Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing

Vulnerabilities of UMTS Access Domain Security Architecture

Muzammil Khan
College of Telecommunication
NUST Rawalpindi, Pakistan
muzammil_khan@hotmail.com

Attiq Ahmed
College of Telecommunication
NUST Rawalpindi, Pakistan
attiq_ahmed@mcs.edu.pk

Ahmad Raza Cheema
College of Telecommunication
NUST Rawalpindi, Pakistan
ahmed_raza@mcs.edu.pk

Abstract

This paper presents vulnerabilities of UMTS access domain security architecture. The security architecture of UMTS offers some protection against known threats including false base station attacks, man-in-the-middle attacks and replay attacks. The system also successfully ensures user data confidentiality and signaling data integrity. However, a few novel vulnerabilities have been identified in this paper.

It has been shown that modification of unprotected initial messages prior to the security mode command may result in DoS and man-in-the-middle attacks. Non-integrity protection of rrcConnectionReject message can also be exploited to launch DoS attack. Clear transmission of IMSI on some occasions is a violation of user identity/location confidentiality and user traceability. This exposed IMSI can be exploited for new attacks.

1. Introduction

Modern bandwidth hungry applications have set new standards for wireless communication. As a result, mobile communications technology has evolved amazingly during the last decade to meet an exceedingly demanding market. Usage of mobile has gone beyond making calls and checking e-mails. Cell phones are now used for increasingly complex and critical tasks such as accessing patient medical records, closing sales, managing inventories and dispatching service representatives.

Third generation (3G) wireless networks [1] represent the more recent stage in mobile communication evolutionary process. The 3G proposal for cellular communications (Universal Mobile Telecommunication System - UMTS) claims to provide global roaming, high transfer rates and advanced services such as: commerce, global positioning system and multimedia messaging services via audio and video.

UMTS is built on top of the existing Global System for Mobile communications (GSM) infrastructure and integrates both packet and circuit data transmission. The design allows UMTS to be used in parallel with GSM therefore allowing reception in areas where UMTS has not yet been fully implemented. Integration of these two components leads to a smooth transition into UMTS, so GSM is still very important and will continue to run in parallel for some years to come.

The mobile users are now much interested in mobile payment systems, mobile online banking and mobile shopping [2]. When such type of vital data is exposed in the air and is flowing through the network, naturally it attracts hackers to get fraudulent transactions, stolen user accounts, etc. Therefore, security of the network connections and service availability are necessary for user confidence. This paper digs deep into the current security features offered by UMTS and identifies vulnerabilities that can be exploited to launch attacks.

The rest of the paper is organized as follows: Section II explains the existing UMTS security architecture. Section III provides the related work, analyzing the security features of UMTS. Section IV identifies vulnerabilities that can be exploited. Section V concludes the paper while section VI gives some ideas about future work.

2. UMTS Security Architecture

The main objectives and principles of UMTS security are specified in [3]. The emphasis is on protection of user information and user data. Legitimate use of resources and services is ensured by addressing man-in-the-middle and Denial-of-Service (DoS) attacks. Security features are adequately standardized to guarantee world-wide interoperability and roaming between different serving networks. TS 33.102 [4] defines the

978-0-7695-3263-9/08 $25.00 © 2008 IEEE
DOI 10.1109/SNPD.2008.78

architecture of UMTS security which is briefly appended below:

2.1. Switching on the Mobile

When UMTS mobile equipment (ME) is switched on, it scans for available node-Bs and tries to connect with the one having best signal strength. Initially a *Location Update Procedure* is carried out which may be International Mobile Subscriber Identity (IMSI) attach, *Normal Location Update* or *Periodic Location Update* [6]. Location Update starts with Radio Resource Control (RRC) *Connection Request* sent by the ME to Node-B. No dedicated channel is available yet, therefore, this first message is transported through *Common Control Channel* (logical channel) that is mapped on *Random Access Channel* (physical channel) for uplink direction. Along with other attributes *rrcConnectionRequest* message contains IMSI (in clear) and security capabilities of the ME (un-protected) as shown in message 1 of Fig-1.

2.2 Authentication and Key Agreement (AKA)

After *rrcConnectionRequest*, the AKA procedure is carried out. The AKA provides two way authentication, it authenticates the ME and the network simultaneously. The procedure starts with authentication data request by Visitor Location Register/Serving GPRS Support Node (VLR/ SGSN). It forwards IMSI of Universal Subscriber Identity Module (USIM) to Home Location Register/ Authentication Center (HLR/AuC), shown as message 2 in Fig 1.

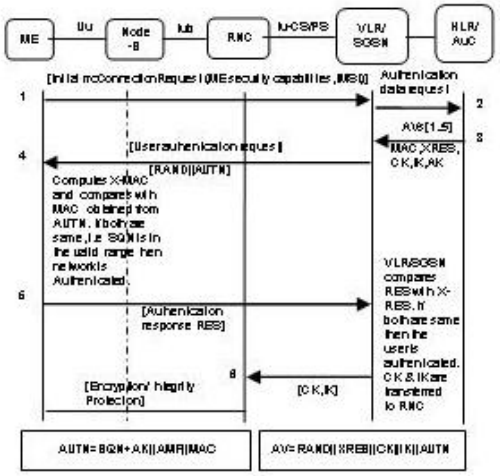


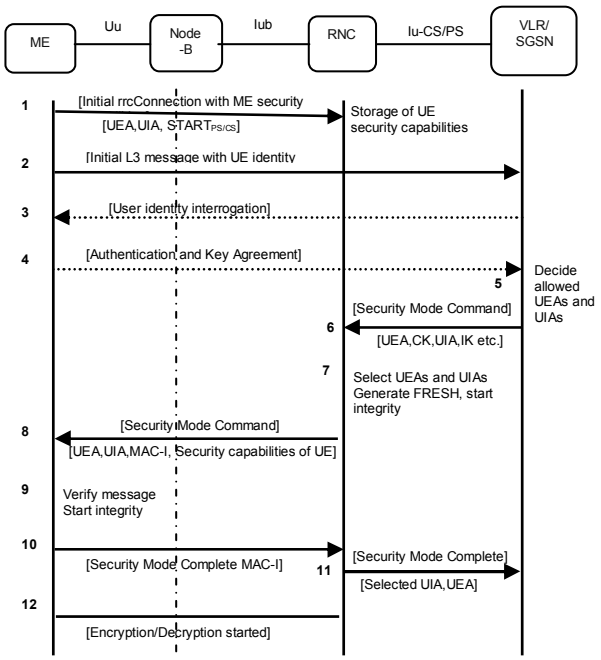
Fig-1 UMTS Authentication and Key Agreement [4]

IMSI and key K are pre-shared between USIM and HLR. On the basis of IMSI, K and Random Number (RAND), five Authentication Vectors (AV) are generated by HLR and forwarded to VLR/SGSN, shown as message 3 of Fig 1. VLR/SGSN selects RAND and Authentication Token (AUTN) corresponding to one AV and forwards it to ME as shown in message 4 of Fig 1. Now ME computes expected message authentication code (X-MAC) and compares it with message authentication code (MAC) obtained from AUTN. If both are same, i.e sequence number (SQN) is in the valid range then the network is authenticated. Now ME calculates response (RES) and forwards it to VLR/SGSN as shown in message 5 of Fig 1. VLR/SGSN compares RES with expected response (X-RES), if both are same then the user is authenticated. VLR/SGSN now transfers Ciphering Key (CK) and Integrity Key (IK) to Radio Network Controller (RNC) as shown in message 6 of Fig 1. Only after this step, both ME and RNC have their respective keys for encryption and integrity protection.

It may be noted that message number 1 to 6 shown in Fig 1 are neither encrypted nor integrity protected because they are transmitted before key agreement. These messages are transmitted through air on Uu interface between ME and Node-B and hence are susceptible to interception, insertion and modification. Their modification by intruder, may cause user specific DoS.

2.3. Security Mode Setup Procedure

Security Mode Command is issued by RNC to start encryption and integrity protection. Complete procedure is depicted in Fig 2. At each new connection this procedure is mandatory for start of integrity protection of signaling data. RNC now has both versions of security capabilities supported by ME and VLR/SGSN. It now selects highest priority common algorithms and forwards them to ME as shown in message 8 of Fig 2. Point worth noting is that this is the first integrity protected message. It contains the security capabilities earlier forwarded by ME in order to thwart the chances of deliberate or accidental modification of initial ME security capabilities. After verifying the MAC-I the acknowledgement is sent back to RNC which finally informs the same to VLR/SGSN. This is shown in messages 10 and 11 of the Fig 2. Now all is set for secure communication between ME and RNC.



Fige-2 UMTS Security Mode Setup Procedure [4]

The confidentiality function f8 is used for provision of data encryption while function f9 is used for integrity protection of signaling data. These functions are used in USIM and RNC. Presently KASUMI algorithm is standardized for use in these algorithms [5,6]. Security function f8, integrity function f9, and the algorithm used in these functions have been analyzed by different researchers and have been found having adequate security [17].

3. Related Work

3.1. Threats to Access Security

The UMTS air interface is easiest to intercept and most difficult to protect. 3GPP has identified following threats to UMTS communication; eavesdropping, impersonation of a user, impersonation of the network, man-in-the-middle attack and compromising authentication vector in the networ*k* [7]. The procedure for an attacker to attack UMTS with these capabilities is also explained.

3.2. Denial of Service (DoS)

DoS attacks on UMTS architecture are difficult to launch as integrity protection of critical signaling messages avoids the DoS attacks using User de-registration request spoofing, Location update request spoofing and Camping on false BS/MS [7]. However, we will show that unprotected messages before security mode command may be utilized for launching DoS attacks.

3.3. Impersonation of the Network

Integrity protection of security mode command provides protection against suppressing the encryption between target user and the intruder. Inclusion of security capabilities of the ME (which were sent during initial *rrcConnectionRequest*) in security mode command by RNC enables the ME to verify that encryption has not been suppressed between target user and the network [4]. However, in combined UMTS/GSM networks, impersonation of network is still possible [8].

3.4. Impact of GSM Attacks on Interoperating GSM/UMTS Networks

As discussed earlier, GSM and UMTS systems coexist for wide area coverage. UMTS supports handover to and from GSM networks. UMTS supports encryption and integrity protection while GSM supports only encryption. It has been shown in [9] that for GSM subscribers a single handover to GSM breaks all pre-handover and post-handover UMTS communication. During intersystem handovers if encryption was disabled before handover, it will stay disabled after handover. It has been explained in [9] that forced handover coupled with man-in-the-middle attack as described in [8] may disable the encryption in pure UMTS networks.

4. Identified Vulnerabilities

4.1 Reveal of Subscriber's Identity

UMTS offers little protection against identity catching. Although IMSI is replaced by TMSIs after the initial connection request, IMSI is sent clear during the first *rrcConnectionRequest* and also on the occasions like VLR database crash, VLR's inability to identify the TMSI.

In a multi service providing system, where the mobile will be used for e-commerce, banking transactions and wireless mobile payments, the confidentiality of identity and location of a user is a necessity. Hence, the above stated occasions are sufficient to attract an attacker to identify the user and even trace him. Particularly, the first connection request message is sent on *Random Access Channel*

which is a common channel and can be intercepted very easily.

There has been a lot of research on GSM for extracting the IMSI during a connection. Presently, GSM based IMSI catcher devices are available in the market but their prices are as high as $500,000 and are only sold to government agencies. Some researchers are interested in building an IMSI catching unit that has all the capabilities of the commercial product [10]. UMTS has been evolved after GSM and has adopted the functionality of sending IMSI in clear at the start of the connection request. Hence the above devices can also be used to obtain the IMSI of a UMTS subscriber. Also some UMTS debugging and Testing Tools like Air Protocol Analyzer AP-6000 and Protocol Tester K1297-G20 have the capability to obtain the IMSI. There are also reports that police can successfully trace suspects through mobile phone by just using the IMSI [11]. Hence the user identity/location confidentiality and user traceability are clearly violated.

A simple scenario of obtaining IMSI of a UMTS subscriber is shown in Fig 3. The attacker impersonates as a UMTS VLR/SGSN. During *rrcConnectionRequest* the victim may use TMSI. If TMSI can not be resolved, then the network can make an identity request. In such a case ME has to send its IMSI in clear. After obtaining the IMSI, the attacker disconnects himself.

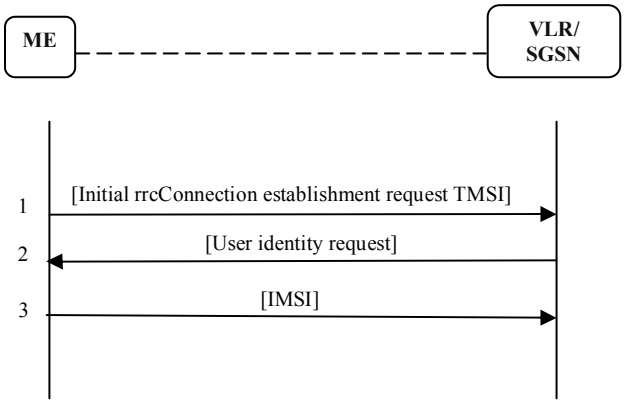


Fig-3 Obtaining IMSI [4]

4.2. User Specific DoS by Modifying Initial Security Capabilities of ME or Authentication Parameters

This attack works in two phases. Initially, the attacker obtains IMSI of the victim as described in section 4.1 above. In the second phase, the attacker waits for this particular user (IMSI) to make a connection request. When an *rrcConnectionRequest* is made by this user, the attacker modifies the message 1 of Fig 2 which contains initial security capabilities of the ME. This message is not integrity protected, therefore, an intruder can modify the ME security capabilities and this change will remain undetected until the security mode command reaches the ME which is shown in message 8 of Fig 2. In case of mismatch of sent and received security capabilities of the ME the connection procedure will terminate. Sufficient time, bandwidth and computing resources have been consumed from message 1 till message 8 including AKA procedure. Such a mechanism capable of changing the initial ME security capabilities may result in DoS to the user.

Modification of any of the authentication parameters including AUTN, RAND, or RES (message 4 or 5 of Fig 1) may also result in DoS. These messages are neither encrypted nor integrity protected. Any change in the way will result in non-authentication of network and/or user. In both the cases the network will not be able to distinguish between illegitimate user and DoS attack.

4.3. DoS using rrcConnectionReject Message

This is a user specific attack. Again in the first phase the attacker obtains IMSI of the victim. Now attacker waits for *rrcConnectionRequest* by this user. Initial UE identity is the unique identifier of this message. Initial UE identity may be Temporary Mobile Subscriber Identity (TMSI), Packet Temporary Mobile Subscriber Identity (P-TMSI), IMSI or International Mobile Equipment Identity (IMEI). Usually the first *rrcConnectionRequest* message contains IMSI of the user. The attacker will respond with *rrcConnectionReject* message. We know that *rrcConnectionReject* message is not integrity protected [12]. The only way to assess its genuineness is the comparison of the value of the "Initial UE identity" in the received *rrcConnectionReject* message with the value of the variable "INITIAL_UE_IDENTITY" already available with UE. If the values are different, the UE shall ignore the rest of the message. If the values are identical, the UE shall terminate the connection [13]. Hence an intruder knowing IMSI of the victim can easily generate a genuine *rrcConnectionReject* message and cause DoS to the user.

4.4. DoS by Flooding the HLR/AuC

This is a much dangerous attack. It is a mobile operator specific attack. Using this attack, services of

a particular mobile operator can be blocked. The attack may be launched in two phases:

Phase I: In this phase the attacker builds a database of IMSIs corresponding to the victim operator. The attacker can easily obtain IMSIs using the procedure mentioned in section 4.1 above. The attacker can identify the operator from IMSI as digits 4 and 5 (or 4, 5 and 6) represent the operator, within the IMSI structure [14].

Phase II: In this phase the attacker quickly generates *rrcConnectionRequests* corresponding to each IMSI using an automatic procedure. For each request, (except already connected one) VLR/SGSN sends the IMSIs to the HLR/AuC (message 2 Fig 1). HLR/AuC checks the validity of IMSIs. Since attacker has obtained all valid IMSIs in phase I, therefore, all the IMSIs pass this validity test. Now HLR computes 5 AVs corresponding to each IMSI. This is a cumbersome process of calculating RAND, MAC, XRES, CK, IK, AK for each IMSI. The AVs corresponding to each IMSI are then sent to VLR/SGSN (message 3 Fig 1). For each IMSI, VLR/SGSN selects one AV and sends the RAND and AUTN for authentication [4]. It is the stage where the attacker will not be authenticated, as it cannot calculate RES without knowledge of secret key of the USIM. But this is not the desire of the attacker, actually he has already done the job. His goal is to exhaust the computing resources of HLR/AuC by flooding more and more valid *rrcConnectionRequests* and making it to compute AVs. This may also cause bandwidth exhaustion between VLR/SGSN and HLR/AuC. This exhaustion of resources will result in DoS to new users who are attempting to connect.

4.5. Impersonation of the Network

An intruder can fool the pure UMTS networks as well. The attack scenario is as follows: The attacker impersonates as a valid GSM BS to the UMTS user and to the network. Now UMTS mobile having capability to connect to both UMTS and GSM systems will send security capabilities. These capabilities can be modified by the intruder, since the message is not integrity protected. Upon reception of security capabilities UMTS AKA procedure will be carried out between ME, VLR/SGSN and HLR/AuC. The impersonated GSM BS will simply forward these messages. GSM cipher key Kc is derived from the UMTS cipher/integrity keys and sent to impersonated GSM BS [4]. Now the network will issue the security mode command according to GSM BS. This command does not include the security capabilities earlier forwarded by ME. The ME will accept this command by considering that it is connected to a GSM BS. In this way the attacker can succeed in getting the encryption algorithms of his choice. It has been mentioned in [15, 16] that GSM encryption algorithms A5/1 and A5/2 can be compromised.

4.6. Integrity Protection of User Data

Cryptographic integrity protection in UMTS is implemented in only a limited part of the system. Only signaling data is protected and the protection is limited to transmission between the SRNC and UE. User data is not integrity protected. Presently, it is assumed that if the data is successfully decrypted then it has not been changed in the way. The above assumption might be valid for speech and written prose. For user data with high uncertainty of outcome, e.g. figures in a bank transaction, the low-grade integrity protection implicitly offered by encryption/ decryption is not satisfactory.

5. Conclusion

The architecture of UMTS access security including AKA procedure, security mode set-up procedure, security function f8, integrity function f9, and the algorithm used in these functions have adequate security. Some protocol flaws have been identified and presented in this paper, which may result in DoS attacks, compromise the integrity of signaling messages, man-in-the-middle attacks, bidding down attacks and revealing of user identity/location and its traceability. Unprotected initial UE security capabilities, unprotected transmission of AUTN, RAND and RES during AKA and unprotected *rrcConnectionReject* message may cause DoS attacks. Clear transmission of IMSI during first connection, coupled with non integrity protection of messages before security mode command can cause operator specific DoS attacks. User data is not integrity protected thus posing serious threats against vital data transfers like bank transactions etc. In order to gain complete user trust, the above mentioned vulnerabilities should be addressed.

6. Future Work

Following are some suggested areas for work on UMTS security. A mechanism should be implemented for protection of all messages before security mode command. IMSI of the user should never be transmitted in clear. It may be hashed with some sequence number in order to avoid clear transmission and replay of hash value. *rrcConnectionReject* message should also be integrity

protected. A mechanism may be developed for integrity protection of user data, in order to gain user trust and confidence.

7. References

[1] http://www.3gpp.org. Dec. 2007.

[2] Deutsche Bank Research. E-Banking Snapshot http://www.dbresearch.com Dec. 2007.

[3] 3GPP TS 33.120 (4.0.0), "3G Security; Security Principles and objectives", *Release 4*, March, 2001.

[4] 3GPP TS 33.102 (7.1.0), "3G Security; Security Architecture", *Release 7*, December, 2006.

[5] 3GPP TS 35.201 (7.0.0), "3G Security; Specification of 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification", *Release 7*, June, 2007.

[6] 3GPP TS 35.202 (7.0.0), "3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification", *Release 7*, June, 2007.

[7] 3GPP TR 33.900 (1.2.0), "A Guide to 3G Security" January, 2000.

[8] U. Meyer, S. Wetyel, "A Man-in-the-Middle Attack on UMTS", *Proc. of 5th International Conference on Web Information System Engineering,* Brisbane, 2004.

[9] U. Meyer, S. Wetyel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperation GSM/UMTS networks" *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004*. Published: 2004, Page(s): 2876 - 2883 Vol.4

[10] http://www.binrev.com/forums/index.php?showtopic=28559

[11]http://news.bbc.co.uk/2/hi/technology/4738219.stm. Jan. 2008.

[12] R. Kreher, T.Rudebusch, UMTS Signaling, Wiley 2005.

[13] 3GPP TS 25.331 (8.0.0), "Radio Resource Control protocol for the UE-UTRAN radio interface", *Release 8*, September, 2007.

[14] 3GPP TS 33.120 (7.5.0), "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification" ", *Release7*, September, 2007

[15] P. Ekdahl and T. Johansson, "Another attack on A5/1", *Transactions on Information Theory*, vol. 49, pp. 84-289, 2003.

[16] E. Barkan, E. Biham and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication", in *Advances in Cryptography* – CRYPTO 2003, vol. 2729 of LNCS, pp. 600-616, August 2003.

[17] Abdul Bais, Walter T. Penzhorn, Peter Palensky, "Evaluation of UMTS security architecture and services" *in proceedings of IEEE International Conference on industrial informatics 2006*, pages 570-575.