Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

3GPP AKA Protocol: Simplified Authentication Process

Anilmit Choudhary, Randhir Bhandari
Computer Science Department
Shoolini University, Solan, H.P., India

Abstract: This paper reviews about the establishment of connection between client and server in authentication and key agreement protocol (AKA); a client-server key exchange protocol resulted from the Third Generation Partnership Project (3GPP). AKA was adopted by the Universal Mobile Telecommunication System (UTMS) which is considered as the standard for the Third Generation (3G) wireless communications. This paper focuses on the simplified description of the key exchange process of the 3GPP AKA protocol. We have explained in detail the key exchange process of the 3GPP AKA protocol which would provide beginners a basic idea about authentication process of the protocol. Here we analyzed key feature of the 3GPP i.e. mutual authentication, through well explained and documented mathematical expressions.

Index terms– Authentication and key agreement, wireless, GSM, UMTS, Third generation (3G).

I. INTRODUCTION

There has been a tremendous growth in the field of wireless communication in past years and it has become an important part of our communication system due to its flexibility with respect to its unwired connectivity and ease of use. The security of a communication system is based on its features such as its access, authentication issues, encryption and decryption issues etc. A wireless system is considered less secure as compared to the wired one due to the fact that the wireless systems are not limited by the physical boundaries like cables. This makes them more vulnerable to attacks like eavesdropping (intercepting the information in between the sender and the receiver). First Generation (1G) communication systems suffered major drawbacks with respect to its security issues which gave rise to the need of a more secured communication system. Thus Second generation (2G) cellular systems were developed.

Global System for Mobile Communication (GSM) is the standard for the Second Generation (2G) mobile communication systems which is an improvement in the security features of the First Generation (1G). The GSM provided security features like privacy of data and client authentication by a challenge-response method [5]. In this method, the client verifies its identity by replying to the challenge initiated by the server or the network. The GSM authentication and key agreement is considered as simple and reliable standard used by 2G networks but possess certain limitations. The major limitation of the GSM technology is in its core advantage over 1G network i.e. authentication issue. Since in GSM authentication, the server verifies the client through the challenge-response mechanism but on the contrary, the server is never asked to prove its identity to the client [6, 7]. This limitation makes 2G communication system vulnerable to various attacks and threatens its security.

To improve the security limitations founded in the GSM and 2G network systems Third Generation Partnership Project (3GPP) came up with the Universal Mobile Telecommunication System (UMTS), a standard for Third Generation (3G) wireless communication systems. UMTS adopted the successful features of the GSM to make 3G communication system much more secured as compared to the Second Generation (2G). 3GPP introduced Authentication and Key Agreement (AKA) protocol which retains the framework of the GSM AKA and also introduces the concept of mutual authentication and key freshness.

II. EXPLANATION OF GSM AND 2G

GSM is considered to be the standard for the 2G cellular systems. Second Generation (2G) helped in the transmission of the information in digital form by using air as the medium. Using these digital signals between the client's handset and the service provider, 2G helped in increasing the system capacity in following two ways [4]:

- Digital voice data is much easier to be compressed when compared to the analog signals through the use of various codecs. Same amount of bandwidth allowed more traffic (calls) using the 2G environment.
- 2G systems were designed with a view to emit reduced radio power which helped increased number of devices (cells) to be placed in the same space.

In 2G Data Transmission, with GPRS (General Packet Radio Service) we can achieve about 40 Kbit/s whereas with EDGE (Enhanced Data tonality Rates for GSM Evolution) we have 1mbit/s of practical transmission speed. The GSM was designed with a view to provide the security regarding the user authentication and also focused on the exact billing of the phone calls. Besides these advantages, 2G communication uses lossy compression technology to filter out the background noise in its digital calls. But along with these advantages this system has following threats involved:

- Second Generation (2G) communication authenticates client (user) but limits the authentication of the base station (Network). This limitation of 2G helps the attacker to create a false base station in the middle of the communication line. The false base station can then be used for the eavesdropping scenario.
- The GSM uses ciphering algorithms which are weak in nature [8]. These weak crypto algorithms allow various attacks over the system.

Authentication process involves a Secret Key stored in the SIM (Subscriber Identity Module) of client's mobile device. Complete process involves challenge response mechanism in which the server (network) sends a challenge to the client's (User) device that contains a random number. The client's device computes the output based on that random number. This output is then sent back to the server where an expected response is already stored. If the two values match with each other, then the client's mobile is authenticated and connection is established.

III. EXPLANATION OF UMTS AND 3G

Universal Mobile Telecommunication System (UMTS) is a standard for Third Generation (3G) cellular system. UMTS is developed and maintained by Third Generation Partnership Project (3GPP), a group of telecommunication associations called as the Organizational partners. 3G provided a boost to the mobile telecommunication technology with greater reliability in terms of security features and data transmission rates. 3G provides data transmission rates of about 2 Mbit/s and 384 Kbit/s for static users and travelling users respectively. In terms of its security features 3G offers mutual authentication which authenticates user as well as the network. To some up 3G network provides following advantages over 2g network :

- Increased data transmission speed in 3G network than 2G.
- Client receives video or satellite based programs in 3G technology.
- Client can use the wireless broadband service in 3G networks.

IV. EXPLANATION OF AKA PROTOCOL

Authentication and key agreement protocol is an authentication protocol for 3G networks based on the mutual authentication principle. By mutual authentication, we mean that the client authenticates the network and the network authenticates the client by using the secret keys and authentication vectors respectively. . The 3G security objective focuses mainly on adopting the strong security features of the 2G network and removing the limitations of the same. The 3G network retained some of the security features of 2G network such as user authentication, radio interface encryption, user identity and location confidentiality, the SIM (Subscriber Identity Module) ;kept as a hardware (removable) which contains all the security functions (except encryption). By retaining these features of the second generation (2G) communication systems, 3GPP AKA provides following security features to its users:

- *Assuring the freshness of key to the user:* The user is made sure that the cipher key and the integrity key shared are fresh (not used before).
- *Authentication of the network to the user:* 3G provides the flexibility to authenticate the network which reduces the chances of most prevalent attack in 2G systems i.e. false base station attack.

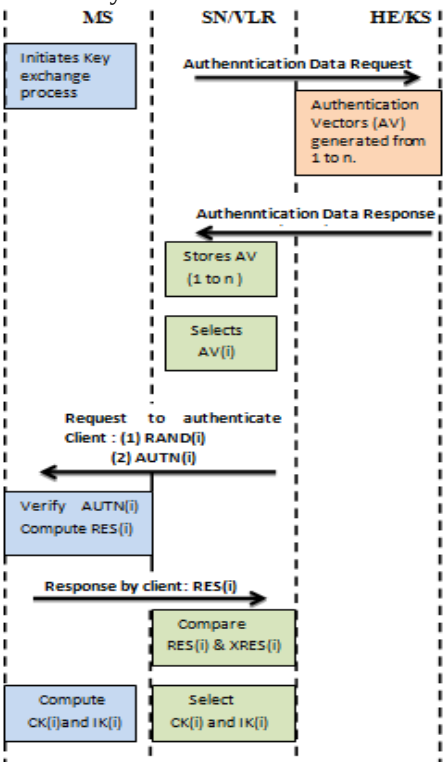

Fig.1. Working of AKA Protocol.

- *Authenticated Key distribution field HE:* It shares secret key with the client and authentication vector with the network.
- *Establishment of CK and IK:* Two 128 bit keys (Cipher key and Integrity Key) are also established during authentication process in the 3GPP AKA.

Authentication and Key Agreement (AKA) protocol uses symmetric cryptography. It shares a secret key with the client represented by the Mobile Station (MS) which is used to maintain the private information between the MS and the Home Environment (HE). AKA protocol is usually run in the UMTS IP Multimedia Services Identity Module (ISIM). ISIM is the application which runs on the smart card in a 3G device in IP Multimedia Subsystem (IMS). Main objective of the ISIM is to provide assistance for the authentication of the client to the IMS. The ISIM application works well with both the GSM and the UMTS networks.

Table 1: Abbreviation Table

MS	- Mobile Station
SN	- Serving Network
VLR	- Visitors Location Register
HE	- Home Environment
KS	- Key Server
AV	- Authentication Vector

Authentication and Key Agreement protocol has following three important components during distribution of keys, Authentication and key establishment process [3, 9]:

- *Client (C):* C is the client or the mobile phone which is also referred to as the mobile station (MS). MS is the component which initiates the key exchange process by requesting access to the network. It shares a secret key (K) with HE.
- *Serving Network (SN):* It is also called as the Server (S). It authenticates C and grants access to the source by using its authentication vector (AV). It is sometimes also referred to as Visitors Location Register (VLR).
- *Home Environment (HE):* It is also known as the Key server (KS). KS shares Secret Key (K) with the client (C) and provides authentication vectors to the Serving Network (SN) to facilitate the mutual authentication between server and the client.

A) Flow of Data:

The client represented by Mobile Station (MS) initiates request for the key exchange. Key server (KS) shares a secret key (K) with MS. This key is not known to the Serving Network (SN). Now SN sends an authentication data request to the KS or HE. Based on this data request HE sends back the response to SN which contains an array of authentication vectors (AV [1 . . . n]). Each Authentication vector consists of :

- A random number (RAND),
- An expected response (XRES),
- A cipher key (CK),
- An integrity key (IK),
- An authentication token (AUTH).

Once the array AV (i) is received by SN, it selects one authentication vector from the array and sends RAND and AUTH component of that AV to MS. MS uses AUTH to authenticate SN, calculates its session keys using random number (RAND) and secret key and sends back response (RES) to the SN. SN uses its selected authentication vector to compare RES with the XRES. If RES = XRES then the client and the server both successfully authenticates each other.

B) Authentication and Key Agreement:

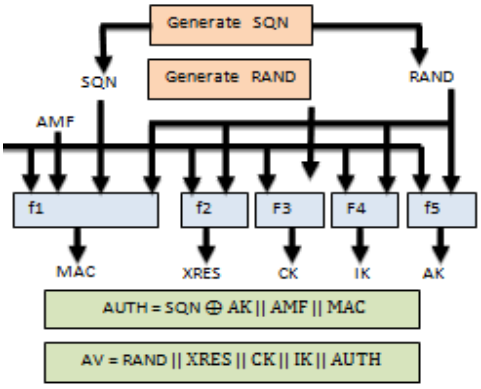

Fig.2. Authentication Vector for AKA

In the beginning HE generates SQN_{HE} and RAND. Also, HE maintains its sequence counter SQN_{HE} for each individual client. On the other hand, the client also maintains its sequence counter (also called as sequence number) SQN_{MS}. Firstly, the Home Environment (HE) computes expected response (XRES), cipher key (CK), integrity key (IK), anonymity key (AK), message authentication code (MAC) and finally authentication token (AUTH) [2, 3].

- Expected response
  $XRES = f2_k (RAND)$
- Cipher key
  $CK = f3_k (RAND)$
- Integrity key
  $IK = f4_k (RAND)$
- Anonymity key
  $AK = f5_k (RAND)$
- Message Authentication Code
  $MAC = f1_k (SQN \| RAND \| AMF)$ (|| denotes concatenation)
- Authentication Token
  $AUTH = SQN \oplus AK \| AMF \| MAC$
  ($\oplus$ is the bitwise exclusive OR)

Here, f1 and f2 are the message authentication functions and we have three key derivation functions i.e. f3, f4 and f5 [10]. AMF is defined as the Authentication Management Field which defines the timeout vales and algorithms for multiple authentications. Complete working of 3GPP AKA can be explained in the following steps:

Step1: Once the distribution of key and authentication vector (AV) is over, then the serving network (SN) sends AUTH and RAND from an authentication vector of the array (AV (i)) to the mobile station (MS).

Step2: MS uses the equation $AK = f5_k (RAND)$ to get SQN by using the formula $SQN = (SQN \oplus AK) \oplus AK$.

Step3: MS then uses this SQN to calculate its MAC (say XMAC).

Step4: Now, if XMAC (MAC of MS) = MAC (MAC of SN), then the MS checks for the correctness of SQN_{HE}. The SQN_{HE} should be greater than the SQN_{MS}.

Step5: If correct, then the client authenticates the serving network (SN).

Step6: On the contrary, if not correct then HE receives a synchronization failure message and needs to resynchronize its counter $SQN_{HE.}$

Step7: When SN has been authenticated by MS then MS calculates its $RES = f2_k (RAND)$, CK and IK. These values are then sent back to the SN.

Step8: On the server side, SN compares RES with the XRES. If RES = XRES, then the client is also verified by the SN. Once the process of mutual authentication is successful, SN selects the CK and IK from the selected AV.

V. CONCLUSION

3GPP AKA provides improved security features by adopting some features of 2G network and introduces the concepts like of mutual authentication and freshness of keys. The distribution of keys and authentication process of 3GPP AKA is complex and needs through understanding. This paper has the simplified explanation of the concept and the beginners can understand the working of 3GPP AKA in detail easily. In next paper we will take into detail the security weakness in 3GPP AKA protocol considering the false base station attack and will also suggest method to prevent it providing proof for the same.

REFERENCES

[1] Babbage. E and Biham. E and Keller. N (2003),” Instant Cipher text-Only Cryptanalysis of GSM Encrypted Communication”, Proceedings of Crypto 2003, Springer-Verlag.

[2] European Telecommunications Standards Institute (ETSI), GSM 02.09: Security Aspects, June 1993.

[3] http://en.wikipedia.org/wiki/2G.

[4] Kolesnikov. V (2010),”A Security Enhancement and Proof for Authentication and Key Agreement (AKA)” 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings, pp. 235-252.

[5] Kataria. J and Bansal. A (2013) ,”Exploration of GSM and UMTS Security Architecture with AKA Protocol ”, International Journal of Scientific and Research publications, Volume 3, Issue 5, ISSN 2250-3153.

[6] Lee. C. H, Hwang. M. S and Yang. W. P (1999),”Enhanced Privacy and Authentication for the Global System for Mobile Communications”, Wireless Networks, vol. 5, pp. 231-243.

[7] Saxena. N and Chaudhari.N. S (2013),”NPA: Protocol for Secure Communications in GSM Cellular Network”, the 10th Annual IEEE CCNC- Wireless Communications Track.

[8] Zhang. M and Fang. A (2005),” Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol”, IEEE Transactions on Wireless Communications, vol. 4, No.2.

[9] 3rd Generation Partnership Project. 3GPP Technical Specification 3GPP TS 33.102 V7.1.0: (2006) “Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 7)”.

[10] 3rd Generation Partnership Project. . 3GPP Technical Specification 3GPP TS 33.205 V7.0.0 (2007),” An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; 3G Security; Document1: General (Release7)”.

