GSM Security and Encryption

David Margrave
George Mason University

"…The use of authentication, encryption, and temporary identification numbers ensure the privacy and anonymity of the system's users, as well as safeguarding the system…"

Reviewer: Jihong Li

GSM Security and Encryption

- Introduction of GSM
- Structure of GSM
- Overview of Cryptography
- Security Features of GSM
- Conclusion

Introduction

- History of GSM

1982:	A study group, Group Special Mobile formed by CEPT
1990:	Phase I GSM specification
1991:	Commercial service
1997:	North America entry, Global System for Mobile communication

- Feature of GSM

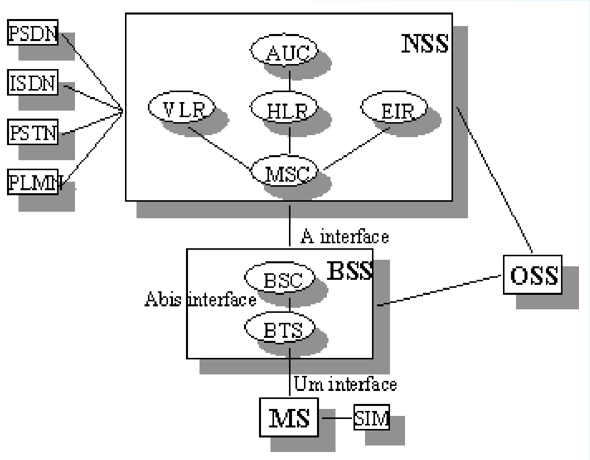
Total Mobility

High capacity and Optimal Spectrum Allocation

Security

Service: telephony, data service, SMS, supplemental services

Structure of GSM



- Mobile Station
- Base Station Subsystem
  - Base Transceiver Station
  - Base Station Controller
- Network and Switching Subsystem
  - Mobile services Switching Center
  - Home Location Register
  - Visitor Location Register
  - Authentication Center (help to verify the user's identity)
  - Equipment Identity Register (contains a list of all valid terminals)
- Operation and Support Subsystem
  - (control and monitor, traffic load of the BSS)

Overview of Cryptography

- Symmetric Algorithms

  Encryption and decryption use the same key

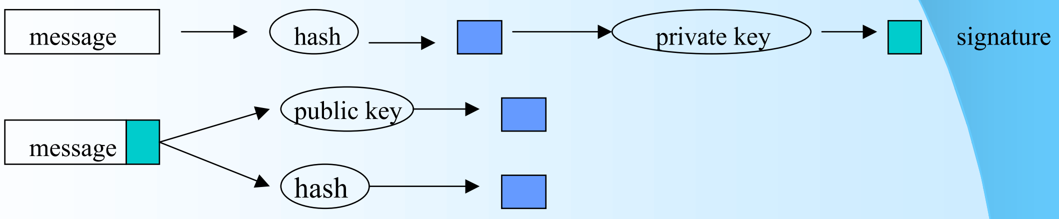
  - Block ciphers: encrypt or decrypt data in blocks or groups of bits. (DES)
  - Stream ciphers: on a bit by bit basis. XOR with the keystream

- Public Key Algorithm

  Data encrypted with a given public key, decrypted with the corresponding private key.

  “one way trap-door” function, factorization problem

- One- way Hash Function (GSM authentication method)



message → hash → → private key → signature

message → public key →

message → hash →

Security Features of GSM

- Aspects of security
  - Subscriber identity authentication
  - Subscriber identity confidentiality
  - Signaling and user data confidentiality
- System elements
  - SIM: IMSI (International Mobile Subscriber Identity)
    Ki (individual subscriber authentication key)
    A8 (ciphering key generation algorithm)
    A3 (authentication algorithm)
    PIN
  - Handset: A5 (ciphering algorithm)
  - GSM network: AUC consists IMSI, TMSI, LAI (location area identity), and Ki
    EIR consists white-listed, grey-listed, and black-listed

Security Features of GSM

- Subscriber identity authentication
  - AUC: send 128 bit RAND
  - MS (SIM): 128 bit + A3 + Ki = 32 bit
  - AUC: re-calculate to verify, check EIR, agree, write information to HLR VLR
- Signaling and user data confidentiality
  - Between MS and BSS:
    SIM: A8 + RAND + Ki = 64 bit ciphering key (Kc)
  - Between MS and NSS:
    A5 + Kc + data

    Kc may be changed at regular intervals as required by network design and security consideration
- Subscriber identity confidentiality

  Same area: TMSI (Temporary Mobile Subscriber Identity)

  Different area: TMSI + LAI (Location Area Identification)

  "… such that the sensitive information is never transmitted over the radio channel…"

Conclusion

- Even with no encryption, GSM is more secure than analog system by using the speech coding, digital modulation and TDMA
- GSM's security methods (authentication, encryption, and temporary identification number) ensure the privacy and anonymity of the system users, as well as safeguarding against fraudulent use.
- My experience is that GSM security adds complexity to the system implement. And the current systems have different kinds of defect

Question?

Do you feel unsafe when you use the mobile phone?