Radio Access Link Security for Universal Mobile Telecommunication Systems (UMTS)

Tomas Flanagan
Tom Coffey
Reiner Dojen
Department of Electronic and Computer Engineering,
University of Limerick, Ireland
Phone: 061-202268 Fax: ++353 61 338176
E-mail: tomas.flanangan|tom.coffey|reiner.dojen@ul.ie

Abstract

The Universal Mobile Telecommunications System (UMTS) security features address known problems with GSM (Global System for Mobile Communications) networks. This paper introduces the UMTS security architecture. The procedure for allocation of a temporary mobile subscriber identity, which is used to provide user confidentiality, is shown. The protocols used to provide network access security are presented and analysed. A discussion of the merits of these protocols concludes the paper.

Keywords: *UMTS, 3G communications, network access security, security architecture, radio access link, authentication and key agreement, local authentication and connection set up.*

1. Introduction

UMTS will replace the Global System for Mobile Communications (GSM) networks and is expected to have 2 billion users worldwide by the year 2010 [1]. In addition to delivery of images, graphics and video communications, UMTS will be used for such applications as banking and e-commerce and hence security is a critical concern.

Data confidentiality and integrity, entity authentication and user confidentiality are the main objectives of UMTS security [2]. Special consideration of network access security is warranted because radio transmitted data is susceptible to fraud and eavesdropping. Network access security encompasses the protocols used to ensure secure communication over the radio link between the mobile station and the serving network; authentication and key agreement (AKA) and connection establishment. A further component of network access security is the use of temporary mobile subscriber identities which provide user confidentiality. The merits of UMTS security are discussed in this paper with emphasis on improvements over the GSM system.

2. UMTS Security Overview

2.0. Improving on Second Generation (2G) Security

UMTS retains useful 2G security features, improves on these features and adds some new features. Among the 2G features being maintained are authentication for subscribers, radio interface encryption, and the operation of security features independent of the user.

Despite these features, security problems exist within GSM. These problems mainly concern design limitations on what is protected rather than defects in the security mechanisms themselves. Only access security is provided allowing clear transmission of cipher keys and authentication data within and between networks. Integrity protection of data is not provided and GSM does not address active attacks, whereby network elements such as base stations, may be impersonated. In addition, there is a lack of confidence in the algorithms [3] used for GSM, as they were not made publicly available and the key length of 64 bits is considered too short. One major motivation for new security features in UMTS is to address GSM weaknesses.

2.1. Security Services in UMTS

Data Confidentiality is the service of information concealment; it ensures that sensitive information is not available to intruders. This can be achieved by encrypting all messages using a secret key known only to authorised entities before they are transmitted.

Data Integrity is the service of keeping information in its original state; it ensures that a false message has not been substituted for a legitimate one, and that a legitimate message cannot be altered. To achieve this, a message authentication function is applied on signalling information elements transmitted between the mobile station (MS) and the serving network (SN).

Entity Authentication is the service of identifying entities. It ensures that an intruder cannot masquerade as a legitimate party. Entity authentication in UMTS includes user and network authentication. To achieve this mutual authentication occurs during the Authentication and Key Agreement using a secret known only to the user and the network.

User confidentiality is the service that the permanent user identity cannot be eavesdropped. This service is implemented using a temporary user identity, which is known by the visited serving network. In addition, any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Local authentication and connection set up allows the user and the network to agree on algorithms and keys to be used for integrity and encryption. This procedure is required before ciphering and integrity protection can begin.

2.2. UMTS Architecture Overview

Entities evolved in UMTS network access security (figure 1) are the Mobile Station (MS), the Radio Network Controller (RNC), the Visited Location Register in the Serving Network (VLR/SN) and the user's Home Environment (HE). Information is transferred between these entities in order to allow security procedures to take place.

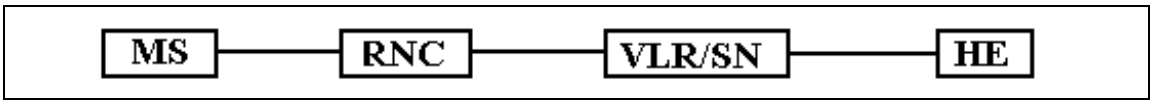

Figure 1: The entities involved in UMTS security

A mobile station consists of the user equipment and the UMTS mobile subscriber identity (USIM). The subscriber information required to carry out network authentication and key agreement is stored on the USIM along with the subscriber identity. The user equipment

(UE) is the hardware which allows the UMTS subscriber to obtain services independent of location, in most cases a mobile phone. The Radio Network Controller (RNC) controls the use and integrity of radio resources. Further, it handles information exchanges between the user and the network. The visited location register in the serving network (VLR/SN) is a database that contains temporary information about subscribers that is needed by the visited SN in order to service visiting subscribers. When a mobile roams into a new SN, the VLR of that SN will request data about the user from the user's HE. This information will be used for authentication and key agreement and call setup. Within one serving network VLRs can exchange such information. The home environment (HE) is responsible for enabling a user to obtain UMTS services in a consistent manner regardless of user location or terminal used. The HE provides authentication and encryption parameters that verify the user's identity and ensure confidentiality [2].

3. Temporary Mobile Subscriber Identity (TMSI)

Traffic analysis is the analysis of encrypted messages. Some potentially useful information can be obtained without knowing the content of such messages; including where they come from, where they go to, how long they are there, when they are sent, how often and more [4]. A TMSI is used to prevent traffic analysis and provide user confidentiality on the radio access link. The procedure used to distribute TMSIs is similar to that used in GSM and is performed after the start of ciphering.

The Visited Location Register, VLR, generates a new temporary identity $TMSI_N$. The association of $TMSI_N$ and the permanent identity, IMSI (international mobile subscriber identity), is stored. It then sends the $TMSI_N$ to the user. The user stores $TMUI_N$ and removes the association with any previously allocated TMSI. Next, the user sends an acknowledgement back to the VLR, after which the VLR removes the association with the old temporary identity ($TMSI_O$) and the IMSI from its database.

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity, it shall maintain the association between $TMSI_O$, $TMSI_N$, and the IMSI. For a user-originated transaction, the network shall allow the user to identify itself by either temporary identity. For a network-originated transaction, the network shall identify the user by its permanent identity (IMSI). Subsequently, in either of the above cases, the network may initiate the normal TMSI reallocation procedure.

Identification of a user on the radio path by means of the permanent identity (IMSI) occurs whenever the user cannot be identified by means of a TMSI. This occurs when the subscriber registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the TMSI by which the user identifies itself on the radio path. The latter may occur when the old VLR is not contactable or when a software error occurs.

This gives rise to situations where it is necessary to send the permanent user identity in cleartext between the communicating parties. Sending the IMSI over the radio interface without encryption represents a breach of user identity confidentiality. However, the number of calls for which the IMSI is used under normal conditions is minimal and is not expected to pose serious security problems for UMTS.

4. Authentication and Key Agreement (AKA) Protocol

A new feature of UTMS is mutual authentication of the user and the network which takes place during AKA as shown in figure 2 (RNC is not included in this figure as it does not

participate in the protocol). Other changes to AKA include the introduction of counters and the generation of an integrity key. Mutual authentication of the user and the network is achieved using a secret key which is known only to the USIM and the user's HE.

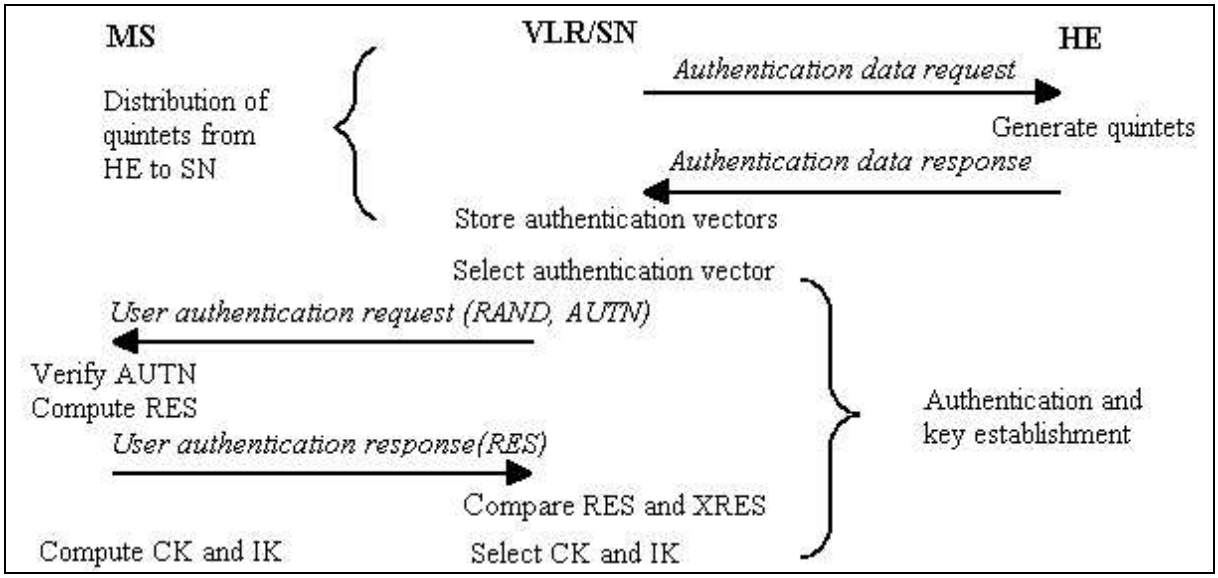

Figure 2: Authentication and key agreement

Upon receipt of a request from the VLR/SN (which includes the user IMSI), the HE/AuC sends an ordered array of n authentication vectors (quintet) to the VLR/SN. Each vector, consisting of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN, enables the VLR/SN to perform one user authentication.

In order to produce the quintet, the HE first generates an unpredictable challenge RAND. This number and the secret key K, shared between the user and the HE, are used to generate XRES, CK, and IK. For each user, the HE keeps track of a counter $SQN_{HE,}$ which is incremented in order to generate a fresh sequence number. $SQN_{HE,}$ RAND and K are used to create AUTN.

The VLR/SN initiates an authentication and key agreement by sending the random challenge RAND and the authentication token AUTN to the user. The USIM evaluates the authentication token AUTN. If the evaluation is successful and AUTN is fresh the network is authenticated. A counter SQN_{MS} is kept in the MS that corresponds to SQN_{HE}. Freshness of AUTN is provided, if SQN_{HE} is within a particular range of SQN_{MS}. If AUTN can be accepted, the USIM calculates a response RES to the challenge RAND. RES is sent back to the VLR/SN. The USIM also computes CK and IK. The VLR/SN compares the received RES with XRES. Agreement of these parameters provides authentication of the user and key agreement exchange is successfully completed.

AKA is not required at every call set up. Authentication in such cases is based on a shared integrity key. Possession of the key provides authentication, as only parties authenticated during the last AKA have knowledge of the integrity key.

4.1 Security of Authentication and Key Agreement Protocol

Mutual authentication has been added to UMTS to prevent false base station attacks. Such a false base station could tell a phone not to use encryption. Calls would then proceed unprotected with the false station relaying information between the real one and the handset [5]. This would allow an intruder to listen to user communications.

Integrity protection is required for UMTS messages to ensure that no modifications to messages or signalling data occur during transit. An integrity key, IK, must be agreed upon between the MS and the network in order to enable integrity protection to take place.

Replay attacks involve recording legitimate messages used for authentication between genuine parties and using them at a later stage, in an attempt to subvert the protocol. Such attacks are detected by comparing the counters SQN_{HE} and SQN_{MS}.

5. Local Authentication and Connection Establishment Protocol

Local authentication and connection establishment in UMTS is different from that used in GSM networks. Firstly, integrity protection has been added. Further, publicly known algorithms and 128 bit key lengths are used for UMTS. The procedure in which the user security capabilities are made known to the network is also changed.

Local authentication and connection establishment (figure 3) describes the information transfer at initial connection establishment that leads to integrity protection. Authentication and ciphering may also occur during connection set up.

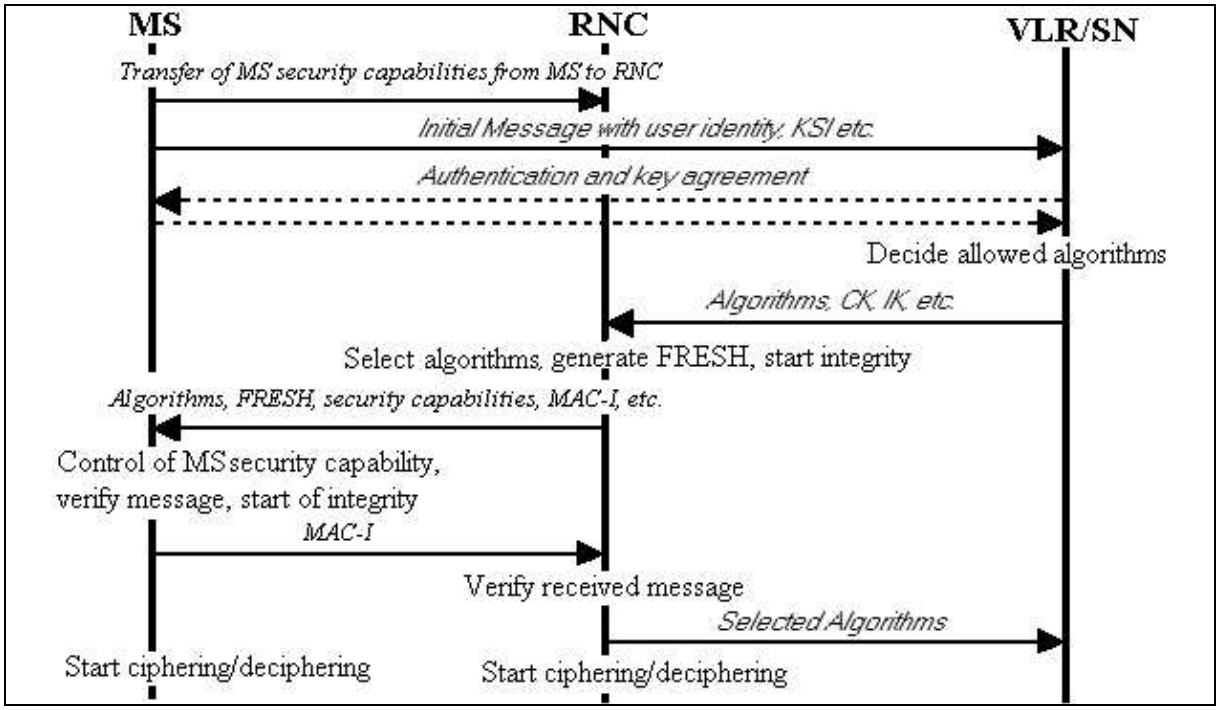

Figure 3: Local Authentication and connection establishment

Connection establishment includes the transfer from user equipment MS to RNC of the user's security capabilities, including the ciphering and integrity algorithms supported by the MS. This information is stored in the RNC. The MS sends an initial message to the RNC. This message contains the KSI (Key Set Identifier) and the user identity. The KSI is associated with the cipher and integrity keys and is available to the MS and the network. Authentication of the user and generation of new security keys may be performed. This step does not occur during every connection set-up. The VLR/SGSN determines which algorithms are allowed. The VLR/SGSN initiates integrity protection and possibly also confidentiality protection by sending a message to RNC. This message contains a list of allowed algorithms to be used.

The RNC uses the first algorithm it supports from the list. Next, the RNC generates a random value, FRESH, and initiates downlink integrity protection. If the RNC supports no algorithms in the list, this is indicated in a message to the network. The procedure is aborted. Otherwise, the RNC sends a message to the MS including the used algorithm, FRESH and the user's security capabilities. This message is integrity protected by the selected algorithm. Upon reception of this message, the MS compares the received user's security capabilities with those sent in the initial message. The MS verifies the integrity of the message. A counter is used to avoid replay attacks. The MS sends a response message to the RNC. Successful integrity protection of the response message authenticates the MS to the RNC. A final message from the RNC to the VLR/SN completes local authentication and connection setup.

5.1 Security of Local Authentication and Connection Establishment Protocol

GSM uses a key length of 64 bits. Although the algorithm used for GSM was originally secret, reverse engineering made the algorithm publicly available. Successful attacks have been carried out against GSM security, which focus on the shortness of the key and weaknesses in the algorithm [6]. In order to overcome such concerns 128 bit keys are used in UMTS. Further, the algorithms used in UMTS are publicly available and hence can be the subject of independent research. This provides higher confidence in the security of the algorithms.

The security capabilities of UMTS users are send to the network from the MS. In GSM the user security capabilities were obtained from the user's home environment. The UMTS method reduces the computational burden on the HE. It also allows call set up to take place in situations where the HE is not available and the amount of signalling is minimised.

6. Conclusions

This paper described the current state of UMTS network access security. It reviewed the use of temporary identities to provide user confidentiality. Protocols for authentication and key agreement and for connection establishment were presented. These merits of these protocols were discussed.

UMTS addresses known security problems in GSM. Mutual authentication has been introduced to UMTS to address false base station attacks and counters are used to deter replay attacks. Greater key lengths, stronger encryption algorithms and the addition of integrity protection ensure that the security level of UMTS is greater than that of GSM. The security features of UMTS provide for data confidentiality and integrity, entity authentication and user confidentiality.

References

[1] What is UMTS, http://www.umts-forum.org, 1999

[2] Security Architecture, 3G TSPP 33.102 version 3.7.0, Release 1999

[3] Walker, M.: On the Security of 3GPP Networks, Eurocrypt, 2000

[4] Schneier, B.: Applied Cryptography, John Wiley & Sons Inc, 1996

[5] Robson, S.: Design flaw in mobile phone protocol, IT week, 2000

[6] Biryukov, A., Shamir, A., Wagner, D.: Real Time Cryptanalysis of the A5/1 on a PC, Fast Software Encryption Workshop 2000