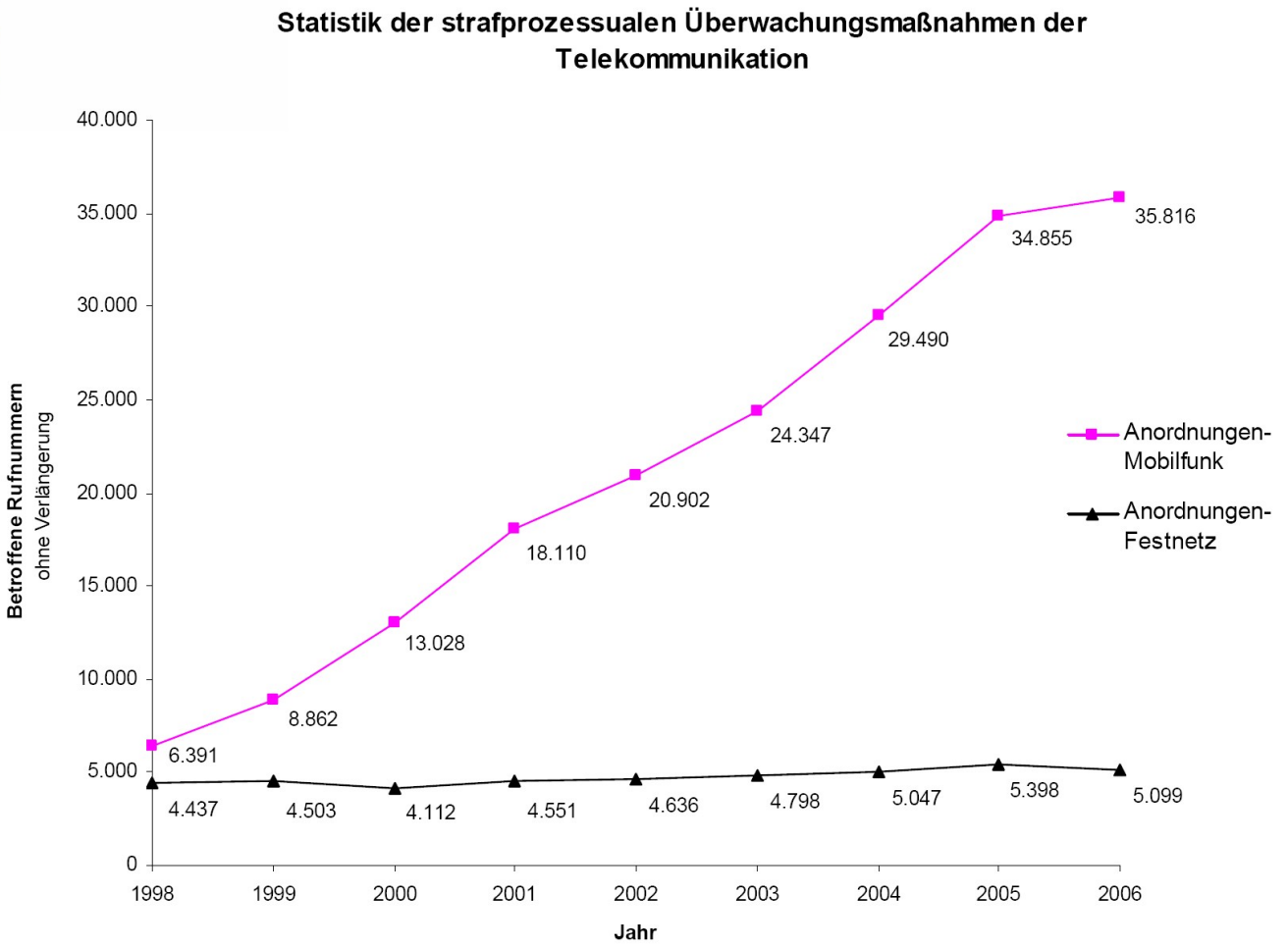
24.Juli 2007

Gliederung

- Einleitung
- Global System for Mobile Communications (GSM)
- Universal Mobile Telecommunications System (UMTS)
- Nachteile
- Fazit

Einleitung

Bundesnetzagentur



Einleitung

Abhörmöglichkeiten im Mobilfunk:

- Netzbetreiber
- IMSI Catcher

Einleitung

- Was ist eine IMSI?
  - International Mobile Subscriber Identity
  - 15-stellige eindeutige Teilnehmernummer, bestehend aus:
    - Mobile Country Code: 3 Zeichen, z.B. 262 für DE
    - Mobile Network Code: 2-3 Zeichen, z.B. 01 für T-Mobile
    - Mobile Subscriber Identification Number: max. 10 Zeichen
  - gespeichert auf der SIM

Einleitung

IMSI Catcher

- Entwickelt von Rohde & Schwarz
- 1.Präsentation im Dezember 1996
- 2 Versionen:
    - GA 090: Ermittlung der Identität eines Netzteilnehmers
    - GA 900: zusätzliche Überwachung ausgehender Gespräche

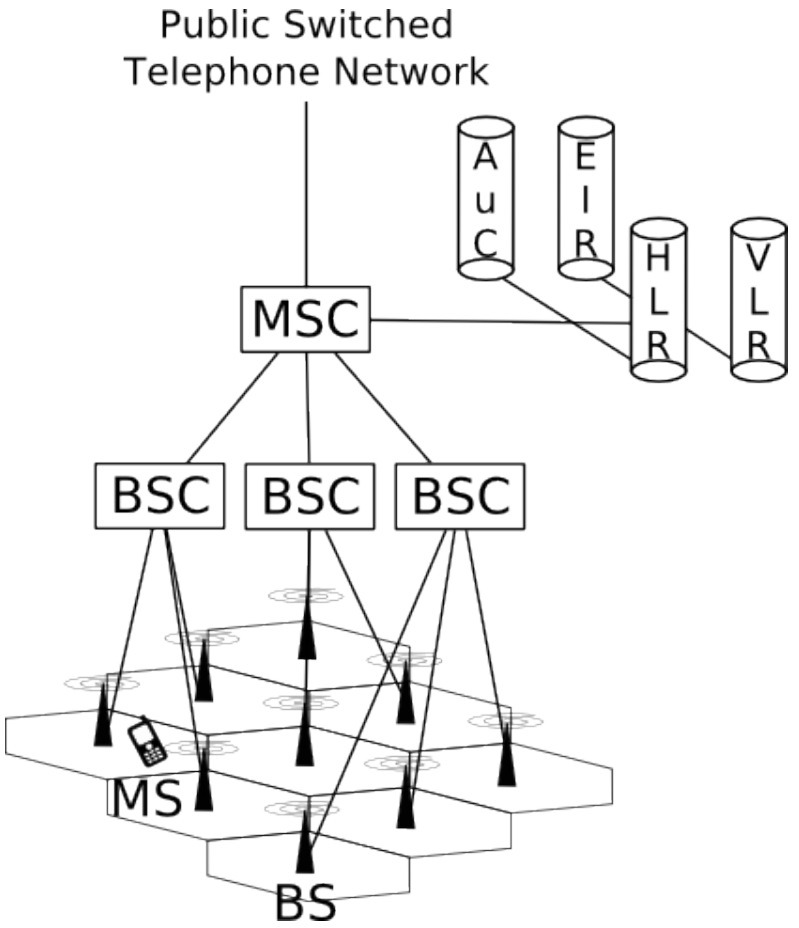
Global System for Mobile Communications

(**GSM**)

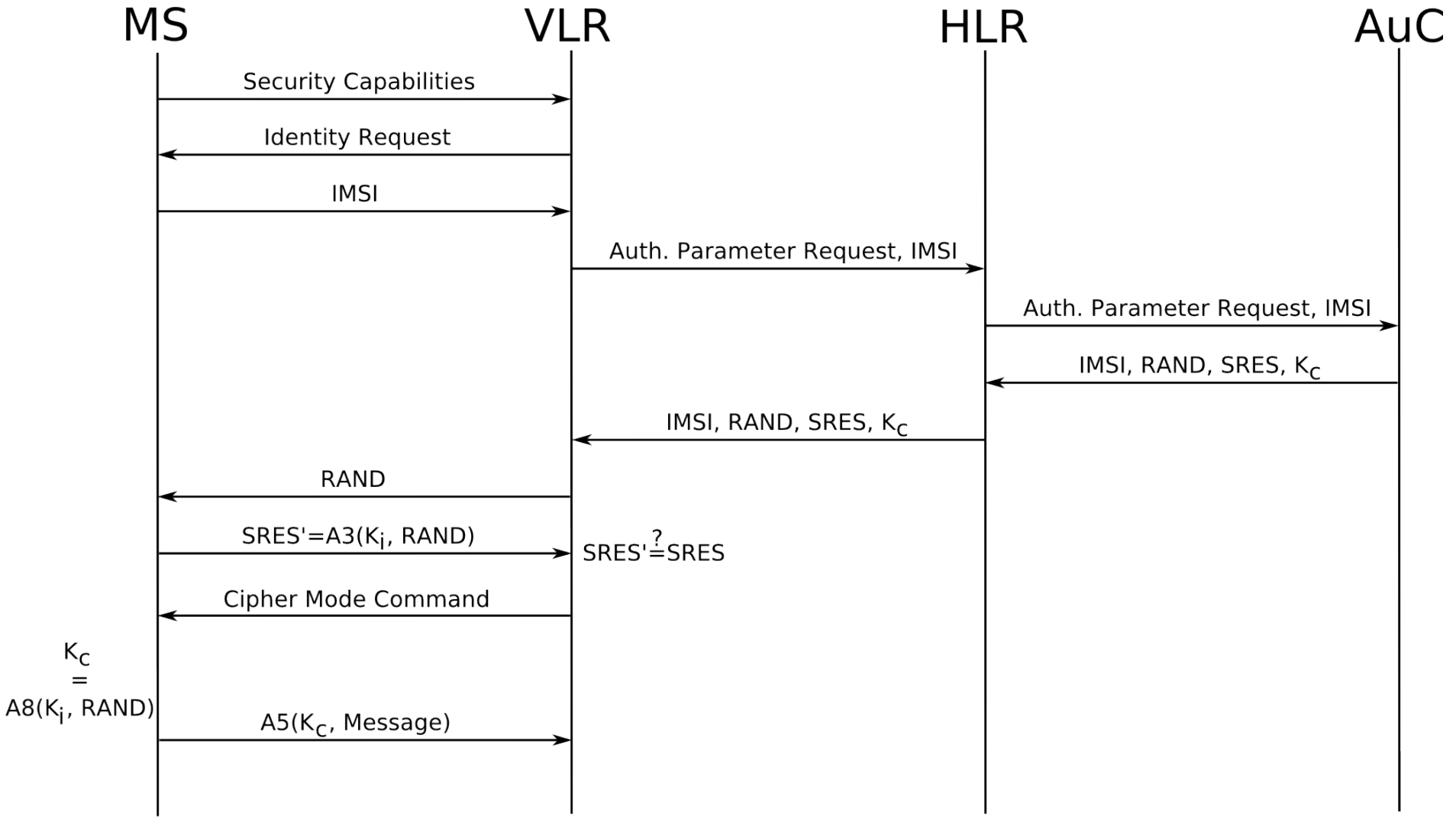
GSM

Aufteilung in 4 Ebenen:

- Mobile Station: Handy + SIM
- Base Station: Mobilfunksender
- Base Station Controller: Steuereinrichtung für mehrere Base Stations
- Mobile Switching Center: Vermittlungsstelle mit Zugang zu Datenbanken



GSM - Authentifikation



GSM - Authentifikation

Schwachpunkt:

Einseitige Authentifikation – MS authentifiziert sich gegenüber dem Netz, aber nicht umgekehrt!

=> IMSI Catcher

Einsatz des IMSI Catchers

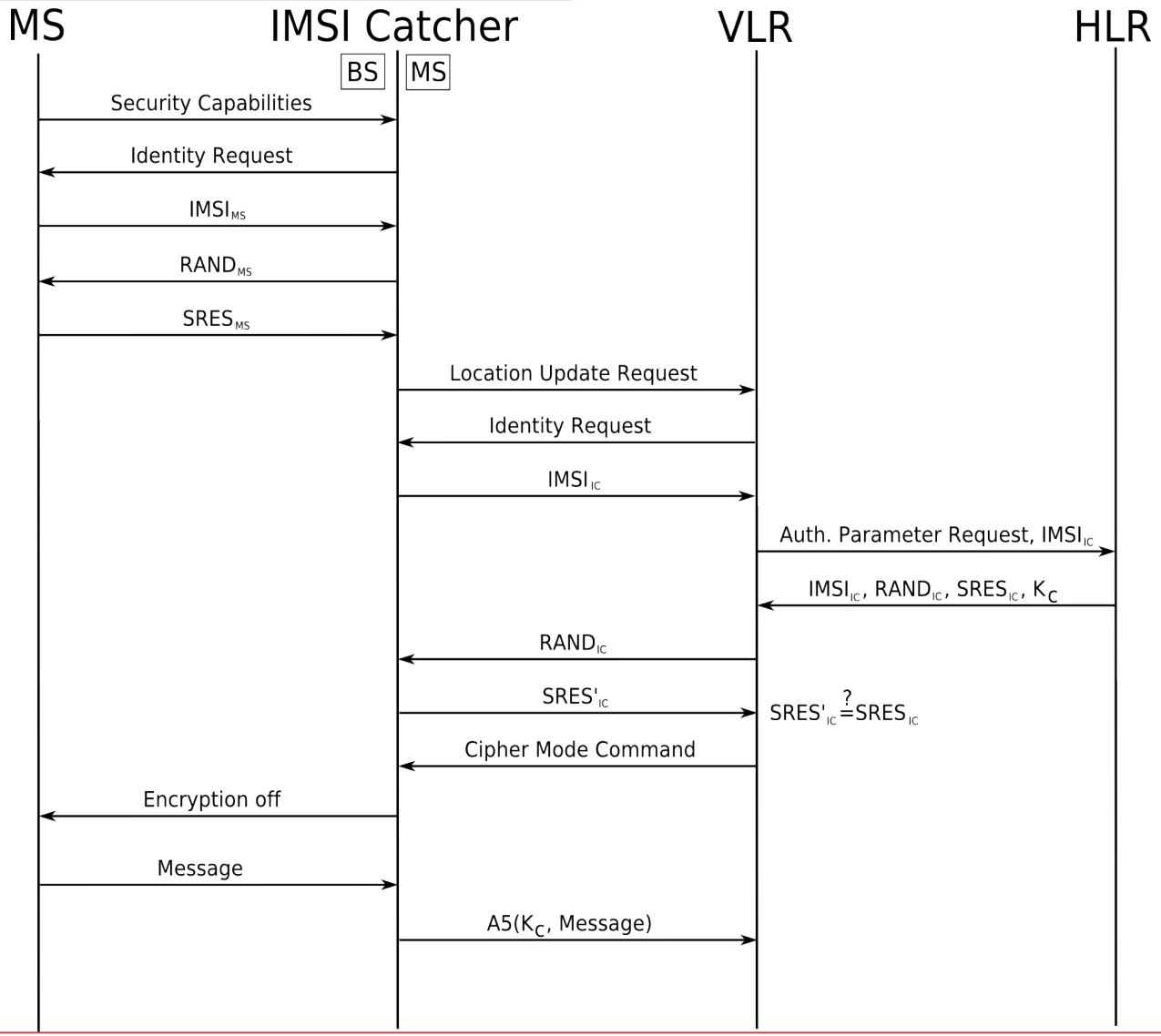
Masquerade attack (GA 090):

- IMSI Catcher gibt sich gegenüber der MS als BS aus

Man-in-the-middle-attack (GA 900):

- IMSI Catcher besitzt eigene SIM
- gibt sich gegenüber der MS als BS aus und gegenüber der BS als MS

Einsatz des IMSI Catchers (Man-in-the-middle Attack)



Universal Mobile Telecommunications System

(UMTS)

UMTS

Bewährte Sicherheitsmerkmale von GSM wurden übernommen und durch zusätzliche Eigenschaften erweitert, u.a.

Mutual entity authentication:

Beide Seiten müssen sich authentifizieren

UMTS

Bewährte Sicherheitsmerkmale von GSM wurden übernommen und durch zusätzliche Eigenschaften erweitert, u.a.

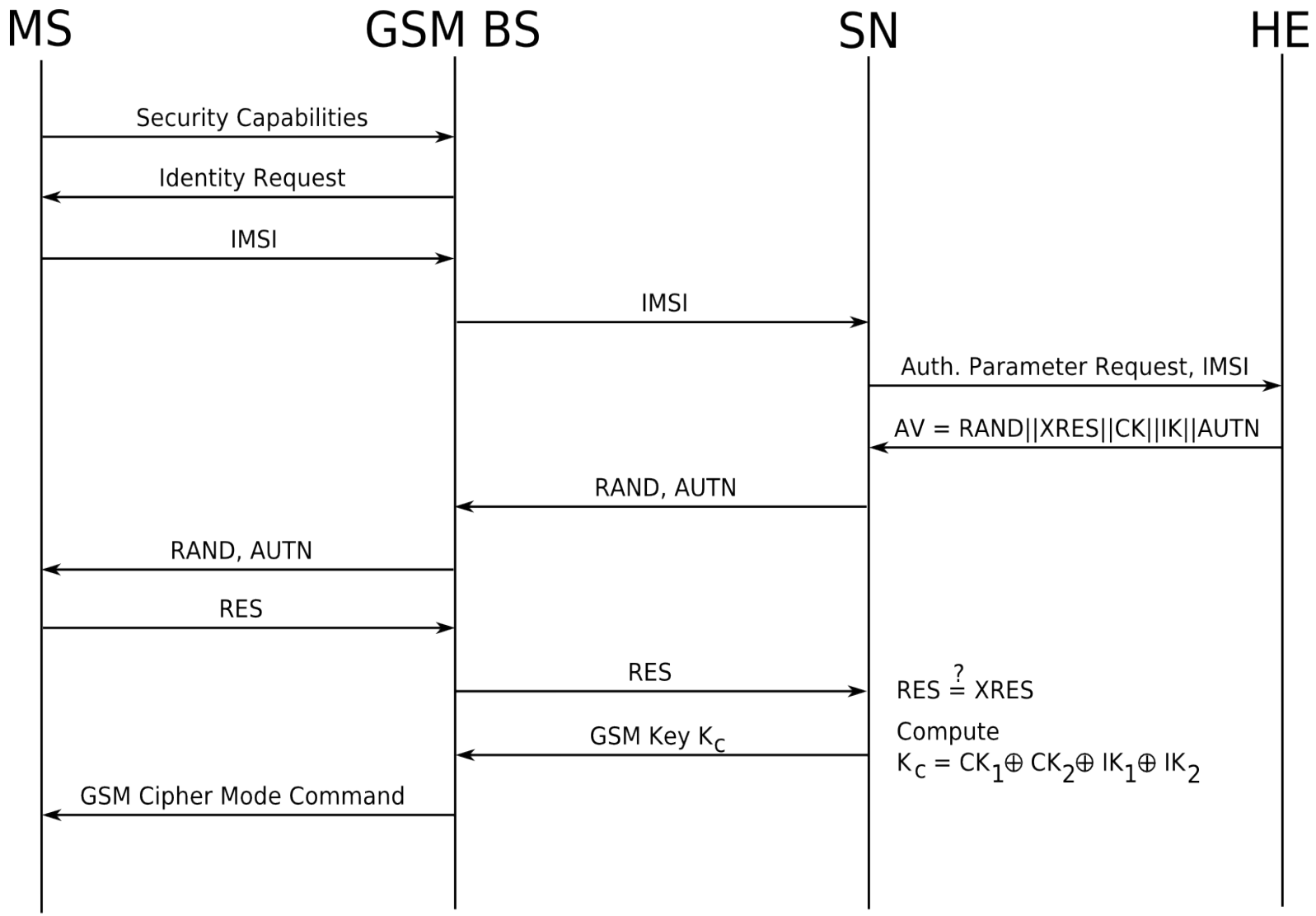
Mutual entity authentication:

Beide Seiten müssen sich authentifizieren

Aber:

Interoperabilität mit GSM um größtmögliche Netzabdeckung zu gewährleisten

UMTS (Authentifikation über GSM-Base Station)



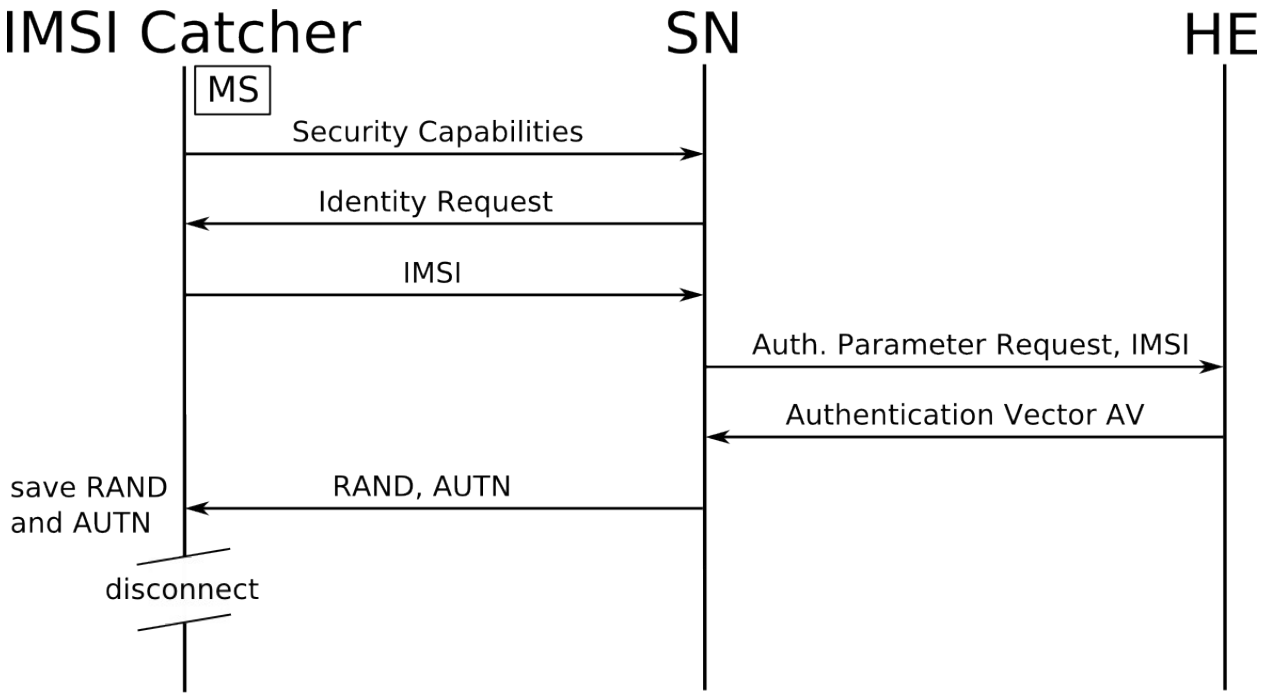
Einsatz des IMSI Catchers (Man-in-the-middle Attack)

1.Phase: IMSI des Teilnehmers anfordern

Einsatz des IMSI Catchers (Man-in-the-middle Attack)

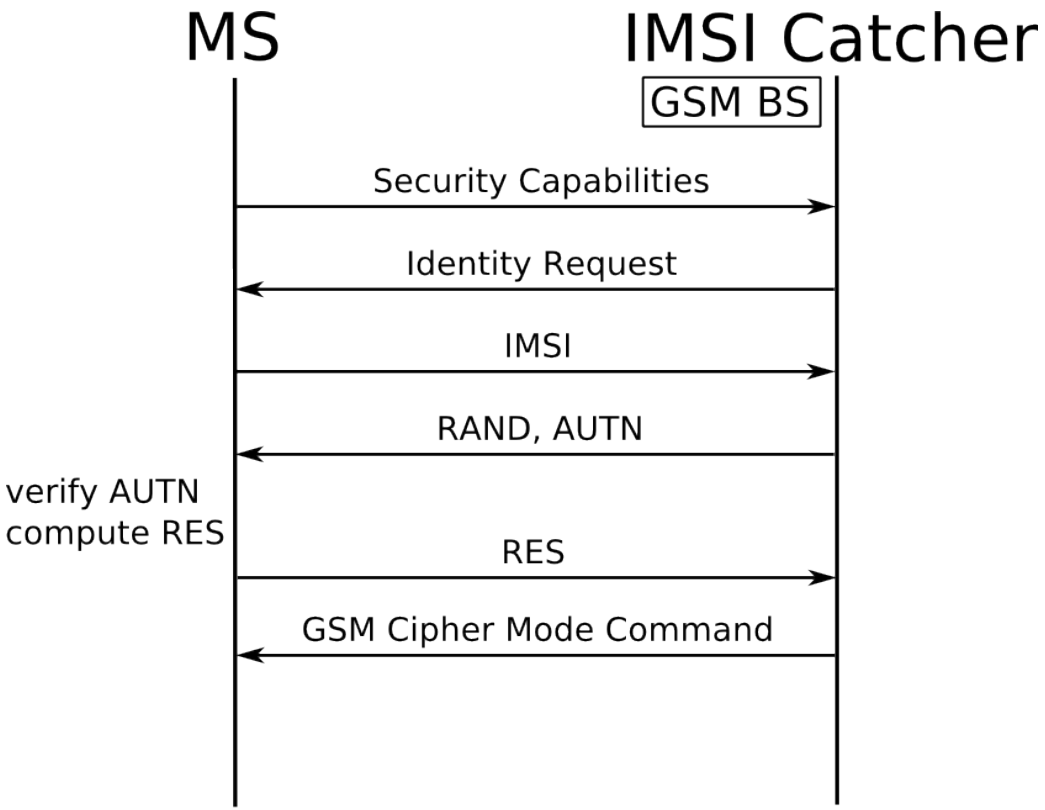
1.Phase: IMSI des Teilnehmers anfordern

2.Phase: Gültiges AUTN erlangen



Einsatz des IMSI Catchers (Man-in-the-middle Attack)

3.Phase: GSM-Base Station vortäuschen



Nachteile

- Netzanbieter muss im Vorfeld ermittelt werden
- Je nach Signalstärke befinden sich mehrere MS im Einzugsgebiet
- Nur ausgehende Anrufe können mitgehört werden
- Die MS im Einzugsgebiet können nicht auf das Netz zugreifen
- Einsatz kann evtl. bemerkt werden

Fazit

Einsatz des IMSI Catchers möglich, da

- GSM sehr weit verbreitet
- viele Handys kein UMTS unterstützen
- UMTS-Netz nicht bundesweit verfügbar
- Fallback auf GSM möglich

ENDE