EVALUATION OF SECURITY ATTACKS ON UMTS AUTHENTICATION MECHANISM

Mojtaba Ayoubi Mobarhan, Mostafa Ayoubi Mobarhan

and Asadollah Shahbahrami

Department of Computer Engineering, Faculty of Engineering,
University of Guilan, Rasht, Iran
E-mail: Mojtaba.ayoubi@gmail.com, Mostafa.ayoubi7@yahoo.com,
shahbahrami@guilan.ac.ir

ABSTRACT

In this study security of internet access over the Third Generation (3G) telecommunication systems is considered and Universal Mobile Telecommunications System (UMTS) is selected as the most popular system among 3G systems. The study then focuses on network access security mechanism of UMTS, called Authentication and Key Agreement (AKA). In addition, twenty types of important attacks and threats in UMTS system are presented and classified based on three major security factors; authentication, confidentiality, and data integrity. The evaluations finally show that the authentication factor is more interesting than other factors for hackers. Then, we describe four attacks named; man-in-the-middle, denial of service, identity catching, and redirection as the most significant attacks against authentication mechanism. Furthermore, we provide some solutions and methods to improve AKA mechanism and prevent these attacks in UMTS system.

KEYWORDS

GSM System, Telecommunications System, UMTS Security, Denial of Service Attack, Authentication and Key Agreement.

1. INTRODUCTION

The Third Generation (3G) plan for cellular communications enables to provide global roaming, high transfer rates and modern value added services such as internet access, e/m-commerce, Global Positioning System (GPS), mobile payment and Multimedia Messaging Services (MMS) using audio and video. The Universal Mobile Telecommunications System (UMTS) is one of the famous 3G mobile cellular communication systems being developed within the structure designed and introduced by the International Telecommunication Union (ITU) and known as IMT-2000. It builds on the ability of today’s mobile technologies by providing increased capacity, data ability and a greater domain of services using a radio interface standard called UMTS Terrestrial Radio Access (UTRA). The structure and characteristics of UMTS like basic radio, network and essential service parameters, were organized and defined by the European Telecommunications Standards Institute (ETSI) in early 1998. The UMTS system is built on top of the well-known and existing Global System for Mobile communications (GSM) infrastructure and combines both packet and circuit data broadcast. Hence, the design concurrently allows UMTS to be used in parallel with GSM [1, 2].

Recently, the mobile users are much interested in finance services by their mobile equipment. These services include mobile payment, mobile banking and mobile shopping. When such type of sensitive data is transferred in the air, it attracts hackers and attacker to get fraudulent

DOI : 10.5121/ijnsa.2012.4403

transactions, stolen user accounts, and so on. Hence, the security of the network connections is necessary for user trust. Unfortunately, First Generation (1G) mobile systems provided mainly no security quality. After that, the Second Generation (2G) mobile system (for instance GSM) was designed and presented such that it provides security similar to that of eavesdropping in fixed phones, and to protect against cloning of mobile identities. The GSM allows its network operator to verify the identity of a user such that it is fundamentally impossible for attacker to masquerade as a valid user [3].

UMTS security is built on the success of GSM by retaining its strong security features and advantages. Although GSM security has been very successful compared to 1G, one of the purposes of the UMTS security design was to address its original and noticed GSM weaknesses. The following are some of these weaknesses and threats [4, 5, 6].

- Active attacks utilizing a "false base station".
- Unidirectional Authentication and Key Agreement (AKA) protocol.
- Possibility of replay attacks.
- Cipher keys and authentication data are transmitted in clear between and within networks.
- Encryption does not extend far adequate towards the core network and data is transmitted in clear on the microwave links.
- Weak cryptographic (at present lots of successful attacks have been published on A5/1 and especially A5/2) and short cipher key size (64 bit).
- Data integrity as one of the most significant security factors in radio interface is not provided.
- User authentication on a previously generated cipher key and channel hijack depends on the use of encryption.
- 2G systems do not have the flexibility to upgrade and enhance security functionality over time.

Therefore, 3G defined the UMTS system to improve security of communication systems. It provides a high level of security in comparison with GSM. It also prepares significant improvements to overcome the vulnerabilities in the 1G and 2G systems. These improvements include mutual authentication, freshness and liveliness assurance of AKA, sufficient and suitable Integrity Key (IK) and Cipher Key (CK) sizes (128 bits) and data integrity of signalling messages in radio interface. The following are the major aims of carrying out this work.

1. The most important security mechanisms of the UMTS system are presented.
2. Most efficient attacks on UMTS system are studied and analyzed.
3. UMTS attacks are classified based on three major factors and demonstrate authentication is more attractive than others for attacker.
4. Some solutions and methods are presented to improve AKA mechanism in UMTS system.

The rest of the paper is organized as follows. Section 2 reviews the existing UMTS security architecture. In section 3, we focus on network access security mechanism in UMTS. Section 4 identifies two types of confidentiality services. In section 5, we explain data integrity in UMTS system. Then, KASUM algorithm is mentioned in section 6. In section 7, we evaluate security of keys in UMTS system. Section 8 studies some threats and attacks on UMTS and describes four important of them. Some solutions to improve UMTS AKA are depicted in section 9, and conclusions are presented in section 10.

2. THE UMTS SECURITY ARCHITECTURE

The UMTS security architecture defines five separate security domains, intended to meet specific threats and to establish definite security mechanisms:

1) **Network access security:** In this domain some issues like; mutual authentication, confidentiality of user identity and transferred data, integrity protection of important data, are discussed.

2) **Network domain security:** enables different nodes in the network domain to securely exchange data, and protects against attackers on the wire line network.

3) **User domain security:** ensures only authorized access to Universal Subscriber Identity Module (USIM).

4) **Application domain security:** enables applications in the user and provider domains to sensitive exchange messages.

5) **Visibility and configurability of security:** notifies the user whether a security feature is in action and if the use and provision of services should depend on the security important.

As we said before, the UMTS security has five domains. But we focus our efforts on network access security because this is the most vulnerable and important part in UMTS architecture. The other domains use well established security protocols such as IPsec [5].

3. AUTHENTICATION AND KEY AGREEMENT

The network access security mechanism, called AKA, is based on a secret key, K, distributed between the Home Network (HN) and the USIM. The design of AKA protocol for UMTS reflects the results of an analysis of the threats and risks in GSM system as we mentioned in section 1. The main alterations with respect to the GSM authentication and key agreement protocol are [1]:

- The first challenge is protected against replay attacks by a Sequence Number (SQN) and it is also ‘signed’. This means that authentication data intercepted by a hacker cannot be reused.

- The AKA generates an IK in addition to a CK. This key is used to protect the integrity of the signalling data between the Mobile Station (MS) and the Radio Network Controller (RNC).

The UMTS AKA is selected in such a way as to achieve maximum compatibility with the current GSM security architecture [6]. UMTS AKA is a one-pass challenge response protocol. The UMTS authentication mechanism has been studied [7, 8, 9, 10, 11], resulting in suggestions for some improvements. The AKA mechanism executes mutual authentication of the user and the network using a symmetric key, K and derives the new cipher and integrity keys. There are three important parts included in this process:

1) The home environment of the user (Home Location Register/Authentication Centre (HLR/AuC)), that uses the secret key, K, to create the Authentication Vectors (AV).

2) The service network (Serving GPRS Support Node/Visitors Location Register (SGSN/VLR)), where the users are stationed, that receives and employs these AV to authenticate.

3) The User Equipment (UE) that uses its secret key, for authentication and security establishment with the network.

3.1. International Mobile Subscriber Identity

A fundamental entity authentication is that the entities have well defined unique identities. The primary user identity is the International Mobile Subscriber Identity (IMSI) number. It is not the well-known subscriber number (called MSISDN number). The MSISDN number (or numbers) is a telephone number with full international prefix and is associated with the IMSI number in the valid databases. The MSISDN numbers are (generally) public information, while the IMSI number is designed for system internal identification and routing intentions [10, 12].

3.2. Temporary Mobile Station Identity

Identity presentation must precede identity verification (authentication), since it is the authentication procedure that generates the session keys used for encryption. We have a situation where the permanent identity (IMSI) will be visible on the air interface. This is unsecured since it allows for subscriber location tracking. To solve the problem the Serving Network (SN) may issue a local temporary identity called the Temporary Mobile Station Identity (TMSI) to be used for subsequent identification [12]. The normal procedure is therefore that the UE presents itself with its IMSI the first time. It enters a new service area (SGSN or VLR). Thereafter encryption has commenced, the SN sends a TMSI number to the UE. This identity is called the International Mobile station Equipment Identity (IMEI) and is a unique identity. The IMEI number will regularly be checked against a database called the Equipment Identity Register (EIR).

3.3. Authentication and Key Agreement Procedure

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 IMSI attach, Normal Location Update (NLU) or Periodic Location Update (PLU). Location update starts with Radio Resource Control (RRC) connection request sent by the ME to BS. No dedicated channel is available yet; therefore, this first message is transported through common control channel that is mapped on random access channel for uplink direction. After this step, the AKA procedure is performed. As we said previously, the AKA provides two way authentication. It authenticates the ME and the SN simultaneously. This procedure starts with authentication data request by VLR/SGSN. It forwards IMSI of USIM to HLR/AuC. This request is shown as message 1 in Figure 1. The IMSI and key, K are shared between USIM and HLR. On the basis of IMSI, K and Random Number (RAND), five AV are produced by HLR and forwarded to VLR/SGSN, shown as message 2 in Figure 1. The VLR/SGSN selects RAND and Authentication Token (AUTN) corresponding to one AV and forwards it to ME as shown in message 3. Now the ME computes expected Message Authentication Code (X-MAC) and compares it with MAC obtained from AUTN. If both are same and SQN is in the valid range then the network is authenticated. A consequence of having mutual authentication is that the USIM is now an active entity. In UMTS, the USIM attempts to authenticate the network and it is now possible that the USIM will reject the network. But in GSM, the user could not authenticate the network. Hence, the UE could not reject the network. Now ME calculate response (called RES) and transmit it to VLR/SGSN as shown in message 4 (Figure 1). VLR/SGSN compares RES with expected response (X-RES). If both are same then the user is authenticated.

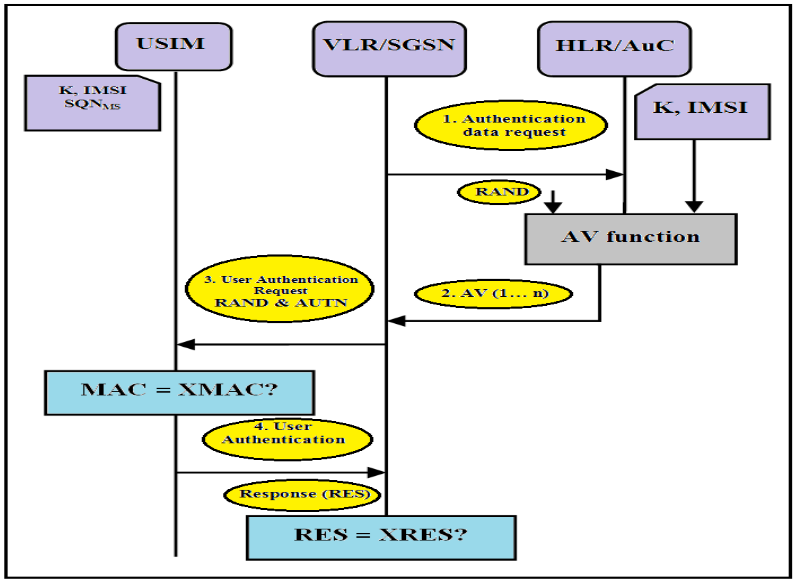

Figure 1. UMTS authentication and key agreement

The VLR/SGSN now transfers CK and IK to RNC. After this step, both RNC and the ME have their respective keys for encryption and integrity protection. The message numbers 1 to 4 (shown in Figure 1) are neither encrypted nor integrity protected because they are transported before key agreement. These messages are transmitted through air on interface between ME and BS and hence are susceptible to interception and modification. Their modification by intruder may cause specific attack such as Denial of Service (DoS) and Man-In-the-Middle (MiM) [2].

3.4. Authentication Vectors

The AVs contain sensitive and important data like challenge-response authentication data and cryptographic keys. It is therefore clear that the transfer of AVs between the HLR/AuC and the SGSN/VLR requires to be secured against eavesdropping and modification attacks. The actual transfer mechanism for the AVs is the SS7-based Mobile Application Part (MAP) protocol. The MAP protocol principally includes no security functionality, but a security extension to MAP called MAPSec [12] has been developed by the 3G Partnership Project (3GPP). The MAPSec protocol belongs to the Network Domain Security (NDS) work area in UMTS security architecture as we mentioned in section 2. It includes both the MAPSec specification and specifications for how to protect internet protocol connections on the control plane of the UMTS core network. The AV has five components generated using five security functions (f1, f2, f3, f4 and f5), as shown in Figure 2.

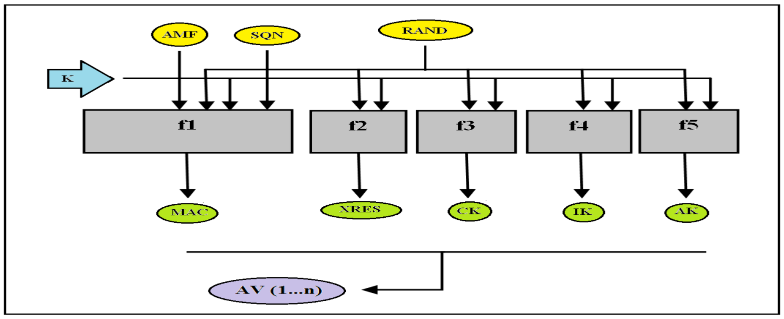

Figure 2. AV functions

Table 1. Components of AV

	Description
RAND	Random value.
SQN	Sequence number, masked with the key AK.
AMF	Authentication Management Field is a 16 bit field used for management purposes.
MAC	Message Authentication Code that is verified by the user.
XRES	The response that the service network expects to receive from the user.
CK	Confidentiality Key.
IK	Integrity Key.
AUTN	Authentication token, verified by the user to authenticate the network.

3.5. Secret Key in AKA Mechanism

The authentication sequence performed between the SGSN/VLR and the USIM is based on a mutual authentication scheme using a long-term pre-shared secret key, K (128-bit). This master key, K is only stored on the Universal Integrated Circuit Card (UICC) or USIM and in the AuC. The UICC is a tamper-resistant smartcard subscriber identity module, and the USIM is an application running on the UICC. For security to be maintained, it is an essential requirement that K is never disclosed or otherwise compromised for the given UICC/USIM during its lifetime. The AKA sequence is normally initiated by the VLR/SGSN when the network needs to verify the identity of the subscriber. If the SGSN/ VLR do not already possess a valid AV (Figure 1) for the claimed subscriber identity, it must request at least one AV from the HLR/AuC. The AV is computed by and stored at the AuC. The AV is generated by means of the operator-specific authentication functions.

4. CONFIDENTIALITY

The confidentiality mechanism is realized by means of encryption in many systems and services. The cryptographic keys such as CK and IK to be used are generated by the AKA procedure. The CK is always 128 bits long, but one can control the number of significant bits by configuring the key derivation f3 function (showed in Figure 2). The default produced by MILENAGE f3 is for a confidentiality key of 128 significant bits. We can classify confidentiality in two different types; user identity confidentiality and data confidentiality.

4.1. User Identity Confidentiality

The main objectives of user identity confidentiality feature are to prevent intruders from some attacks like eavesdropping the IMSI. To achieve this purpose the user is identified by means of a TMSI on the radio interface which has local importance and is combined with Location Area Identifier (LAI) or Routing Area Identifier (RAI), for the circuit switched and packet switched domain respectively. Whenever a UE tries to access 3G services, it identifies itself by means of the TMSI/LAI or TMSI/RAI [3].

4.2. Data Confidentiality

In the UMTS Security, user data and some information elements are considered sensitive and may be confidentiality protected. The need for a protected mode of transmission is fulfilled by a confidentiality f8 function. This encryption function is applied on dedicated channels between the ME and the RNC. In current specifications the f8 function is based on KASUMI algorithm.

4.3. Confidentiality Function

The UMTS encryption f8 function is a link layer symmetric synchronous stream cipher. This function is designated to generate a pseudo-random key stream block that is combined with a plaintext block by means of bitwise modulo 2 operations (XOR function). The function takes a 128 bit key CK, but operates mentally on 64 bit blocks. This confidentiality function (Figure 3) takes as input the confidentiality key (CK, 128 bit), a sequence number (COUNT-C, 32 bit), the radio channel indication (BEARER, 5 bit) and a direction indication (DIRECTION, 1 bit). Additionally, the length (LENGTH, 16 bit) of the key stream block is provided.

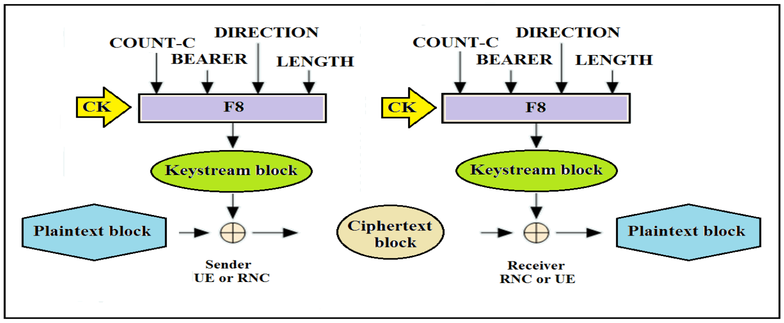

Figure 3. f8 Function

5. DATA INTEGRITY

As discussed in section 3.3 the integrity protection of signalling messages, between ME and RNC starts as soon as the integrity key and integrity protection algorithm is known. The IK is always 128 bits long, but similar to CK, one can also configure IK to have fewer significant bits if required. The default MILENAGE f4 function produces an IK with 128 significant bits (Figure 2). A MAC function is applied to each special message at the RRC layer of UMTS Terrestrial Radio Access Network (UTRAN) protocol stack. Integrity protection of critical messages provides protection against many active threats and attacks such as an MiM. Partial integrity protection of user data UMTS also has a mechanism which prevents the insertion or deletion, but not the modification, of user data. This characterize is meant to prevent certain bandwidth hijacking attacks while avoiding the cost of full-blown integrity protection mechanisms for user data [1, 3]. The integrity security service is comprehended by means of a MAC mechanism that provides both message authentication and integrity protection against intentional modifications.

5.1. Data Integrity Function

UMTS data Integrity is restrict to insuring messages between the MS and the RNC. The integrity function, f9 (Figure 4) takes as input the integrity key (IK, 128 bit), the message (MESSAGE) to be protected, a sequence number (COUNT-I, 32 bit), a random value (FRESH, 32 bit), and a direction indication (DIRECTION, 1 bit) value. The computed MAC-1 is comprised in the signalling message by the sending side. The receiving side calculates the corresponding XMAC-1 over the message, and data integrity is considered to be confirmed if the calculated XMAC-1 and the received MAC-1 are identical.

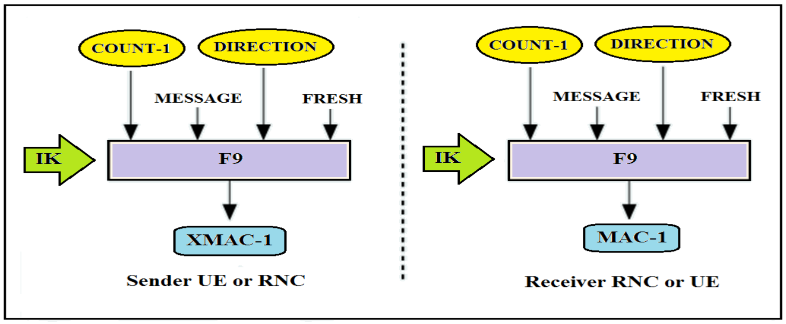

Figure 4. f9 Function

In UMTS system, signalling messages are generally short; hence, the lengths of the MESSAGE main components are correspondingly short. The actual length of the MESSAGE element presented to the f9 function is longer than the message sent over the air since the five bits utilized to indicate the bearer channel are extracted from the radio bearer context. The specifications arbitrarily limit the size of an f9 input message to 5000 bits. The standard f9 function is based on the KASUMI block cipher (like f8). This function is a variant of the familiar Cipher-Block-Chaining Message Authentication Code construction (CBC-MAC) technique. Had an ordinary CBC-MAC mode been used for KASUMI, it would have been restricted by the block size of 64 bits, but a strange chaining technique has allowed the f9 function to support a 128 bit internal situation. The final output from the KASUMI used in f9 is a 64-bit cipher block, which is truncated to become the 32-bit MAC value [12]. Figure 4 illustrates the use of integrity algorithm f9 to authenticate the data integrity of an RRC signalling message [3, 4].

6. KASUMI ALGORITHM

As we said in section 4 and 5, the confidentiality function, f8 is used for provision of data encryption while f9 function is used for integrity protection of signalling data. These functions are used in USIM and RNC. Presently KASUMI algorithm is standardized for use in these algorithms. The f8 function (confidentiality), function f9 (integrity), and the algorithm used in these functions have been analyzed by different researchers and have been found having sufficient and suitable security [2]. The block cipher KASUMI is a modification of MISTY1. KASUMI is a Feistel cipher with eight rounds. It operates on a 64 bit data block under control by a 128 bit key. The security architecture of UMTS allows for 16 different encryption algorithms and 16 different integrity algorithms specified through the UMTS Encryption Algorithm (UEA) and UMTS Integrity Algorithm (UIA) identifier [3, 12].

7. SECURITY OF KEYS IN UMTS

As indicated previously, the UMTS security uses three keys, K (the secret key shared between the HN and the USIM and used during the AKA procedure), CK (confidentiality key), and IK (data integrity key). These three keys are exposed on the radio link in a similar manner against cryptographic attacks. If the hacker wants to retrieve CK or IK, he must use the data sent between the UE and the SN in order to attack the functions (f8 or f9). In this occasion, the attacker has access only to the protected data; hence hacker can only mount cipher-text only attacks [24]. In another scenario, if the attacker wants to break K, he will intercept the messages that are exchanged during the AKA procedure and will use them to mount attacks against the security functions f1, f2, f3, f4 and f5. The significant values that the attacker can intercept are AMF, MAC, RES and RAND (Table 1). Hence, when the attacker tries to retrieve K, the attacker can mount both cipher-texts only and known plaintext attacks. In previous case, attacker tries to retrieve CK or IK, he has more text that he can use, but can mount only cipher-text only attacks. Therefore, we can conclude the similarity of the exposure to attacks is in contrast to the enormous difference of the importance of a successful attack if CK or IK are broken only a limited amount of data is compromised, whereas if K is broken the entire security of past and future communications is compromised. So K is more interesting and attractive than CK and IK for attackers and hackers. Hence, protection of this key is so important for both UE and SN. Some mechanisms and procedures are proposed to enhance the security of the secret key. Three methods were previously presented an enhanced identification procedure that allows the establishment of a Temporary Key (TK), the encryption of the authentication messages that will protect them from attacks and the increase of the size of the secret key, K.

In first measure, we can use a protocol that has already been proposed and we can enhance it order to assure adequate protection for the master key. This protocol is the Enhancement Mobile Security and User Confidentiality for UMTS (EMSUCU) that was proposed for the protection of IMSI [26, 27]. As we said before, the UMTS system limits the usage of the IMSI identity as much as possible. Whenever possible a temporary identity, the TMSI, is used. Furthermore, the TMSI is sent encrypted over the radio link. Correspondingly, we propose that the AV be generated using a TK, instead of the K. For the establishment of the secret key TK we propose adapting the EMSUCU protocol. A new TK will be generated each time the Enhanced EMSUCU protocol is performed [5]. As we discussed in section 3, in the UMTS security standard when the cryptoperiod of the keys pair CK, IK has expired the ME will delete their value. Subsequently, a new AKA procedure will be initiated in order to produce a new pair of keys CK and IK. Other proposition is very easy and suitable: when the cryptoperiod of CK and IK expires, the ME initiates the AKA procedure before deleting the keys pair CK and IK. In this case, these keys will be used to protect the messages that are exchanged during the AKA procedure. It will be very simple to implement this method, because it involves only a minor change in the order of events of the UMTS security protocols. As with all other messages, the encryption will be performed by the ME at the user side and by the RNC at the network side using the same security algorithms. Although the encryption of the AKA messages are efficient and easy to implement, it has a drawback it needs a set of valid secret keys CK and IK. So, there will be cases when it will not be possible to use it to protect the AKA messages, e.g. when the user turns his UE on. Besides the above mentioned measures we also propose to increase the size of the secret key K from 128 bits to at least 256. Due to the importance of the secret key K, we advise a minimal length of 256 bits.

8. THREATS AND ATTACKS ON UMTS

On one hand, it is easy to intercept into the UMTS system because its interface is air. On the other hand, the UMTS system protection is difficult. The 3GPP has identified different threats into the UMTS system. Some of them are as follows, DoS, impersonation of a user, and impersonation of the network, MiM attack, and identity catching. In a multi service providing system, where the mobile is used for e-commerce, banking transactions and wireless mobile payments, the authentication, confidentiality and data identity of a user is a necessity. Hence, the above attacks are sufficient to attract an attacker to identify the user and even trace him. Table 1 depicts these attacks. They are studied and categorized based on three security factors namely, authentication, confidentiality, and data integrity.

A: Authentication C: Confidentiality D I: Data Integrity

Table 2: UMTS Security Attacks

UMTS Attacks	*A*	*C*	*D I*	*Risk*
1. Replay Attack [2, 13, 16, 23]	Yes	No	No	Low
2. Man-In-the-Middle (MiM) Attack [2, 3, 8, 13, 14, 15, 16]	Yes	Yes	Yes	High
3. Brute Force Attack [8]	Yes	No	Yes	Medium
4. Eavesdropping Attack [2, 3, 4, 13, 15]	No	Yes	No	Low
5. Impersonation of The User Attack [2, 3, 4, 22]	Yes	No	No	Low
6. Dictionary Attack [8]	Yes	No	No	Low
7. Impersonation of The Network Attack [2, 3, 22]	Yes	No	No	Low
8. Compromising AV In The Network Attack [2, 3, 10]	Yes	No	No	Low
9. Denial of Service (DoS) Attack [2, 3, 8, 18, 22]	Yes	Yes	Yes	High
10. Identity Catching Attack [3, 20, 21]	Yes	Yes	Yes	High
11. Redirection Attack [13, 14]	Yes	Yes	Yes	High
12. Sequence Number Depletion Attack [13]	Yes	No	No	Low
13. Roaming Attack[13]	Yes	Yes	Yes	High
14. Bidding Down Attack [19]	No	Yes	Yes	Medium
15. Guessing Attack [23]	Yes	Yes	No	Medium
16. Substitution Attack [23]	Yes	Yes	Yes	High
17. Disclosure Of User Identity(IMSI) Attack [16]	Yes	No	No	Low
18. Packets Injection Attack [8]	No	No	Yes	Low
19. Content Modification Attack [8]	No	No	Yes	Low
20. Secret Key Exposure Attack [21]	Yes	Yes	Yes	High

As this Table shows, some attacks threaten on one factor and some of them carry out on two or three factors. Hence, the attacks are classified into three risk level, Low, Medium, and High. In this section, we have selected four attacks with high level of risk in Table 2. These attacks can exploit a weakness of the system and focus on AKA mechanism. We will try to give a brief explanation of each one. They can be noted in their referenced articles with their details.

8.1. Man-In-the-Middle Attack

An ability of the intruder to put himself between two communicating parties, a user (MS) and the network, enabling him for various actions including eavesdropping, modifying, deleting, reordering, replaying, and spoof signalling or user data. A MiM attacks are one of the most popular and challenging threats in communication systems (such as GSM, GPRS and especially UMTS) and there is a large body of research dedicated to the detection and analysis of different forms of these attacks [13, 14, 15, 16, 17]. A MiM attack is defined as an attack in which the intruder is able to read and write messages communicated between two parties of network without either party being conscious of this fact.

8.2. Denial of Service Attack

The DoS attacks on UMTS systems are difficult to launch as integrity protection of critical signalling messages avoids the DoS attacks using User de-registration request spoofing, location update request spoofing and Camping on false BS/MS. We show that unprotected messages before security mode command may be used for launching DoS attacks [8, 18, 22].The following will result in complete or partial DoS to the target user.

1) **User de-registration request spoofing:** If the network side cannot authenticate messages, then an attacker (with a modified MS) can send a de-registration request to the network, which is compiled by the network and simultaneously sends instructions data to the HLR to do the same. Thus Integrity protection of critical signalling messages is mandatory. The SN verifies the de-registration request for integrity and replay.
2) **Location updates request spoofing:** Instead of sending requests for de-registration, the attacker sends a location update request from a different area of SN (or another networks) in which the user is presently located. As a result the user is paged in the new area. The location update request is always protected against replay and modification.
3) **Camping on a false BS/MS:** The attacker with a modified BS/MS place in himself between the SN and the target user. The integrity protection of critical signalling messages protects against the DoS to some degree, as the intruder can’t modify signalling messages. However, the system does not prevent the attacker and hacker from relaying of messages between the network and the target user or ignoring some of them (not all of them) [3, 18].

8.3. Redirection Attack

Redirection attack is one of the possible attacks on multi homed mobile networks. In this attack, an attacker owns a device that can simultaneously impersonate both the Base Station Subsystem (BSS) and the MS. To cheat the victim MS, the attacker masquerades as a legitimate BSS by broadcasting a bogus BSS ID. It also disguises as the victim MS to trick the BSS. The attacker connects to another legal foreign network on behalf of the legitimate MS and builds up a clear tunnel to relay messages between the authorized foreign network and the victim MS. Since AUTN, RAND, and secret keys are successfully negotiated, the victim MS will then be authenticated by the foreign network. The redirection attack annoys a victim MS with billing Problems, forcing the victim MS on his HN to be charged for roaming into a foreign domain operated by another service provider. In this case, neither the HN nor the victim MS can detect the redirection attack. It is also possible that the attacker can redirect the victim MS to an insecure network with weak or none encryption. Hence, the adversary can eavesdrop the communication sessions [14].

8.4. Identity Catching

Unfortunately, UMTS system offers little protection against identity catching. Although IMSI is replaced by TMSIs after the first connection request, IMSI is sent clear during the initial rrcConnectionRequest and also on the occasions like VLR database crash, VLR’s inability to identify the TMSI. The attacker impersonates as a UMTS VLR/SGSN. During rrcConnectionRequest the victim may use TMSI. If TMSI cannot be resolved, then the network can make an identity request. In this case, ME has to send its IMSI in clear. After obtaining the IMSI, the attacker disconnects himself. We classify this attack as follow [2].

1) ***Passive identity catching***: The attacker with a modified MS waits inactively for a new registration or a database crash as in this state the user is requested to send its identity in clear text. The use of temporary identities inhibits passive identity catching since the intruder has to wait for a new registration or a mismatch in the SN database in order to capture the user's permanent identity in clear text.
2) ***Active identity catching:*** In this case, the attacker with a modified BS entices the user to camp on his BS and then asks him to send his IMSI. Unfortunately 3G does not provide perfect protection against this type of attack.

9. IMPROVING AKA SECURITY MECHANISM

In this section, we present some protocol and method such as Cocktail-AKA, S-AKA, and PANA/UMTS to improve UMTS authentication mechanism. Most of these techniques focus on AKA as an important authentication mechanism in UMTS system. Some of them are designed to protect specific attacks such as MiM and DoS. The study tries to describe briefly different scenarios and procedures to enhance UMTS authentication mechanism (AKA). They are as follows [8, 9, 10, 11, 13, 14, 16, 19, 21, 22, 23, 25].

The first Scenario proposes an authentication method combining the USIM mechanism and the concepts of AAA (Authentication, Authorization, and Accounting) for the fast authentication. In a wireless environment, authentication is required every time the mobile user moves from one cell to another. Therefore, authentication time should be taken into account as a significant and major factor in mobility. This method presents the procedure to achieve the secure and rapid authentication by applying the USIM mechanism well-suited over 3GPP to AAA.

In the second scenario, we propose special protocol to provide an IP compatible, lightweight, and flexible technique to authenticate a user to an access network. This protocol is based on Protocol for carrying Authentication for Network Access (PANA), a network-layer access authentication protocol carrier, which communicates, via Extensible Authentication Protocol (EAP), with an AAA infrastructure interacting with a UMTS AuC. PANA/UMTS is also based on EAP/AKA, which allows to using the AKA mechanism in new mobile generations comprising devices equipped with a USIM technology. PANA/UMTS prevents some significant attacks such as MiM, reply, hijacking, packets injection and content modification. It imposes data-origin authentication, replay protection based on SQN and integrity protection. In addition, it uses a 128 bit key length and is not vulnerable to brute-force or dictionary attacks.

As it is known Secure Sockets Layer (SSL) protocol has proved its efficiency in the wired internet and it will probably be the most promising candidate for wireless environments. In this scenario, this famous and previous protocol is purposed to improve some existing problems related to AKA procedures, such as compromised authentication vectors attacks, as they appear in current mobile communication systems such as GSM and UMTS. This method proposes how SSL, combined with Public Key Infrastructure (PKI) elements, can be used to resolve these vulnerabilities. measurements display that SSL-based authentication can be possible in terms of service time in wireless systems, while it can concurrently provide the suitable flexibility and scalability to network operators and a high level of confidence and assurance to mobile users.

In this part, new authentication protocol based on previous scenario is introduced (but with some modification) for 3G UMTS networks. This proposed protocol uses digital certificates PKI and SSL symmetric key generation schemes to generate CK and IK. In this scenario IMSI is sent encrypted while it is sent in plaintext in AKA procedure. The proposed protocol is more secure than 3GPP AKA and provides IMSI privacy against eavesdropping attack. In addition, it does not use AVs and find a new solution to vector attack vulnerability in UMTS AKA. This method reduces the total signalling traffic between entities and decreases the bandwidth consumed between database entities, while increasing the bandwidth consumed between MS and VLR.

As discussed in section 8, two important attacks of UMTS AKA are redirection and MiM. In these attacks, an adversary can launch these attacks to eavesdrop, or cause billing problems. To cope with these problems, a new Secure Authentication Key Agreement Protocol (S-AKA) is proposed in this scenario to improve the security to resist these threats. The analysis shows that proposed S-AKA not only defeats those attacks mentioned above, but also reduces up to 45% of bandwidth consumption. The formal proof of S-AKA is also given to ensure the security strength of S-AKA. In this method, S-AKA can resolve these attacks with the MS assistance itself and the SGSN. In S-AKA, the MS can reject illegal BS connection, and on the other hand the SGSN can verify the LAI sent from the MS. If the LAI is illegal, the SGSN will drop the connection. The LAI in UMTS AKA is not encrypted by any means, and thus can be altered by the adversary for significant attacks. In S-AKA, we use MAC to protect the integrity of LAI. If an attacker attempts to modify LAI, the illegal modification will be detected immediately.

This scenario introduces a new way to overcome the congenital defects and weaknesses of the AKA mechanism in UMTS. In this method, Ou et al. propose an improved protocol called the cocktail-AKA protocol to prevent some significant and powerful attacks such as DoS and impersonation. Cocktail-AKA protocol follows the essence of eminent cocktail therapy that is, using two kinds of AVs in the protocol. All SNs produce their own AVs in advance, which are called Medicated Authentication Vectors (MAV). These MAVs can be reused; hence, they need to be produced only once. When the authentication phase is initiated, the HE calculates a private AV for the MS and transfers it to the SN. This is called the Prescription Authentication Vector (PAV). The SN dispenses the PAV with the MAV, which can produce many effective AVs that can be used later for mutual authentication with the MS.

This method proposes a new and secure authentication mechanism by integrating the public key with the hash-chaining technique. The proposed protocol satisfies the security requirements of 3G mobile networks. It also provides the protection of IMSI to ensure subscriber un-traceability, key refreshment periodically, strong key management and a new non-repudiation service in a simple and elegant way. To avoid the complicated synchronization as in UMTS this protocol does not use SQN, the management of a hash chain is simple and elegant compared to that of SQN. This proposed protocol is secure against network attacks, such as replay attacks, guessing attacks, and other attacks.

In this scenario enhancements for the initial identification and for the AKA protocols are proposed that solve two known vulnerabilities and attacks of UMTS system like identity catching and secret key exposure. This solution, inspired from Al Saraireh identification protocol, realizes the encryption of the permanent identity of the subscriber and protects the messages exchanged during the AKA protocol. The proposed improvements that we proposed are in line with the UMTS security development philosophy: it is preferred to propose modifications to the current security protocols or to already proposed ones rather than proposing radical new protocols.

10. CONCLUSIONS

In this paper the security framework and mechanisms in the UMTS system are reviewed. The focus was on authentication mechanism, called Authentication and Key Agreement (AKA) as important security mechanism in this system. In addition, the most important security attacks such as Denial of Service (DoS), Man-In-the-Middle (MiM), Redirection, and Replay attacks, which threaten the mobile and network users, are presented. The results of these attacks mainly concern the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. We evaluated these attacks and classified them based on three security factors, authentication, confidentiality, and data integrity. The evaluations showed that the authentication factor is more interesting for attackers and hackers. In addition, we described the DoS, MiM, Identity catching, and Redirection attacks as the most prevalent and significant attacks which are target authentication factors in UMTS system and finally some resolves and purposes to improve authentication mechanism against these attacks and threats were found and presented.

REFERENCES

[1] K. Boman, G. Horn, P. Howard, and V. Niemi, (2002) "UMTS Security", Electronics & Communication Engineering Journal, Vol. 14, No. 5, pp. 191-204.

[2] M. Khan, A. R. Cheema, and A. Ahmed, (2008) "Vulnerabilities of UMTS Access Domain Security Architecture", 9th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 350-355.

[3] A. Bais, W. T. Penzhorn, and P. Palensky, (2006) "Evaluation of UMTS Security Architecture and Services", IEEE International Conference on Industrial Informatics, pp. 570-575.

[4] Z. Ahmadian, S. Salimi, and A. Salahi, (2009) "New Attacks on UMTS Network Access", Proceedings of the Conference on Wireless Telecommunications Symposium, pp. 291-296.

[5] D. Caragata, S. Assad, I. Tutanescu, and C. A. Shoniregun, (2011) "Security of Mobile Internet Access with UMTS/HSDPA/LTE", IEEE World Congress on Internet Security, pp. 272-276.

[6] Bogdanov, T. Eisenbarth, and A. Rupp, (2007) "A Hardware-Assisted Real time Attack on A5/2 without Precomputations", Cryptographic Hardware and Embedded Systems, Vol. 4727, pp. 394-412.

[7] G. Rose, and G. M. Koien, (2004) "Access Security in CDMA2000, Including a Comparison with UMTS Access Security", IEEE Journal of Wireless Communications, Vol. 11, No. 1, pp. 19-25.

[8] P. S. Pagliusi and C. J. Mitchell, (2004) "Heterogeneous Internet access via PANA/UMTS", Proceedings of the 3th International Conference on Information Security, pp. 38-46.

[9] H. Kim, and H. Afifi, (2003) "Improving Mobile Authentication with New AAA Protocols", IEEE International Conference on Communications, pp. 497-501.

[10] G. Kambourakis, A Rouskas, and S. Gritzalis, (2004) "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems", Journal on Wireless Communications and Networking, Vol. 2004, No. 1, pp. 184-197.

[11] O. A. Amir, S. Yousef, and S. A. Khayatt, (2010) "Analysis and Enhancement of SSL Based UMTS Authentication Protocol", 7th International Symposium on Communication Systems Networks and Digital Signal Processing, pp. 295-299.

[12] M. Koien, (2004) "An Introduction to Access Security in UMTS", IEEE Journal of Wireless Communications, Vol. 11, No. 1, pp. 8-18.

[13] Y. L. Huang, C. Y. Shen, Sh. Shieh, H. J. Wang and Ch. Chun Lin, (2009) "Provable Secure AKA Scheme with Reliable Key Delegation in UMTS", 3th IEEE International Conference on Secure Software Integration and Reliability Improvement, pp. 243 - 252.

[14] Y. L. Huang, Ch. Y. Shen, and Sh. W. Shieh, (2011) "S-AKA: A Provable and Secure Authentication Key Agreement Protocol for UMTS Networks", IEEE Transactions on Vehicular Technology, pp. 4509 - 4519.

[15] U. Meyer, and S. Wetzel, (2004) "A Man-in-the-Middle Attack on UMTS", Proceedings of the 3th ACM Workshop on Wireless Security, pp. 90-97.

[16] J. V. Franklin1 and K. Paramasivam, (2011) “Enhanced Authentication Protocol for Improving Security in 3GPP LTE Networks”, International Conference on Information and Network Technology, pp. 28-33.

[17] B. Aziz, and G. Hamilton, (2009) “Detecting Man-in-the-Middle Attacks by Precise Timing”, Proceedings of the 3th International Conference on Emerging Security Information, Systems and Technologies, pp. 81-86.

[18] P. P. C. Lee, T. Woo, and T. Bu, (2007) “On the Detection of Signalling DoS Attacks on 3G Wireless Networks”, 26th IEEE International Conference on Computer Communications, pp. 1289- 1297.

[19] X. Chen, and M. Ma, (2011) “The Optimization of Security Algorithm Selection for Wireless Communications in UMTS”, International Conference on Multimedia Technology, pp. 3277 - 3280.

[20] S. Yubo, H. Xili, and L. Zhiling, (2011) “The GSM/UMTS Phone Number Catcher”, 3th International Conference on Multimedia Information Networking and Security, pp. 520-523.

[21] D. Caragata, S. E. Assad, C. Shoniregun, and G. Akmayeva, (2011) “UMTS Security: Enhancement of Identification, Authentication and key Agreement Protocols”, International Conference on Internet Technology and Secured Transactions, pp. 278-282.

[22] S. Wu, Y. Zhu, and Q. Pu, (2010) “Security Analysis of a Cocktail Protocol with the Authentication and key Agreement on the UMTS”, IEEE Communications Letters, pp. 366-368.

[23] M. A. Fayoumi and J. A. Saraireh, (2011) “An Enhancement of Authentication Protocol and Key Agreement (AKA) For 3G Mobile Networks”, International Journal of Security, Vol. 5, No. 1, pp. 35-51.

[24] C. Xenakis, and L. Merakos, (2004) “Security in third Generation Mobile Networks”, Computer Communications, Vol.27, pp. 638-650.

[25] E. Barkan, E. Biham, and N. Keller, (2008) “Instant Cipher text-Only Cryptanalysis of GSM Encrypted Communication,” Journal of Cryptology, Vol. 21, No. 3, pp. 392-429.

[26] C. J. Mitchell, (2004) “Security for Mobility”, Electronics & Communication Engineering Journal, Vol. 14, No. 5, pp. 178-178.

[27] J. Al-Saraireh, S. Yousef, and M. Al Nabhan, (2006) “Enhancement Mobile Security and User Confidentiality for UMTS”, Second European Conference on Mobile Government, pp. 20-25.

Authors

M. Ayoubi Mobarhan received the BSc degrees in electrical engineering (electronic) from Islamic Azad University of Lahijan (Iran) in 2008. He has been working at his own private company (IT and Electronic engineering) since August 2007. In October 2009, he joined the Department of Computer Engineering, University of Guilan, Iran, as a full-time MSc. student under advisor Dr. Asadollah Shahbahrami. His research interests include wireless Application Protocol (WAP), image and video processing, wireless networks, and security of mobile communications.

M. Ayoubi Mobarhan received the BSc degrees in electrical engineering (electronic) from Islamic Azad University of Lahijan (Iran) in 2008. He has been working at his own private company (IT and Electronic engineering) and scientific institute since August 2005. In October 2009, he joined the Department of Computer Engineering, University of Guilan, Iran, as a full-time MSc. student under advisor Dr. Asadollah Shahbahrami. His research interests include image and video processing, wireless networks, security of communication networks, mobile communications, and multimedia instructions set design.

A. Shahbahrami received the BSc and MSc degrees in computer engineering (hardware and machine intelligence) from Iran University of Science and Technology and Shiraz University in 1993 and 1996, respectively. He was offered a faculty position in the Department of Electrical Engineering at University of Guilan. He has been working at University of Guilan since August 1996. In January 2004, he joined the Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, Delft, The Netherlands, as a full-time Ph.D. student under advisors Prof. Stamatis Vassiliadis and Dr. Ben Juurlink. He received his PhD degree in September 2008 from Delft University of Technology. He has an assistant professor position in Department of Computer Engineering at the University of Guilan. His research interests include advanced computer architecture, image and video processing, multimedia instructions set design, reconfigurable computing, parallel processing, and SIMD programming.