Mobile networks security

TkL Markus Peuhkuri

2007-04-03

Lecture topics

- Historical background
- Structure of security
- Smart cards
- GSM
- UMTS
- After this lecture, you should
  - know why GSM became success (from authentication perspective)
  - know how UMTS has envolved from that
  - be able to compare GSM and UMTS security

History of mobile phones

- Radio-telephone (0G)
  - manual operation, no cell structure
  - no privacy as signal was transmitted analog, a scanner radio was sufficient to listen
  - no authentication
  - ARP (AutoRadioPuhelin, VHF frequency)
- Analog mobile phones (1G)
  - cell structure (hand-overs)
  - no privacy, weak authentication
  - NMT (Nordisk Mobil Telefon, 450 and 900 MHz), AMPS (Advanced Mobile Phone System, 800 MHz)
- Digital mobile phones (2G. . .)
  - better privacy, better radio frequency utilisation

GSM security principles

- Two main problems with analog phones
  - eavesdropping
    ⇒ should have same security as fixed landlines
  - phone fraud
    ⇒ cloning should be difficult
- Authentication
  - masquerading as an genuine user should be difficult

- Confidentiality
  - user data transmission protected
  - signalling traffic protected, as some parts of signalling traffic such as phone numbers are sensitive
- Anonymity
  - third party could not identify users
  - user tracking should not be possible
- Use of SIM card
  - subscriber personalised
  - all sensitive operations on card, avoids vendor-specific class attack, no serviceable components inside

Smart cards

- Storage cards (2 €)
  - have 1 – 4 KiB (EEPROM) memory to store information
  - no security measures on card
  - magnetic-strip cards have 140 B memory (0.5 €)
- Processor cards (5 – 15 €)
  - 8- or 16-bit processor
  - RAM 2 KiB
  - ROM 64 KiB
  - EEPROM 32 KiB
  - cryptographic accelerators for encryption or public-key operations
- Common standard ISO/IEC 7816

ISO/IEC 7816

- Defines contact smart cards
- Physical size and contacts
- Commands with 4-byte APDU (Application Protocol Data Unit)
  - possibly encrypted and signed commands / responses
- Different files

  MF master file, "root file"

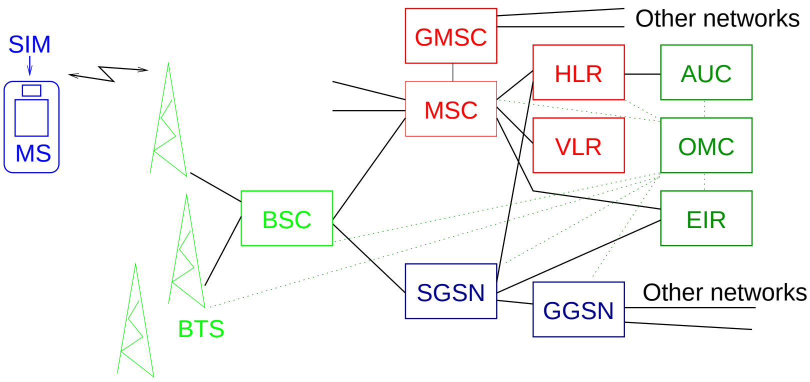
  DF dedicated file, "directory"

  EF elementary file
    - transparent files: files like ones in computers, no structure imposed by card; just array of bytes.
    - linear fixed: fixed-size records, addressed by ID and byte offset.
    - linear variable: as above, but record size can be variable.
    - cyclic files: provides fixed number of records and oldest are overwritten if file gets full.

Development in smart cards

- More power
  - 32-bit processor
  - MiB-class non-volatile memory
- Downloadable program code
  - Java card
  - makes possible to have multi-functional cards
  - SIM application toolkit
- Contactless cards
  - close-coupled cards ISO/IEC 10536 1 cm
  - proximity cards ISO/IEC 14443 10 cm
  - vicinity cards ISO/IEC 15693 1 m
  - for high-security applications contact cards preferable
  - multi-mode cards: for example authentication using contactless part and signatures over contact interface only. Using over-the-air interface posses always some risks. For example, in normal case Bluetooth access to phone is possible withing few meters only. However, someone has communicated with standard mobile phone on Bluetooth over distance of 1.6 km using special antenna and hardware.

GSM system structure (with GPRS)



GSM system components

- Subscriber equipment

  MS Mobile Station — mobile phone

  SIM Subscriber Identity Module — holds subscriber information

- Base Station Subsystem (BSS)

  BTS Base Tranceiver Station — radio interface

  BSC Base Station Controller — controls handover, cell configuration

  TRAU TRAnscoder Unit — converts 9.6 kbit/s GSM speech to 64 kbit/s PCM. Can be integrated to BSC.

Network and Switching subsystem

Acronym: NSS

MSC Mobile Services Switching Center — switches calls, signalling and ticketing

HLR Home Location Register — stores data about each subscriber

VLR Visitor Location Register — holds information of roaming GSM subscribers

GMSC Gateway Mobile Services Switching Center — interconnecting to other telephone networks

GSM system components

- Operation subsystem (OSS)

  OMC Operating and Maintenance Centre – network management

  AuC Authentication Center — stores user authentication data

  EIR Equipment Identity Register — contains lists of white-, grey- and blacklisted equipment

- GPRS extension

  SGSN Serving GPRS Support Node — MSC for packet data

  GGSN Gateway GPRS Supporting Node — interfacing to packet networks

- Virtual operator does not have a radio access network
- Service provider uses network provider's MSC

GSM security

- Shared key $\mathcal{K}_I$ with SIM and AUC
  - used both for authentication and encryption
- Several algorithms

  A3 authentication

  A5 data encryption

  A8 key generation

- Some algorithms selected by operator
- Use of temporary identity TMSI

Authentication in GSM

1. MS send channel allocation request
2. MSC instructs BTS and MS for right channel
3. MSC asks MS for IMSI
4. MSC asks HLR/AUC for authentication data triplets: typically receives 5 triplets to be used

   RAND random value, 128-bit

   SRES response for challenge: A3($\mathcal{K}_I, \texttt{RAND}$), 32-bit

   $\mathcal{K}_c$ Cipher key: A8($\mathcal{K}_I, \texttt{RAND}$) 64-bit

5. MSC sends challenge `RAND`

6. SIM calculates response `SRES`
7. MSC verifies response `SRES`
8. MSC sends $\mathcal{K}_c$ to BSC
   ⇒ communication encrypted
9. TMSI assigned for MS

Selecting A3

- A3 selected by operator
  - in most cases, COMP128 used that was provided as "an example only"
  - can be broken with 2^{17} queries (524288), takes 8 hours
  - side channel attack with 8 plaintext for some SIM cards. [5] A side channel attack is one that uses physical characteristics of device under study to learn secret key. Side channels include power consumption, operation timing and electromagnetic radiation.
- Lession learned
  - do not use weak algorithm as an example
  - provide reasonable set of *good* algorithms
  - ability to change is good

GSM data encryption

- Enciphering key $\mathcal{K}_C = \text{A8}(\mathcal{K}_I, \texttt{RAND})$
- A8 selected by operator
  - in most cases, COMP-128 used
- Data encrypted with A5 stream cipher
  - originally only $\mathcal{K}_C$ 54 effective bits because of cryptographic equipment regulations
  - signalling limits to 64 bits
  - known plaintext attack efficient to A5/1
  - A5/2 very weak, complexity 2^{17} [4]
    ⇒ bidding-down attack: if one can have mobile phone to switch temporally to A5/2, then the key can be easily broken. The phone will use the same key for A5/1.

GSM security problems

- Cipher algorithms were not published. This was mainly because of 1980s political environment (no strong crypto to minions) and thus A5 did not receive public review. However, the attack A5 is vulnerable was known before use of A5 was decided. Also weak COMP128 was published as an example algorithm of A3/A8 so most went with it.
- Too short key lengths because they should work in early 1990s portable equipment; also political reasons.
- Not designed to withstand active attacks as equipment needed for those attacks (fake base station) was considered too expensive. However, this is not anymore the case as network equipment prices have gone down.
- Only MS – BTS protected by cryptology leaving traffic on microwave links without protection (if links do not have any link-layer protection).

UMTS architecture

- Builds on releases
  - R99 based much on GSM/GPRS model
  - R4 improvements
  - R5 towards All-IP
- Native access network UTRAN (Universal Terrestrial Radio Access Network) WCDMA
  - GSM/GPRS/EDGE = GERAN: GSM EDGE Radio Access Network
  - WLAN access network, for example UMA (Unlicensed Mobile Access)
- Changes in protocols: multiple IP addresses and PDP (Packet Data Protocol) contexts

[1]

UMTS security [2]

- Builds on GSM security
  - success
  - interoperability
- Access security
- Network domain security
- IP multimedia subsystem security

UMTS access security

- Mutual authentication
  - both network and user authenticates
  - network conforms user (MS) USIM
  - serving network (SE) is authorised by home network
- Signalling data integrity and authentication
  - secure agreement on the integrity algorithm and the key
  - signalling originates from the right party
- Equipment identification
  - no authentication because of complexity and additional expenses in manufacturing and in service

UMTS access confidentiality

- User traffic confidentiality
  - secure agreement on ciphering algorithm and key
  - both user data and signalling data protected
  - extends to RNC (UMTS-BSC)
  - security indicator, that operator may opt to disable, however
- User identity confidentiality
  - IMSI not communicated in clear
  - location confidentiality, TMSI changed frequently
  - service untraceability

- USIM functions
  - user authentication (PIN)
  - terminal authentication (SIM lock)
  - USIM application toolkit communication

UMTS authentication: script

- Three parties
  - AuC at HE (home environment)
  - VLR at SN (serving network), SGSN for packet data
  - USIM at ME
- Trusts
  - HE gives authentication data to trusted SNs
  - SN handles authentication data securely
  - SN: HE sends correct information and pays for services
  - SN accepts authentication data from trusted HEs
  - networks between HE and SN secure

UMTS authentication

- Authentication data: n quintets from HE to SN

  RAND random number

  XRES expected response

  CK cipher key

  IK integrity key

  AUTN authentication token

- ME receives RAND and AUTH
  - checks that AUTN is fresh
  - computes RES, sends to SN
  - computes CK, IK from $(\mathcal{K}_I, RAND)$
- No long-time authentication data for SN
- Transparent to SN
- Interoperability with GSM (triplet)

UMTS integrity algorithm

- Algorithm f8
- Based on KASUMI block cipher
- Inputs

  IK 128-bit key

  COUNT-I time-dependent 32-bit value

  FRESH 32-bit value

  DIRECTION transmission direction to protect reflection attack

  MESSAGE integrity protected

- Produces MAC

- Integrity protected even if communication plain
  - attacker cannot bid-down communication encryption
  - provides safety margin
  - protects signalling
- Also a mode where only amount of data transmitted and received is protected

UMTS confidentiality algorithm

- Algorithm f9
- Based on KASUMI block cipher
- Inputs

  CK 128-bit key

  COUNT-C time-dependent 32-bit value

  BEARER

  DIRECTION transmission direction

  LENGTH of message
- Produces blocks of key stream

Network domain security

- SS7 (Signalling System #7) network
  - earlier, only small number of trusted parties
  - no cryptographic security
  - interoperability with Internet (VoIP etc.)
- MAPSEC — protect MAP traffic (Mobile Application Part: GSM-specific extensions for SS7)
  - R4
  - similar to IPSec SA
  - network-level SAs
  - encapsulated MAP messages:
    security header || f6(MAP) || f7(security header || f6(MAP))

    f6 AES in counter mode

    f7 AES in CBC-MAC mode
  - only critical messages protected
- R5 will use subset of IPSec
  - ESP in tunnel mode
  - AES encryption
  - IKE with pre-shared secrets

IP multimedia security

- Use of SIP and SDR
- SIP with S/MIME not practical
  - large messages over air interface, although SIP messages are already much larger compared to GSM signalling
- SIP with TLS not suitable
  - mainly used UDP
  - prefer not public-key algorithms
- IPSec tunnels with CSCFs (call session control functions)
- HTTP Digest AKA authentication (Authentication and Key Agreement [3])

Intelligent Network Services

- Camel: IN services for GSM / UMTS networks
- MExE: Mobile Station Execution Environment
  - platform-independent
  - classmarks
    1. WAP
    2. PersonalJava / JavaPhone
    3. J2ME CLDC, MIDP
  - permissions framework: domains
    * operator
    * manufacturer
    * third party (trusted)
    * untrusted

Radio-level attacks in mobile networks

- Radio jamming
  - decrease S/N ratio
  - pulse jamming can be efficient
  - signalling channel most vulnerable
- Channel allocation using RACH (Random Access CHannel)
  - slotted aloha
  - greedy client causes others to backoff
- Traffic analysis
  - services may be identified based on traffic profile

Summary

- Use of smart card provides
  - controlled environment
  - independence from equipment
- Each design decision is a guess
  - availability and cost of hardware
  - business models
- Network authentication improves user security

Part of material on this lecture is based on lecture notes for TKK course S-38.193 by Jouni Karvo and to book Mobile Radio Networks by Bernhard H. Walke.

References

[1] Overview of 3gpp release 99 — summary of all release 99 features. Technical report, ETSI MObile Competence Centre, 2004. URL:`http://www.3gpp.org/Releases/Rel99%20description_v040720.doc`.

[2] K. Boman, G. Horn, P. Howard, and V. Niemi. Umts security. *Electronics & Communication Engineering Journal*, 14(5):191–204, October 2002.

[3] A. Niemi, J. Arkko, and V. Torvinen. *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*, September 2002. RFC 3310. URL:`http://www.ietf.org/rfc/rfc3310.txt`.

[4] Slobodan Petrovic and Amparo Fúster-Sabater. Cryptanalysis of the a5/2 algorithm. Cryptology ePrint Archive, Report 2000/052, 2000. `http://eprint.iacr.org/`.

[5] J.R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely. Partitioning attacks: or how to rapidly clone some GSM cards. In *IEEE Symposium on Security and Privacy Proceedings 2002*, pages 31–41, 2002.