



# Mobile Network Security

**Bart Preneel**  
**Katholieke Universiteit Leuven**  
 Dept. Electrical Eng.-ESAT/COSIC  
 February 2004  
 bart.preneel@esat.kuleuven.ac.be  
 http://www.esat.kuleuven.ac.be/~preneel

1

## Agenda

- GSM security architecture
- GSM weaknesses
- UMTS security architecture
- UMTS algorithms
- the future?
  
- not: Bluetooth, IEEE WLAN (802.11)

2

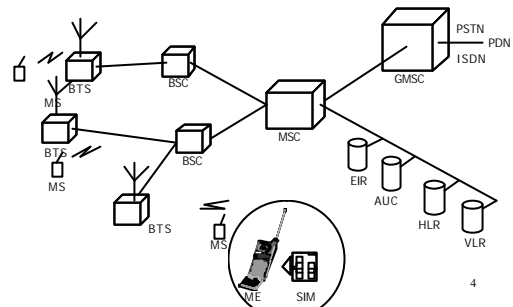


## GSM

- 1982 CEPT: Groupe Speciale Mobile
- 1989 ETSI: GSM
- GSM Association (www.gsm.org) Q1/2004
  - 620 operators on air (includes 3G)
  - 200 countries
  - > 1 billion subscribers
- Evolution towards 3GPP/3GSM:
  - first services: 2002 in Japan and Q3/2003 in Europe

3

## GSM Architecture (1)



4

## GSM Architecture

- User: MS = ME + SIM
  - Mobile subscriber, Mobile Equipment, Subscriber Identity Module
- SIM contains IMSI (International Mobile Subscriber Identity)
- Traffic channels and signalling channels
- Base station, Base station controller
- Visitor Location Register
- Home Location Register
  
- Goal: equivalent security to fixed network

5

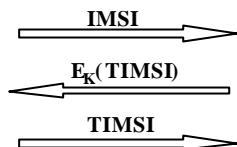
## Security threats

- Interception of data on the air interface
  - data confidentiality
  - anonymity of user
- Illegitimate access to a mobile service
  - billing
  - masquerading
- Security services:
  - subscriber identity confidentiality
  - subscriber identity authentication
  - user data confidentiality
  - signalling information confidentiality

6

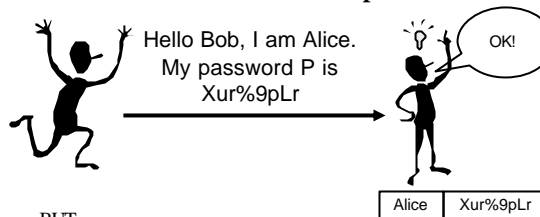
### Temporary identities

- IMSI (15 digits) is used only for first call, or in exceptional circumstances
- replaced by TIMSI (5 digits)
  - assigned by VLR, stored with IMSI and location info
  - sent encrypted to MS
  - replaced at each location update procedure
- TIMSI is forwarded to new VLR



7

### 1G: identification with passwords

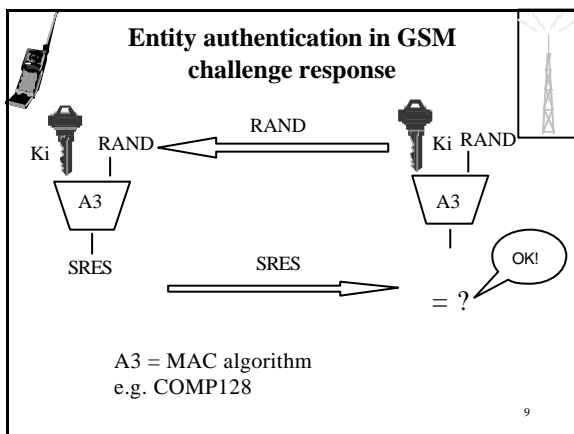


BUT

- Eve can guess the password
- Eve can listen to the channel and learn Alice's password
- Bob needs to know Alice's secret
- Bob needs to store Alice's secret in a secure way

8

### Entity authentication in GSM challenge response



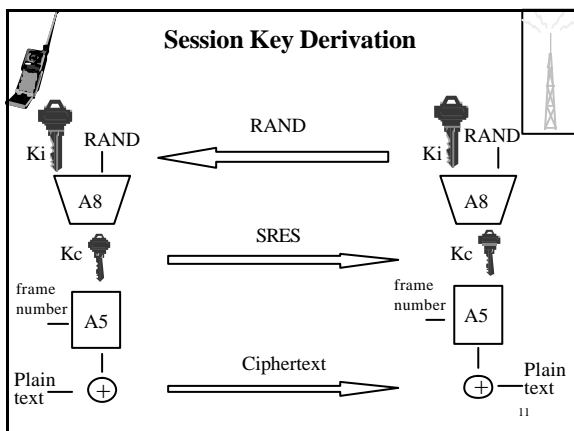
9

### Entity Authentication in GSM (2)

- + Eve cannot guess the secret key  $K_i$  (128 bits)
- + Eavesdropping the channel does not help Eve: next time Bob will ask a different question (different challenge RAND)
- Bob needs to know Alice's secret, and needs to store it securely
- Eve can just wait till the end of the call setup and then.....
  - how to address this problem? AKA

10

### Session Key Derivation

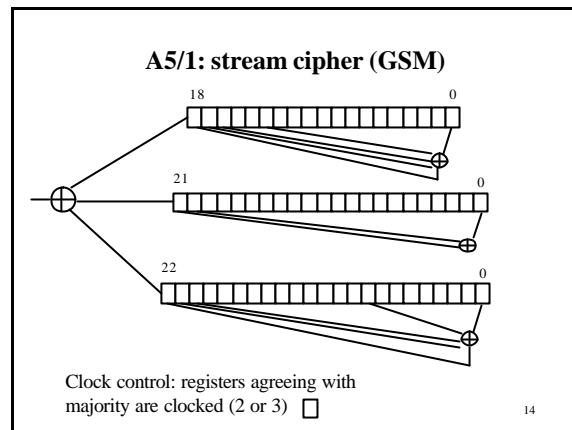
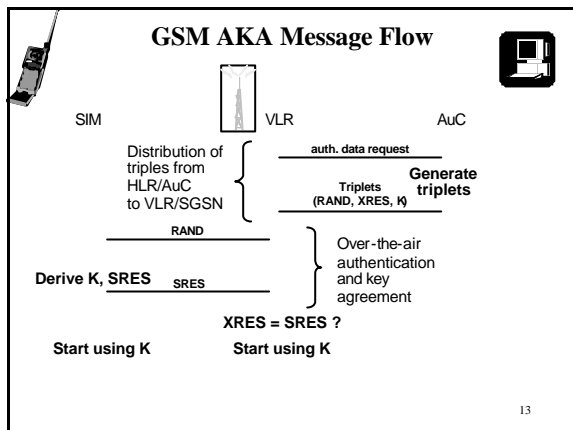


11

### Parameter sizes

- RAND: 128 bits
- Ki: 128 bits
- Kc: 64 bits - 10 bits = 54 bits
- SRES: 32 bits
- plaintext and ciphertext: 114-bit blocks
- A5 (hardware in phone):
  - currently 2 versions A5/1, A5/2
  - A5/3 will be deployed soon
- A3/A8 (software in SIM): operator dependent (example COMP128)

12



- ### A5/1 and A5/2: stream ciphers
- A5/1**
- exhaustive key search:  $2^{54}$
  - search 2 registers:  $2^{45}$  steps
  - [BD00] 2 minutes of plaintext,  $2^{40}$  steps
    - $2^{38}$  precomputation, 64 GB storage
  - [BWS00] 2 minutes of plaintext: 1 second
    - $2^{42}$  precomputation, 300 GB storage
  - [BWS00] 2 seconds of plaintext: 1 minute
    - $2^{48}$  precomputation, 146 GB storage
- A5/2:**
- similar hardware to A5/2 but deliberately weak  
 $2^{16}$  steps, known plaintexts for 2 separate frames (6 sec. apart)<sup>15</sup>
- 16

- ### Key management
- User keys  $K_i$  stored in Authentication Centre (AuC)
  - generation of user keys  $K_i$ :
    - from master key, IMSI and some other data
    - randomly, but then stored encrypted under storage key
  - VLR typically gets only a few triplets (RAND, SRES,  $K_c$ ) - typically transmitted in clear from HLR
- 16

- ### Limitations of GSM Security
- Problems with GSM security stem by and large from design limitations on what is protected rather than on defects in the security mechanisms themselves
    - only provides **access security** - communications and signalling in the fixed network portion aren't protected
    - does not address **active attacks**, whereby network elements may be impersonated
    - designed to be only as secure as the fixed networks to which they connect
    - lawful interception only considered as an after thought
- 17

- ### Limitations of GSM Security, 2
- Failure to acknowledge limitations
    - encryption needed to guard against radio channel hijack
    - the terminal is an unsecured environment - so trust in the terminal identity is misplaced
  - Inadequate flexibility to upgrade and improve security functions over time
  - Lack of visibility that the security is being applied
    - no indication to the user that encryption is on
    - no explicit confirmation to the home network that authentication is properly used when customers roam
- 18

### Limitations of GSM Security, 3

- Lack of confidence in cryptographic algorithms
  - lack of openness in design and publication of A5/1
  - misplaced belief by regulators in the effectiveness of controls on the export or (in some countries) the use of cryptography
  - key length too short, but some implementation faults make increase of encryption key length difficult
  - need to replace A5/1, but poor design of support for simultaneous use of more than one encryption algorithm, is making replacement difficult
  - ill advised use of COMP 128 (A3)

19

### Specific GSM Security Problems

- Encryption terminated too soon
  - user traffic and signalling in clear on microwave links
- Clear transmission of cipher keys & authentication values within and between networks
  - signalling system vulnerable to interception and impersonation
- Confidence in strength of algorithms
  - failure to choose best authentication algorithms
  - improvements in cryptanalysis of A5/1
- Use of false base stations

20

### False Base Stations

- Used as *IMSI Catcher* for law enforcement
- Used to intercept mobile originated calls
  - encryption controlled by network and user unaware if it is not on
- Dynamic cloning risk in networks where encryption is not used



21

### Some SMS Issues

- Early pre-pay phones had free SMS due to lack of billing system integration
- SMS Identity spoofing
  - Faked "caller-ID" data
- SMS viruses ... crash certain phones
  - Badly-formatted binary messages

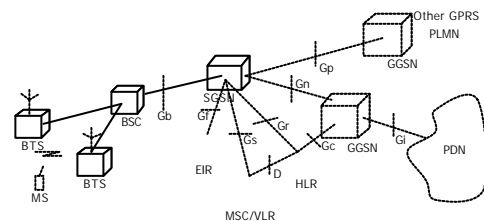
22

### GSM+ or 2.5G

- HSCSD High Speed Circuit Switched Data
- GPRS General Packet Radio Service
- EDGE Enhanced Data Rate for GSM Evolution

23

### GPRS Architecture



24

## GPRS (1)

Data solution over GSM networks

Mobile devices are IP enabled

- “Egg-shell”-type networks
- GGSN Gateway GPRS Support Node
  - limited filtering/firewalls
  - standard UNIX variants without hardening
- Operation & Management Network
  - service both GPRS and bearer networks
  - connect to corporate networks
- no means of synchronization: problem for logs

25

## GPRS (2)

- GSM operators become ISPs
  - immature products
  - inadequate procedures
  - device security not considered
  - no vendors are implementing handset lockout for GPRS-only handsets
  - no user segregation
- GPRS mobile equipment weaknesses
  - risk for flawed SMS clients and PC clients
  - storage of GPRS/WAP credentials in clear on the SIM

26

## UMTS: the terminals

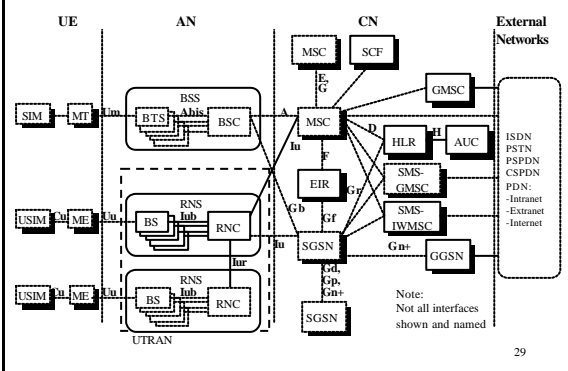


## Principles for 3G Security

- Build on the security of GSM
  - adopt the security features from GSM that have proved to be needed and robust
  - try to ensure compatibility with GSM in order to ease inter-working and handover
- Correct the problems with GSM by addressing its real and perceived security weaknesses
- Add new security features
  - as are necessary to secure new services offered by 3G
  - to take account of changes in network architecture

28

## Building on GSM Security - Architecture



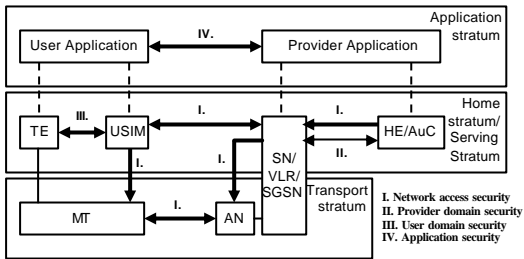
29

## Building on GSM Security, 2

- Remain compatible with GSM network architecture
- User authentication & radio interface encryption
- SIM used as security module
  - removable hardware
  - terminal independent
  - management of all customer parameters
- Operates without user assistance
- Requires minimal trust in serving network

30

### 3GPP Security Architecture Overview



31

### Authentication & Key Agreement (AKA) Protocol Objectives

- Authenticate user to network & network to user
- Establish a cipher key CK (128 bit) & an integrity key IK (128 bit)
- Assure user and network that CK/IK have not been used before
- Authenticated management field HE ? USIM
  - authentication key and algorithm identifiers
  - limit CK/IK usage before USIM triggers a new AKA

32

### AKA Prerequisites

- AuC and USIM share
  - user specific secret key K
  - message authentication functions  $f_1, f_1^*, f_2$
  - key generating functions  $f_3, f_4, f_5$
- AuC has a random number generator
- AuC has scheme to generate fresh sequence numbers
- USIM has scheme to verify freshness of received sequence numbers

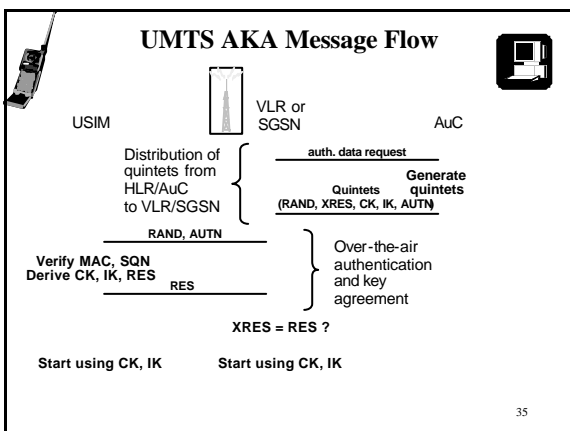
33

### AKA Variables and Functions

RAND = random challenge generated by AuC  
 XRES =  $f_{2K}(RAND)$  = expected user response computed by AuC  
 RES =  $f_{2K}(RAND)$  = actual user response computed by USIM  
 CK =  $f_{3K}(RAND)$  = cipher key  
 IK =  $f_{4K}(RAND)$  = integrity key  
 AK =  $f_{5K}(RAND)$  = anonymity key  
 SQN = sequence number  
 AMF = authentication management field  
 MAC =  $f_{1K}(SQN || RAND || AMF)$  = message authentication code computed over SQN, RAND and AMF  
 AUTN = SQN? AK || AMF || MAC = network authentication token, concealment of SQN with AK is optional  
 Quintet = (RAND, XRES, CK, IK, AUTN)

34

### UMTS AKA Message Flow



35

### Length of AKA Cryptographic Parameters

- K 128 bits
- RAND 128 bits
- RES 32-128 bits
- CK 128 bits
- IK 128 bits
- AUTN 128 bits
  - SQN Sequence number 48 bits
  - AMF Authentication management field 16 bits
  - MAC Message authentication code 64 bits

36

## General Approach to Algorithm Design

- Robust approach to exportability - full strength algorithm and expect agencies to fall into line
- ETSI SAGE appointed as design authority
- Take existing algorithm as starting point
- Use block cipher as building block for both algorithms - MISTY1 chosen (64-bit block)
  - fairly well studied, some provable security aspects
  - parameter sizes suitable
  - designed to be efficient in hardware and software
  - offered by Mitsubishi free from royalty payments

37

## Kasumi

- Simpler key schedule than MISTY
- Additional functions to *complicate* cryptanalysis without affecting provable security aspects
- Changes to improve statistical properties
- Minor changes to speed up or simplify hardware
  - goal: < 10.000 gates / 2 Mbit/s
- Stream ciphering f8 uses Kasumi in a form of output feedback, but with:
  - BLKCNT added to prevent cycling
  - initial extra encryption added to protect against chosen plaintext attack and collisions
- Integrity f9 uses Kasumi to form CBC MAC with:
  - non-standard addition of 2nd feedforward

38

## Choice of algorithms

- Mobile phone: KASUMI in hardware for encryption and MAC calculation (standard for all operators)
- USIM card: operator specific algorithm for f1 through f5
  - example is MILENAGE, based on Rijndael/AES
  - operators inclined to design their own algorithms

39

## Other Aspects of 3GPP Security

- Options in AKA for sequence management
- Re-authentication during a connection and periodic in-call
- Failure procedures
- Interoperation with GSM
- AKA+ and interoperation with 3GPP2 standards
- Formal analysis of AKA
- User identity confidentiality and enhanced user identity confidentiality (R00)
- User configurability and visibility of security features
- User-USIM, USIM-terminal & USIM - network (SAT)
- Terminal (identity) security
- Lawful interception
- Fraud information gathering
- Network wide encryption (R00)
- Location services security
- Access to user profiles
- Mobile IP security (R00+)
- Provision of a standard authentication and key generation algorithm for operators who do not wish to produce their own

40

## References to 3GPP Security

### Principles, objectives and requirements

- TS 33.120 Security principles and objectives
- TS 21.133 Security threats and requirements

### Architecture, mechanisms and algorithms

- TS 33.102 Security architecture
- TS 33.103 Integration guidelines
- TS 33.105 Cryptographic algorithm requirements
- TS 22.022 Personalisation of mobile equipment

### Lawful interception

- TS 33.106 Lawful interception requirements
- TS 33.107 Lawful interception architecture and functions

### Technical reports

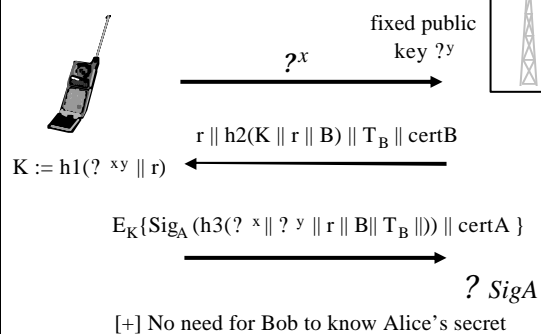
- TR 33.900 A guide to 3G security
- TR 33.901 Criteria for cryptographic algorithm design process
- TR 33.902 Formal analysis of the 3G authentication protocol
- TR 33.908 General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms

### Algorithm specifications

- Specification of the 3GPP confidentiality and integrity algorithms
  - Document 1: f8 & f9
  - Document 2: KASUMI
  - Document 3: implementors' test data
  - Document 4: design conformance test data

41

## Identification in future mobile systems



42

### **Credits**

- Part on GSM: Klaus Vedder, Security Aspects of Mobile Communications, LNCS 741, Springer-Verlag 1993.
- Part on 3GPP is based on: Mike Walker, On the security of 3GPP networks, invited talk at Eurocrypt 2000, May 2000, Bruges, Belgium.

43