3G Security Overview

Peter Howard
Research and Standards Engineer
Communications Security and Advanced Development
Vodafone Limited
peter.howard@vf.vodafone.co.uk

Contents

• Background and context
• Principles and objectives for 3G security
• 3G threat analysis and security requirements capture
• Overview of 3G security features
• The 3G security architecture
• The USECA demonstrator
GSM security

- One of the aspects of GSM that has played a significant part in its global appeal is its set of security features
- GSM was the first public telephone system to use integrated cryptographic mechanisms
- By virtue of GSM penetration, these mechanisms have achieved the status of being the most widespread household use of cryptography
- GSM security model has been adopted, modified and extended for DECT, TETRA and now 3GPP

GSM security features

- Secure user access to telecommunications services
  - Allows a network operator to authenticate the identity of a user in such a way that it is practically impossible for someone to make fraudulent calls by masquerading as a genuine user
- User and signalling traffic confidentiality
  - Protects user traffic, both voice and data, and sensitive signalling data, such as dialled telephone numbers, against eavesdropping on the radio path
- User anonymity
  - Designed to protect the user against someone, who knows the user’s IMSI, from using this information to track the location of the user or to identify calls made to or from that user by eavesdropping on the radio path
GSM security mechanisms

- Cryptographic authentication verifies the subscription with the home network when service is requested
  - Challenge / response authentication protocol based on a subscriber specific secret authentication key
- Radio interface encryption prevents eavesdropping and authenticates the use of the radio channel - the latter is often forgotten
  - The encryption mechanism is based on a symmetric stream cipher
  - The key for encryption is established as part of the authentication protocol
- The allocation and use of temporary identities helps to provide user anonymity

Overview of the GSM security architecture

- Authentication and key agreement
- Encryption
- Allocation and use of temporary identities
**USECA**

**Authentication and key agreement protocol**

**MS/SIM**
- **Ki**: Subscriber authentication key
- **A3**: Algorithm for calculating RES
- **A8**: Algorithm for calculating Kc
- **RAND**: User challenge
- **(X)RES**: (Expected) user response
- **Kc**: Encryption key

{RAND, XRES, Kc}: Security triplet

**MSC/VLR**
- **A3**: Algorithm for calculating RES

**HLR/AuC**
- **Ki**: Encryption key

Authentication Data Request

(RAND, XRES, Kc)

**MS/SIM** Mobile Station / Subscriber Identity Module
**MSC/VLR** Mobile Switching Centre / Visitor Location Register
**HLR/AuC** Home Location Register / Authentication Centre

**The encryption mechanism**

**MS/SIM**
- **Kc**: Encryption key
- **A5**: Algorithm for encryption / decryption

**BS**

**MSC/VLR**
- **Kc**: Encryption key

plaintext ciphertext plaintext ciphertext plaintext ciphertext

**Uplink traffic**

**Downlink traffic**

MS/SIM Mobile Station / Subscriber Identity Module
BS Mobile Switching Centre / Visitor Location Register

IIR Fraud and Security Conference, March 2000 - 7 - 3G Security Overview

IIR Fraud and Security Conference, March 2000 - 8 - 3G Security Overview
**Security for later GSM developments**

- **GPRS security**
  - Same architecture for authentication and key agreement
  - Encryption applied at LLC layer and extended further back into core network
  - New encryption algorithms

- **SIM toolkit security**
  - Allows a secure channel to be established between the SIM and a network server
  - For applications which demand security features beyond those originally offered by GSM
    - applications in electronic commerce
    - secure remote management of SIMs or mobile stations
USECA

Limitations considered

- COMP-128
- A5/1
- False base station attacks
- Encryption key length
- Terminated of encryption in the base station
- Core network signalling security

- Attacks are complex

- This is not like analogue cloning or eavesdropping

USECA

3GPP security principles

- Ensure that 3G security builds on the security of GSM where features that have proved to be needed and that are robust shall be adopted for 3G

- Ensure that 3G security improves on the security of second generation systems by correcting real and perceived weaknesses

- Ensure that new 3G security features are defined as necessary to secure new services offered by 3G
USECA

3G security objectives

- Ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation
- Ensure that the resources and services provided are adequately protected against misuse or misappropriation
- Ensure that the security features standardised are compatible with world-wide availability
- Ensure that the security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks
- Ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks (including GSM)
- Ensure that the implementation of 3GPP security features and mechanisms can be extended and enhanced as required by new threats and services

USECA

3G requirements capture

- Based on the threat analysis, a comprehensive list of security requirements were captured and categorised
- The security requirements help identify which security features need to be introduced in order to counteract the threats
- The requirements capture has lead to the identification of additional security features beyond those retained from GSM
**USECA**

**Development of 3G security architecture**

- System assumptions
- Service requirements
- Threat analysis

security requirements

features instances (e.g., confidentiality on the air interface)

security architecture

security features (confidentiality, integrity etc...)

security mechanisms

system architecture

**USECA**

**Summary of 3G R99 security features (beyond GSM)**

- Protection against active attacks on the radio interface
  - New integrity mechanism added to protect critical signalling information on the radio interface
  - Enhanced authentication protocol provides mutual authentication and freshness of cipher/integrity key towards the user
- Enhanced encryption
  - Stronger algorithm, longer key
  - Encryption terminates in the radio network controller rather than the base station
- Core network security
  - Some protection of signalling between network nodes
- Potential for secure global roaming
  - Adoption of 3GPP authentication by TIA TR-45 / 3GPP2
Overview of 3G security architecture

- Network access security (I)
- Network domain security (II)
- User domain security (III)
- Application domain security (IV)
- Visibility and configurability of security (V)

Enhanced authentication protocol for 3G

Differences from the GSM protocol are highlighted in bold
Abbreviations

- K: Subscriber authentication key
- RAND: User challenge
- (X)RES: (Expected) user response
- CK: Encryption key
- IK: Integrity key
- AUTN: Authentication token for network authentication
- SQNms: Sequence number information at user
- SQNhe: Sequence number information at home system
- {RAND, XRES, CK, IK, AUTN}: Security quintet

- UE/USIM: User Equipment / UMTS SIM
- VLR: Visitor Location Register
- HLR/AuC: Home Location Register / Authentication Centre

USECA demonstrator

- Multi-application smart card: GSM SIM + 3G USIM
- Built on G&D SIM card
- File system and card commands in accordance with 3GPP and ISO/IEC standards
- Two authentication and key agreement schemes implemented on the USIM
  - 3GPP protocol (April 99 release)
  - ASPeCT protocol (public key cryptography)
- USIM commands
  - INTERNAL AUTHENTICATE
  - Response: RES or Re-synch fail or Authentication fail
- Management of sequence numbers
  - USIM stores information to allow it to decide whether to accept a sequence number and to perform re-synch
Summary

- 3G security builds on the security of GSM
- Maximises compatibility with GSM
- Corrects real and perceived weaknesses in 2G systems
- Integrity and enhanced authentication added to protect against false base station attacks
- Encryption is enhanced (longer key, stronger algorithm)
- Some protection of signalling between network nodes
- Potential for secure global roaming
- Feasibility of USIM component tested in a demonstrator

Questions and Answers

Peter Howard
Research and Standards Engineer
Communications Security and Advanced Development
Vodafone Limited
peter.howard@vf.vodafone.co.uk