GSM Security

Helsinki University of Technology
S-38.153 Security of Communication Protocols
Mikko.Suominen@hut.fi
15.4.2003

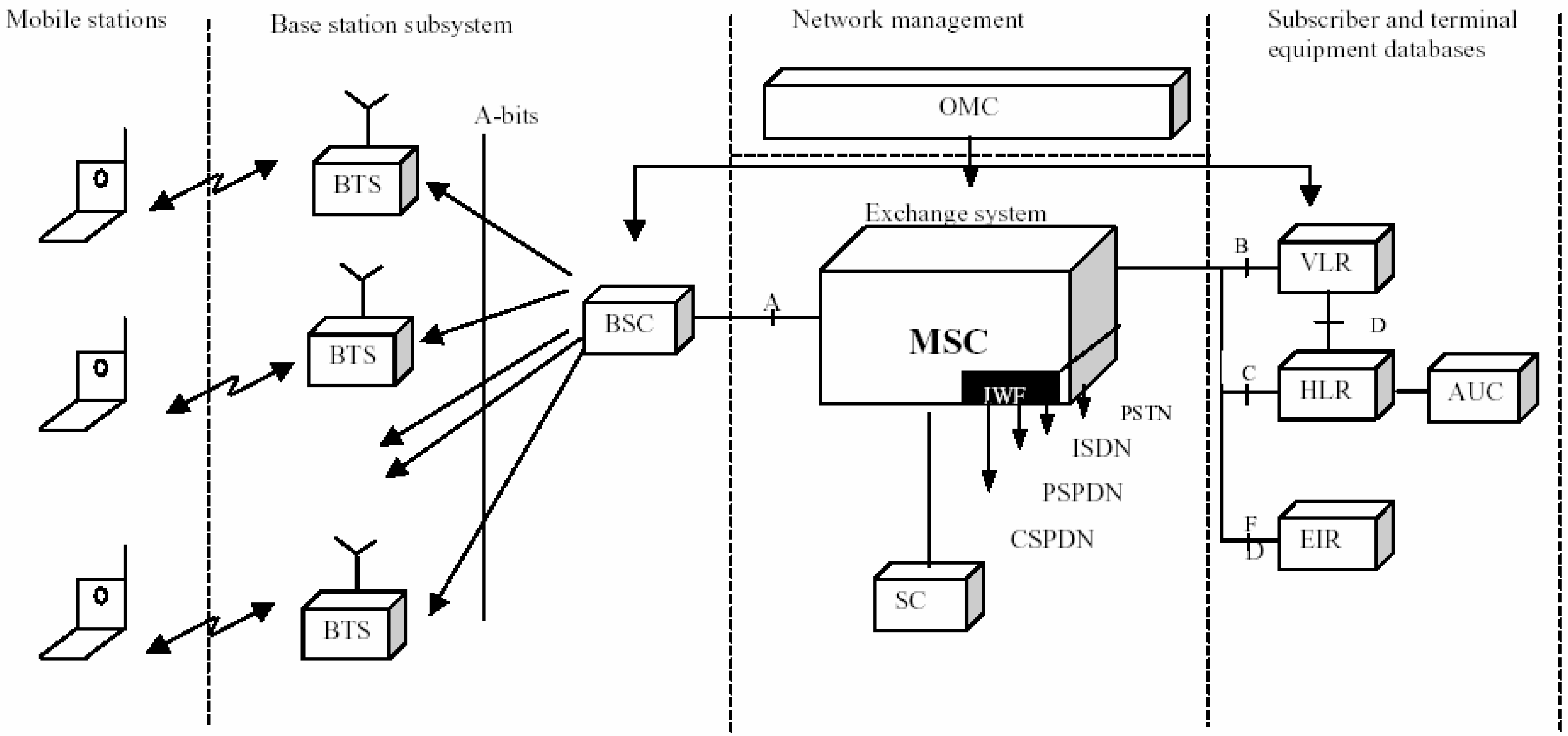
Contents

- Introduction
- GSM security mechanisms
- GSM security concerns
- Conclusion

Introduction

- Global System for Mobile communications
  - Specified by ETSI
  - Digital cellular communications system
  - High mobility (international roaming)
  - Services
    - Voice communication, Short Messaging Service, call waiting, call forwarding, calling line identity, circuit-switched data (packet-switched data with GPRS)

GSM Architecture



Network Databases (1)

- The network subsystem uses the following databases for the authentication and security purposes
  - The HLR database contains all administrative information about each registered user of a GSM network along with the current location of the MS
  - The VLR tracks mobiles that are out of their home network, so that the network will know where to find them

Network Databases (2)

- The EIR contains a list of each MS IMEI allowed on the network
  - White listed – Allowed to connect to the network
  - Grey listed – Under observation for possible problems
  - Black listed – Not allowed to connect to the network
- The AUC database contains:
  - IMSI: International Mobile Subscriber Identity
  - TMSI: Temporary Mobile Subscriber Identity
  - LAI: Location Area Identity
  - Ki: Authentication Key

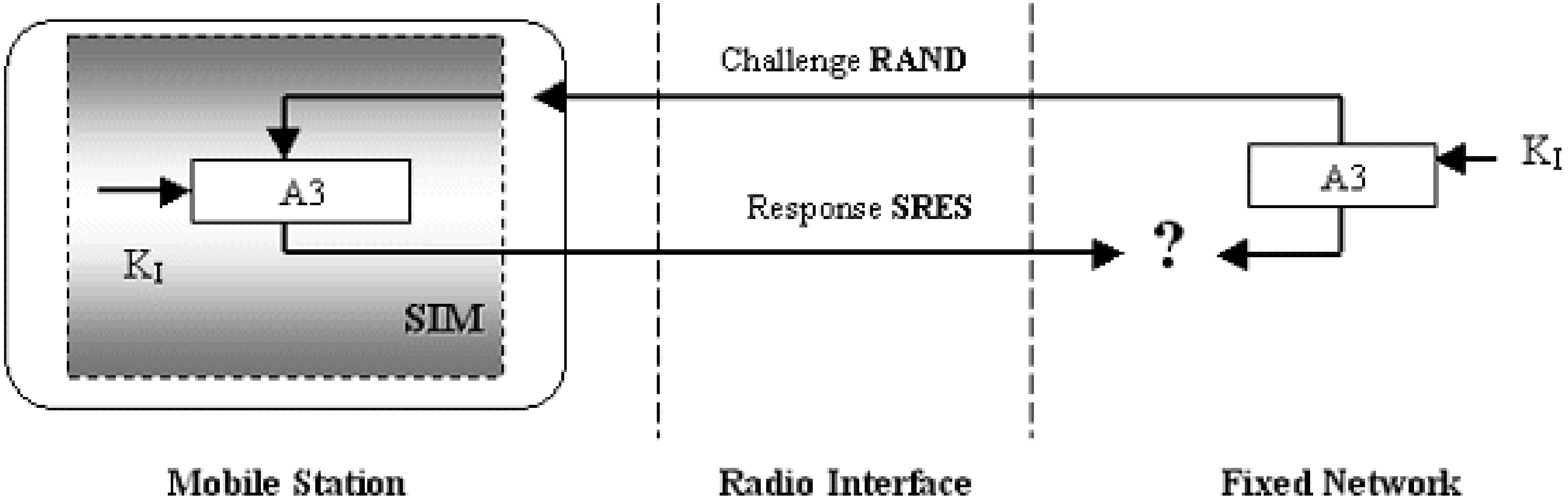
Security Measures in GSM

- PIN code (authentication of SIM = local security measure, network not involved)
- User authentication (performed by network)
- Ciphering of information sent over air interface
- Usage of TMSI (instead of IMSI) over air interface

PIN Code

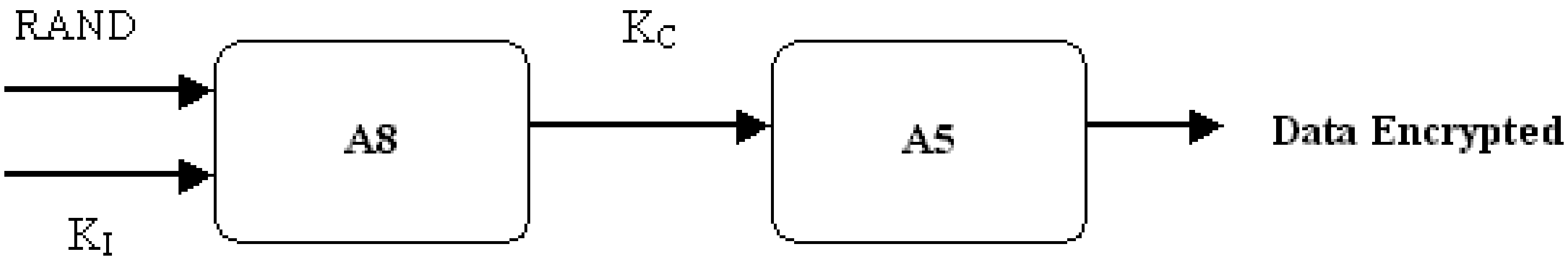
- Personal Identification Number
  - Stored in SIM card
  - Asked when phone is switched on
  - If 3 faulty PIN inputs → longer Personal Unblocking Key (PUK) code is asked
  - If 10 faulty PUK inputs → SIM card is locked → new card from operator

User Authentication



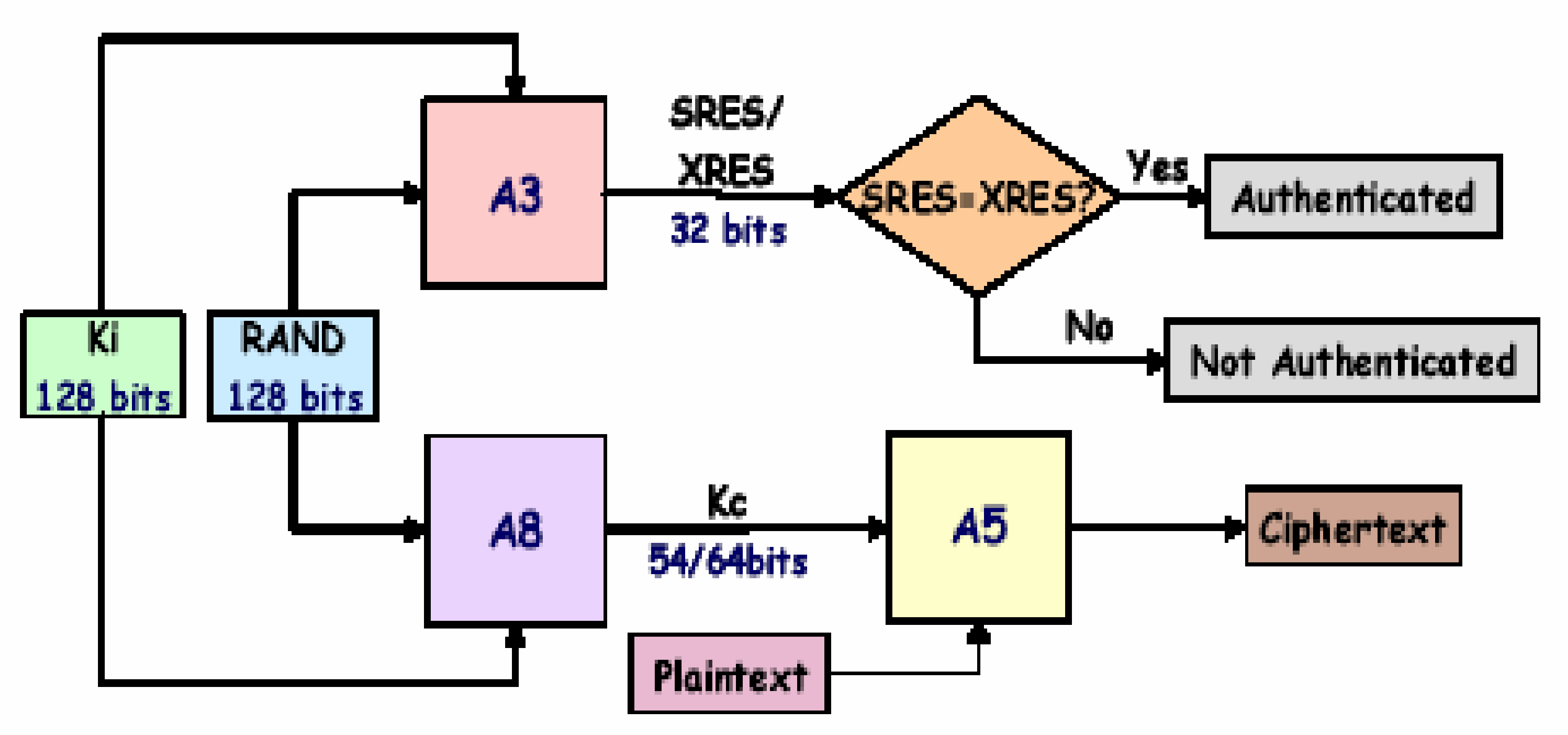
- Authentication key (Ki) is never sent over radio interface!

Ciphering in GSM



- For each call a new ciphering key (Kc) is generated during authentication!

Summary of Algorithms Used



Usage of TMSI (1)

- IMSI uniquely identifies the subscriber
- Rather than sending IMSI, TMSI is sent
- This prevents the intruder from
  - gaining information on the resources the user is using
  - tracing the location of the user
  - matching the user and the transmitted signal

Usage of TMSI (2)

- TMSI is sent to MS after the authentication procedure has taken place
- Mapping of the TMSI to the IMSI is done by the network and is typically handled by the VLR
- IMSI is sent only when necessary, for example
  - when the SIM is used for the first time
  - when there is data loss at VLR

Security through Obscurity

- Authentication and encryption algorithms were never made public
  - Whole security model developed in secret
  - Suspicion that cryptographic algorithms are weak
  - Although never published, ciphering algorithm A5 has been reverse engineered!

SIM Wars: Attack of the Clones

- Cloning of SIM cards is possible
  - Extract Ki from SIM by means of side-channel attack
  - Can retrieve Ki with as little as 8 adaptively chosen plaintexts within a minute
  - Needs physical access to SIM and equipment that is not found from people’s garages (at least at the moment)

Other Concerns

- Only air interface transmission is encrypted
- Ciphering key (Kc) used for encryption is only 54 bits long
- MS is authenticated to the BS, but the BS is not authenticated to the MS → false base stations (man-in-the-middle attack)

Conclusion

- GSM still is a reasonably secure cellular telecommunications system
- However there are some concerns
  - End-to-end security is not provided
  - No open algorithms tested by engineering community
  - SIM cloning is a real threat