Authentication Protocols in GSM Networks

Presented by: Xixi Chen
ID: 97106369
November 14, 2002
For: ECE750

Outline

- Introduction
- What is Authentication Protocol
- GSM Authentication Protocol
- Protocol Proposed by Al-Tawil and Akrami
- Protocol Proposed by El-Fishway and Nofal
- Conclusion
- Future Work
- Q & A

2

References

- N. El-Fishway, M.Nofal, A.Tadros, “An Effective Approach for Authentication of Mobile Users”, *Vehicular Technology Conference*, IEEE 55th, pp 598-601, Vol 2, Spring 2002.
- K.Al-Tawil, A.Akrami, H.Youssef, “A New Authentication protocol for GSM Networks”, IEEE Proceedings on Local Computer Networks, pp.21-30, Oct, 1998

Three levels of authentication

- User level identification: user sends its pins etc. to the system to identify itself
- Device level identification: the phone or device identifies itself to the network.
- Radio line level encryption: use of encryption algorithms to send messages

4

Usually, User level identification and device level identification are combined as the user is the device.

The first two level of authentication is the most important because security critical errors made at this stage will undermine the security of the whole session and possibly subsequent sessions as well. These two levels are often known as call setup process to setup a session. It consists of protocols for authentication and key management.

What is Authentication Protocol

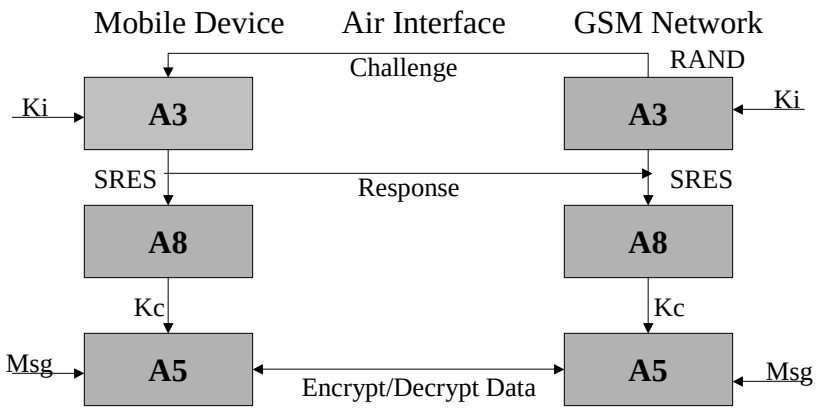
- Protects
  - User Confidentially
  - User Authentication
- Provides three stages:
  - Identification
  - Verification
  - Secret keys established

5

There are two main purposes involved in the forming the authentication protocol. The first is confidentially which is preventing an attacker from know which user is using what resource in the network and which part of the network is providing that service. Authentication is for the communicating party to identify each other. Specifically, the authentication protocol also provides three services.

The identification stage is when the entity or MS presents its identity to the network. The verification stage is where the identity is checked. A the same time, the network is also identified to the MS and that identity is checked so that MS knows, it is communicating with the correct network. The third stage is allowing a secret key to be established once the communicating party has identified each other.

GSM Security Architecture



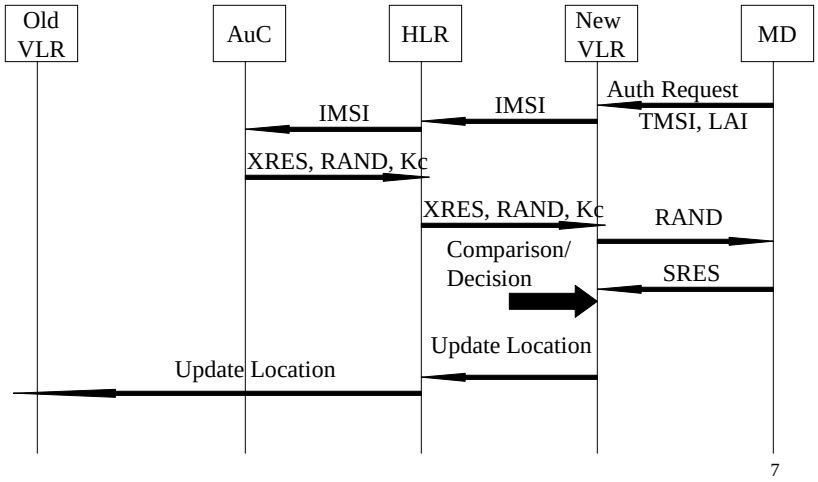
C.Lo, Y.Chen, "Secure Communication Mechanisms for GSM Networks", *IEEE Transactions on Consumer Electronics*, Vol.45, pp.1074-1080, Nov. 1999

6

The GSM security architecture has three tier. The first tier consists of the A3 algorithm that uses the challenge and response method for user authentication. Both MS and the GSM network has a copy of a key Ki that was established upon the device's registration to the network. The Ki will be most likely stored in the MD's SIM card while the Ki for the GSM network is stored in the AuC center. The A3 algorithm will use this Ki to create a 'Challenge' to the MD and the Mobile Device will create a 'Response' using that same Ki to verify itself. I will talk about the detail of this process in the next slide. The second Tier is the A8 algorithm that uses the output from the A3 algorithm to generate the secret key used in the third Tier, the a5 algorithm This algorithm is an encryption/decryption algorithm that encrypts/decrypts data passed between the MD and the Network. The three algorithms will be stored in the Mobile device for the user and in the AuC in the GSM Network.

GSM Authentication Process

- Challenge and Response



When the mobile phone is switched on, a challenge and response session is started to control the validity of the data. The MS transmit the registration request to the base station and the BTS forwards the request to the MSC which informs the Corresponding VLR on the user's location. The request includes the Temporary mobile subscriber id and the LAI.

The New VLR then sends a request ot the HLR asking for authentication parameters for that MS. The HLR forward this request to the AUC. The AuC computes the random challenge(rand) and the Signed response(XRES) using the common key Ki and the A3 algorithm. It also computes the Kc using the A8 algorithm. The AuC sends the result to the VLR through the HLR. The VLR sends the Rand to the MS as a challenge asking the MS to compute SRES using Ki and A3 algorithm. MS computes the SRES using its key Ki and sends it back to the VLR. In the mean time, it also computes Kc and keeps it for later use. The VLR compares the SRES with the XRES fi the two are equal, the MS is authenticated.

GSM Authentication Short Falls

- VLR and HLR communication is not secure. (Effective approach)
- Man in the Middle Attack
- Considerable amount of call setup delay
- Challenge and Response not very secure†
- A3, A8 and A5 algorithm have minimal security features and can be broken easily.

† C.Lo, Y.Chen, "Secure Communication Mechanisms for GSM Networks", *IEEE Transactions on Consumer Electronics*, Vol.45, pp.1074-1080, Nov. 1999

8

The interaction between the HLR and the VLR uses an internet work. If it is safe to assume that this network is safe for today's mobile system, however, the same can not be guaranteed in a global scale. There is a minimal assumption about the security of the intermediate transport network.

Man-in-the-middle attack - The attacker would try to masquerade as either MS or the BS to communicate with the other. Presently, the GSM protocol does not authenticate the GSM network against the MS.

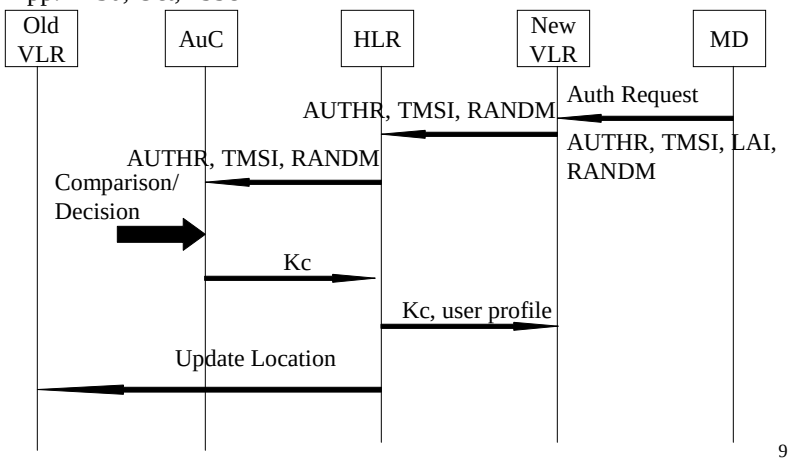
Presently, there are seven signals passed before a decision is made, the number of signals can be reduced. Since authentication is used at the beginning of registration, call termination and call initiation, reducing this is very important.

The challenge and response is a simple protocol, however, it is not very secure as proven by an article by R.Bird et al..

In practice, the service provider usually incorporates the functionalities of the A3 and A8 algorithm in a unique algorithm called COMP128. This is an algo that accepts an 128 bit input string and outputs a 96 bit cipher text. The COMP128 aglgorithm have been made of public domain and a number of online and offline attacks have been proposed. It is demonstrated in certain articles that the Ki key can been reconstructed after collecting 200000 authentication response spending at least 8 ho9urs for an online attack. Other articles [BSW00] have also show the key Kc can reconstructed thus breaking the A5 algorithm.

Protocol by Al-Tawil et all

- K.Al-Tawil, A.Akrami, H.Youssef, "A New Authentication protocol for GSM Networks", IEEE Proceedings on Local Computer Networks, pp.21-30, Oct, 1998



9

This new protocol was proposed in the article illustrated here. The purpose of this protocol is to reduce the authentication delay and the signal load. In this protocol, we introduce a new variable know as countM used for statistics purposes. It is stored in the network HLR and in the SIM of the MS. A random number RANDM is generated locally by the MS. It is concatenated with COUNTM to produce RANDG. RANDG and Ki are then used as inputs to the A3 algorithm. It then passes TMSI, LAI, RANDM and AUTHR to the GSM network. Once the new VLR receives the TMSI, it sends a request to the HLR asking for verification of the AUTHR. HLR adds the COUNTM to the request and forwards to AuC. AuC produces RANDG, then computes AUTHR and Kc by applying the MS's secret key Ki and RANDG. It then compares the two AUTHR. If the two are equal, the MS passes the authentication process.

Comparison and Discussion (1)

- Number of signaling Messages reduced

	GSM Scheme	Proposed Scheme
AuC	2	1
HLR	4	2
VLR	5	2
Old VLR	1	1

- Authentication delay = $T_{\text{Final Decision}} - T_{\text{req}}$
- TDB = Time due to database delay
- TRF= Time between MD and BTS.

10

Show the number if signal messages and how we got this chart

Since the number of signaling message reduced, the load of the network therefore reduced and minimizes collision

The authentication delay is defined as the time interval from the instant the user starts the authentication process until the network takes the final decision. Lets make TDB be the time delay due to network databases messages exchange. Assume TDB is the same between all of them. Let TRF be the time of the radio frequency

Comparison and Discussion (2)

- Tad for original Protocol = 4TDB + 3TRF
- Tad for new Protocol = 2TDB + TRF
- Decrease Call Drop
- Same Security Level
- Requires Higher Bandwidth
  - Messages sent in the air for original protocol: TMSI, LAI, Auth Request
  - Messages sent in the air for new protocol: TMSI, LAI, Auth Request, RANDM, AUTHR

11

As the result, the delay for the new protocol was reduced by half. Show how to get it

Since the delay decreased, the call drop decreased as well. This is because, the old VLR is not updated until the authentication decision is made. As a result, it MS receives a call during that transition time, the network will page it in the old area, but the MS has already moved so the call is dropped or lost. By reducing the authentication time, the number of call dropped will decrease.

In the GSM authentication, the idea is based on comparing the entity called SRES computed in two different laces, the AuC and the SIM. In the this protocol, the variable AUTHR is computed in the same two places. In GSM, SRES and RAND are used as pubic parameters while Ki and Kc are used as private parameters that are never transmitted. In this protocol, AUTHR, and RANDM are public and Ki and KC are maintained as private.

The extra messages if we assume RANDM is 64 bits, AUTHR is 32 bits, that is 12 bytes of extra info passed. This is now a tradeoff between the number of signals and the message size.

Protocol by El-Fishway et All

- N. El-Fishway, M.Nofal, A.Tadros, “An Effective Approach for Authentication of Mobile Users”, *Vehicular Technology Conference*, IEEE 55th, pp 598-601, Vol 2, Spring 2002.
- Mutual Authentication between MD, HLR, VLR.
- Based on computing an authentication token in the form AUTHk(X,Y,Z)

12

This protocol is introduced in this article. The basic assumption behind this protocol is that no entity is safe. Therefore, mutual authentication between MS and VLR is needed as well as authentication between VLR and HLR.

It is based on computing an authentication token known as AUTHK(X,Y,Z). It is a hash function using X,Y,Z as inputs and K as the encryption key.

Protocol Notations

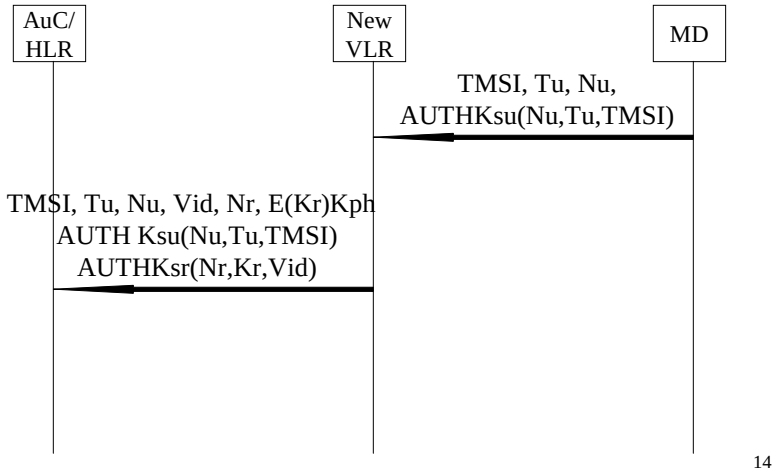
- Kpx – public key of entity X
- Ksx – secret key of entity X
- Nh – Nonce generated by HLR
- Nv – Nonce generated by VLR
- Kh – session key generated by HLR
- Kv – session Key generated by VLR
- Kc – short term session key shared between VLR and MD
- Vid/Hid – temporary ID of the VLR/HLR

13

Nonce is a parameter that varies with time.

Authentication Process (1)

- Pubic key of MD and VLR is stored in HLR



14

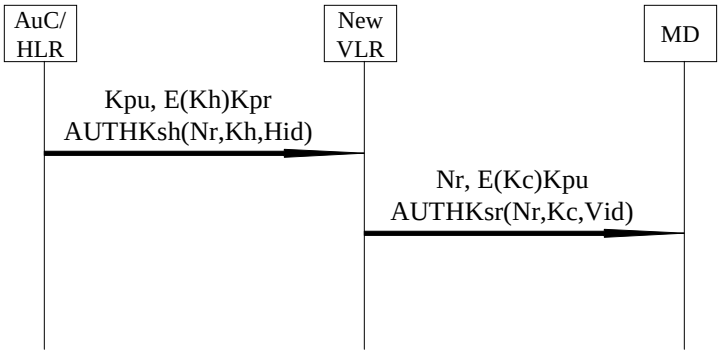
User begin by generating a nonce Nu and timestamp Tu. Next it computes AuthKsu(Nu, Tu, TMSI) under the the MS's secret key Ksu and sends it to VLR

When VLR receives this, it needs to communicate with the HLR by forwarding that information. However it must first authenticate itself against HLR. It first generate a nouce Nv and Kv which is the session key used between VLR and the User. It encrypts Kv with the public key of Kph of HLR so that only HLR can decrypt this key. The VLR then sends TMSI, Tu, Nu, VLRid, Nr, and the encrypted Kph along with the two auth expression to HLR.

When HLR receives these messages, it must first authenticate the VLR. It uses its secrete key Ksh to decrypt the Kv value. Then knowing Kr, Nr, and the VLRid, it can validate AUTHKsr using the public key of the VLR Kpr. A match authenticates the VLR to the HLR. The HLR then searches its database for the public key of the user using TMSI. The Tu is validated by comparing with the current clock and also the last timestamp recorded in the HLR record. If the timestamp is not greater, the record is rejected. This prevent another device from imitating the MS. Given TMSI, Tu and Nu, the HLR validates AUTHKsu using the MS's public key Kpu. A match authenticates the MS to the HLR.

Authentication Process (2)

- Kc = f(Kr,Kh) where f could be XOR function



- All three entities are mutually authenticated

15

Once the MS and the VLR has been authenticated, the HLR computes Kh which is a component of the session key Kc. The HLR then computes Kc and encrypts Kh with the public key of the VLR. It also computes AUTHKSH with Nr, Kh and Hid under its own secret key. It then sends all this info along with Kpu to the VLR. Once the VLR receives this info, it decrypts the Kh using its secret key, given Nr, Kh and Hid, it validates AUTHKSH using HLR's public key. A match in this case authenticates HLR to VLR. It is hard to obtain Kh without having Ksr which is only know to VLR. Without Kh, the HLR would not be authenticated by the VLR. The VLR also validate AUTHKSU with Nu, Tu and TMSI, this step authenticates MS to VLR. With Kr and Kh, the VLR computes the session key Kc and encrypts it with the public key of MS. It also computes AUTHKSR9Nu,Kc,Vid) and sends the info the the MS. Once the MS receives the messages, it decrypts KC using its secret key, then knowing Kc, Nu and Vid it validates AUTHKSR. This step authenticates VLR to U.

At the end VLR<->MS mutual authentication, VLR<->HLR mutual authentication, HLR<->MS mutual authentication, KC is established

Advantages

- Uses the idea of computing authentication tokens and pubic/private keys
- Number of signal messages decreased
- Prevents:
  - Mobile User Attack
  - Base station attack
  - Guess attack
  - Man-in-middle attack

16

Mobile User Attack – is when an attacker pretends to be the base station or VLR. In our case, the attacker would not have the secret key of the VLR which means it can not authenticate it self to the HLR or the MS.

Base Station Attack – attacker pretends as the mobile user. The Attacker would not have the secret key of the user and also the time stamp might be wrong as well.

Guess Attack – The guessing attack occurs when the attackers tries to guess passwords or secret keys I.e. the key Ki. In this case, all the session keys are encrypted and decrypted with public and private keys and without these session keys, the expression can not be authenticated. The guessing attack thus doesn't really apply here.

Man in the middle attack – Occurs when the attacker interrupts the communication between two entities and tries to be either one. This is prevented because each of the auth messages are validated based on the entities having the secret key to decrypt the session key. In the case of the AUTH message passed between the MS and the VLR and HLR, there is no session key, but the HLR had to search for the public key of the MS to validate the expression. Therefore the public is not really public and an attacker would not have that.

The number of signal is now reduced to four versus the seven signals in the original GSM network.

Disadvantages

- Large Bandwidth
- Large computation power on the MD, VLR and HLR
- Complexity
- MD<->VLR authentication should occur first so that message doesn't have to be forwarded to the HLR if authentication fails.

17

As you can see from the authentication process, there is a large bandwidth incurred as a result of passing the id of the entitles, the Nonce and the AUTHR expressions. Much more is required than the original GSM network. This can make the network slower in some cases.

The protocol also require the MS, VLR and HLR to have large computation power. For example, instead of the VLR making the comparison decision to authenticate the MS, it now must validate two authr expressions and create its own authr expression. All three entities must validate the AUTHR expressions and authentication each other. Each also have the additional duty to compute a nonce

The algorithm is extremely complicated and hard to follow

The algorithm should be adjusted so that the authentication between the MS and the VLR occur first. If the MS is not authenticated, the VLR doesn't have to forward all the messages to the HLR and this may save resources.

Conclusion

- The GSM authentication protocol needs much improvement
- The first protocol reduces authentication delay but needs higher bandwidth to carry extra tokens => practical
- The second protocol is complex, huge bandwidth, but secure => not practical

18

As you can see from this presentation, the GSM authentication protocol needs much improvement. The first protocol we looked at reduces authentication delays by decreasing the number of signals passed. However, it introduces one extra token to be passed among the entities. This protocol is clean and simple and the basic security idea is the same with AUTHR and RANDM as pubic parameters and KC and Ki as private parameter. This protocol can be considered to replace the current one.

The second protocol is very complex due to the fact that it assumes no trust between any identities. There is a huge bandwidth incurred as a result of passing many parameters around for verification and the computation power of each of the entity must also be adjusted. All of this came at a cost of having a more secure system. In my opinion, this protocol is too complex and may take too long for the GSM network. Less complex, but equally as secure protocols can be devised.

Future Work

- Synchronizing counter between MD and HLR in the first protocol
- Decrease complexity but maintain security in the second protocol.
- C.Lo and Y.Chen introduces C3, C8 and C5 in IEEE Trans on Consumer Electronic Nov, 1999

19

The article by C.Lo and Y.Chen introduces three algorithms to replace the current A3, A8 and A5.

The C3 algorithm is the authentication algorithm and uses public key to authenticate the message. It also has two phases, the connection phase and the release phase so that the network prevents the MS from denying the service he/she received.

It uses certificates and digital signatures to verify identities preventing man in the middle attacks and the MS and the GSM network is mutually authenticated. The protocol is much simpler and the security is at the same level as the second protocol.

Q & A

All References

[1] N. El-Fishway, M.Nofal, A.Tadros, “An Effective Approach for Authentication of Mobile Users”, *Vehicular Technology Conference*, IEEE 55th, pp 598-601, Vol 2, Spring 2002.

[2] K.Al-Tawil, A.Akrami, H.Youssef, “A New Authentication protocol for GSM Networks”, *IEEE Proceedings on Local Computer Networks*, pp.21-30, Oct, 1998

[3] C.Lo, Y.Chen, “Secure Communication Mechanisms for GSM Networks”, *IEEE Transactions on Consumer Electronics*, Vol.45, pp.1074-1080, Nov. 1999

[4] S.Cimato, “Design of an Authentication Protocol for GSM Java cards”, *Lecture Notes in Computer Science*, pp.355-368, Springer, 2002.

[5] H.Lin, L.Harn, “Authentication in Wireless Communication”, *Global Communication Conference*, Globecome’93, IEEE, pp.550-554, 1993