Graduate seminar in cryptography

19.04.2006

3G security.

Ksenia Orman

Introduction to GSM

- GSM – Global System for Mobile Communications
- 1.7 billion subscribers

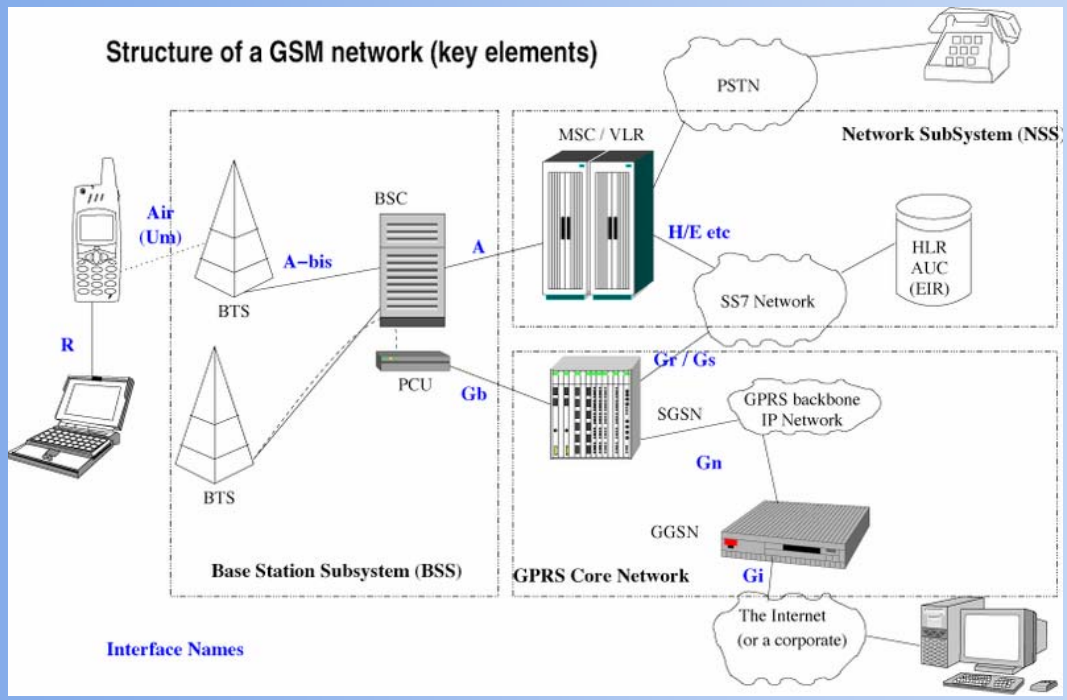
The billionth GSM user was connected in the first quarter of 2004. More than a quarter of a billion GSM users were connected during 2004.

	2002				2003				2004				2005			
Millions	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
World	980.5	1,027.0	1,078.2	1,137.8	1,187.9	1,239.4	1,302.2	1,382.9	1,453.8	1,525.4	1,612.3	1,714.1	1,820.6	1,920.6	2,027.2	-
GSM	676.1	714.6	758.0	809.3	851.5	894.7	945.4	1,012.0	1,070.9	1,131.6	1,207.2	1,296.0	1,378.5	1,467.6	1,561.7	-
3GSM	0.1	0.1	0.1	0.2	0.4	1.0	1.6	2.8	4.4	7.5	11.4	16.3	24.0	29.9	37.9	-
CDMA	108.4	107.6	106.1	104.2	102.3	99.8	99.3	98.9	96.6	93.6	90.6	87.4	72.5	68.5	63.8	-
CDMA 1X	9.4	16.0	25.9	36.1	45.7	56.5	67.5	80.1	93.5	106.6	118.9	131.9	167.6	182.9	197.2	-
CDMA 1X EV-DO	0.0	0.0	0.0	0.2	0.7	1.7	3.0	4.6	7.1	8.7	10.5	12.3	14.7	17.1	19.7	-
TDMA	93.9	97.7	99.2	101.1	100.7	99.8	99.8	100.1	98.1	95.6	92.8	90.0	82.8	79.0	71.9	-
PDC	54.3	54.9	55.4	56.1	57.5	58.2	58.5	58.1	57.7	56.7	55.7	54.2	51.6	49.5	46.5	-
iDEN	9.5	10.0	10.5	11.0	11.5	12.1	12.8	13.4	13.8	14.4	15.0	16.8	19.5	18.8	19.8	-
Analog	28.8	26.0	22.9	19.7	17.6	15.7	14.3	12.9	11.9	10.7	10.2	9.2	8.3	7.6	6.8	-

Source: Wireless Intelligence

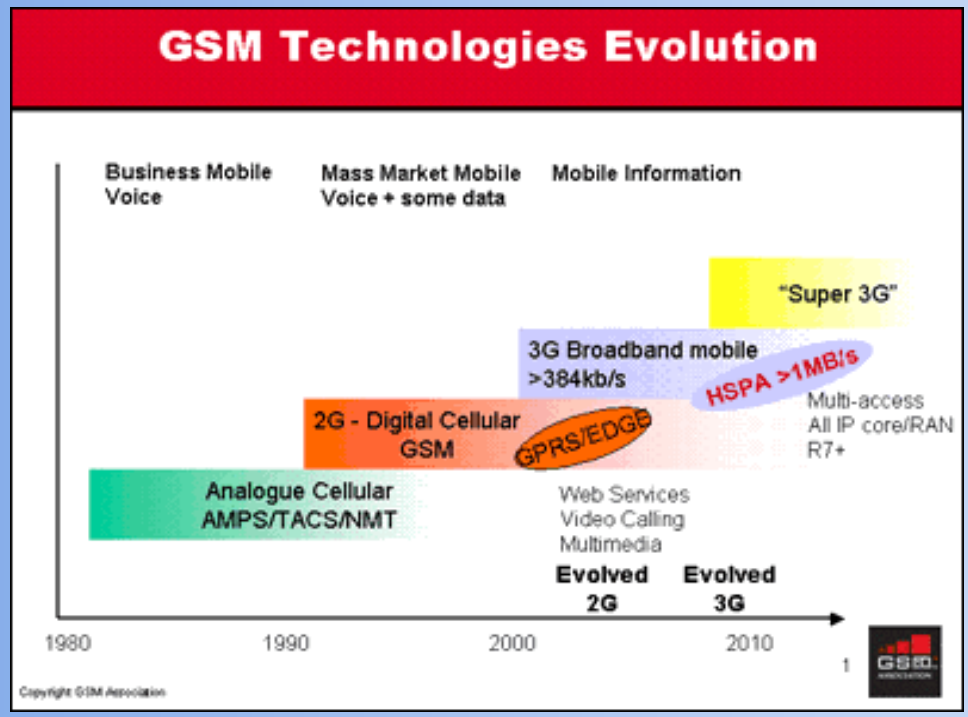
The GSM Network

- BSS
- NSS
- GPRS Core Network



3G

- From 1G to 3G
- 2G Standards: TDMA, CDMA
- 3G Standards: WCDMA, CDMA2000, CDMA 2000 1X



3G offers

- Mobile Internet connectivity
- Mobile email
- Multimedia services
- Wireless application downloading
- Real-time multiplayer gaming
- Video-on-demand

GSM security model

GSM security features:

- Authentication of a user
- Data and signalling confidentiality
- Confidentiality of a user

Overview of the GSM security architecture (1)

- Autentication and key agreement

  - Protect from unauthorized service access
  - Based on the authentication algorith

    A3 (Ki, RAND) → **SRES**

Overview of the GSM security architecture (2)

- Encryption

  - Scramble bit streams to protect signalling and user data
  - Ciphering algorithm A8 (Ki, RAND) → Kc

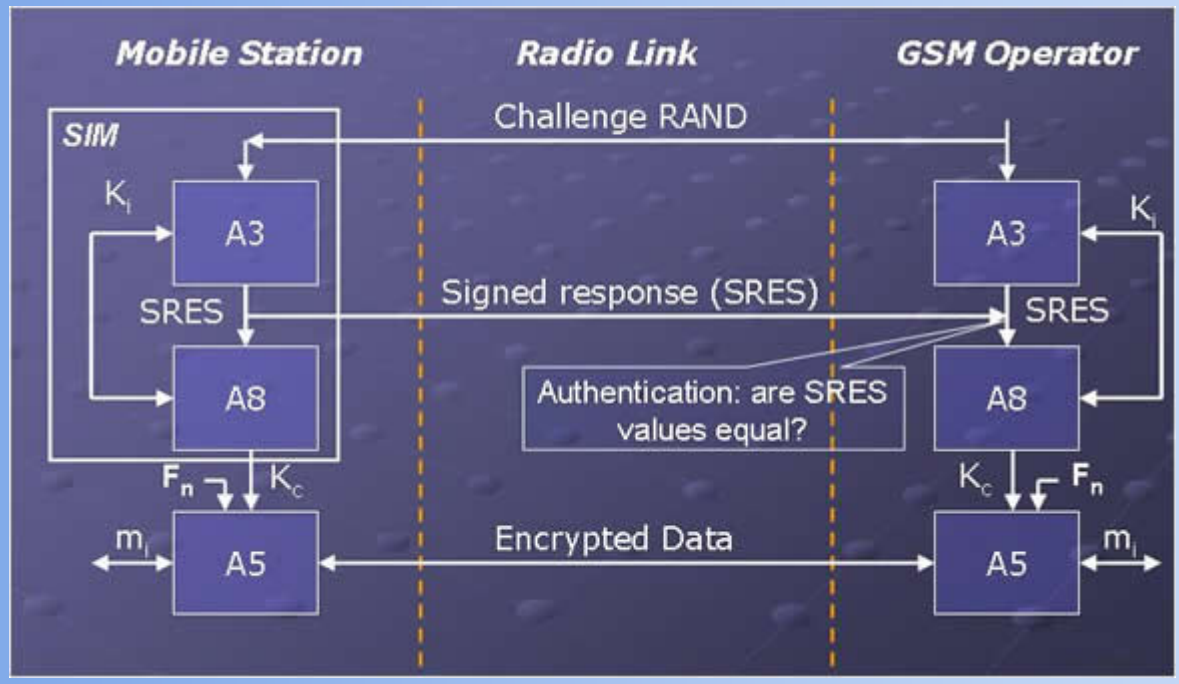
    A5 (Kc, Data) → **Encrypted Data**

Overview of the GSM security architecture (3)

- Allocation and use of temporary identities

  - Prevent intruder from identifying users by IMSI
  - Temporary MSI

Example of GSM security



3G Security Principles

- Builds on the security of the 2G systems
- Corrects weaknesses in 2G systems
- Offers new security features

Weaknesses in 2G security (1)

- active attacks using a „false BTS” are possible
- cipher keys and uthentication data are transmitted in clear between and within networks
- encryption does not extend far enough towards the core network resulting in the cleartext transmission of user and signalling data across microwave links (in GSM, from the BTS to the BSC)

Weaknesses in 2G security (2)

- encryption is not used in some networks, leaving opportunities for fraud
- data integrity is not provided
- the IMEI is an unsecured identity and should be treated as such
- do not have the flexibility to upgrade and improve security functionality over time

3G Security Objectives (1)

- Ensure that information is adequately protected against misuse or misapropriation
- Ensure that the resoursec and services provided are adequately protected against misuse or misappropriation
- Ensure that the security features standardised are compatible with world-wide availability

3G Security Objectives (2)

- Ensure that the level of protection afforded to users and providers of services is better that that provided in contemporary fixed and mobile networks
- Ensure that te security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks

Thank you!