GSM Security

Anshu Anand Jethi, Ajay Rana

Abstract- ***This paper demonstrates the secure communication in GSM. Global System for Mobile Communication (GSM) is a second generation cellular standard developed to provide voice services and data delivery using digital modulation.***

With its great features like providing access to users at anytime and anywhere, mobile communication is very attractive among the users as well as operators and service providers. But, in spite of of several advantages, mobile communication also has been facing many security problems. In 2G and 3G technologies viz GSM, GPRS and UMTS, the architecture comprises of mainly three nodes; the mobile station (MS), Visitor Location Register/Serving GPRS Support Node (VLR/SGSN), and Home Location Register /Authentication Center (HLR/AuC). These nodes are involved to encrypt/decrypt the data and authenticate the user (MS) in GSM, GPRS and UMTS.

Keywords- ***GSM, GPRS and UMTS, (VLR/SGSN), (HLR/AuC).***

I. INTRODUCTION

Wireless and mobile communication systems are very famous among the customers as well the operators and service providers. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The Global System for Mobile Communications (GSM) occupies almost 70% of the wireless market and is used by millions of subscribers in the world [1].

In the wireless services, secure and secret communication is anticipated. It's the interest of both, the customers and the service providers. These parties would never want their resources and services to be used by unauthorized users.

The services like online banking, e-payment, and e/m-commerce are already using the Internet. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as secure as possible from the security threats. Smart cards (e.g. SIM card) have been proposed for applications like secure access to services in GSM to authenticate users and secure payment in Visa and MasterCard [2]. Wireless transactions are facing several security challenges. Wireless data passing through air interface face almost the same security threats as in case of wired data. However, due to limited wireless bandwidth, battery, computational power and memory of wireless devices add further limitations to the security mechanisms implementation [3].

The use of mobile communication in e/m-commerce has increased the importance of security. An efficient wireless communication infrastructure is required in every organization for secure voice/data communication and users authentication. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and reduce the number of updating Home Location Register/Authentication Center (HLR/AuC) while the Mobile Station (MS) changes its location frequently [3].

A. The Purpose of GSM Security:

- The access to the mobile services.
- Any significant item from being revealed at the radio path, generally to ensure the privacy of user-related information.

II. SECURITY FEATURES OF GSM

Several security functions built into GSM to safeguard subscriber privacy which includes:

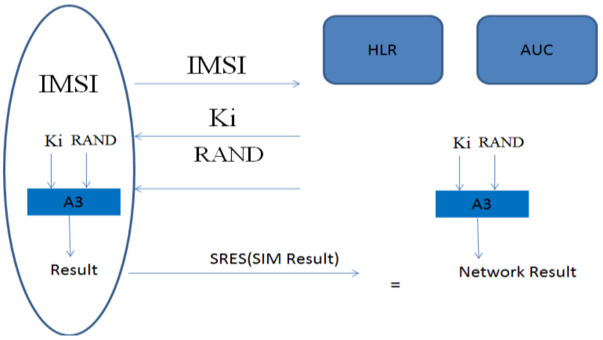
- Registered subscriber's authentication.
- Subscriber identity protection
- Secure data transfer via encryption
- Mobile phones are unworkable without SIM
- Duplicate SIM not allow on the network
- Securely stored KI.

A. Registered subscribers Authentication

The objective of this authentication security feature is to protect the network against unauthorized use. It enables also the protection of the GSM PLMN subscribers by denying the possibility for intruders to impersonate authorized users.

The authentication procedure:

- The MS sends IMSI to the network
- The network receives IMSI and found corresponding KI of that IMSI.
- The network generated 128 bit random number and send to the MS over the air interface.
- The MS calculates a SRES with the A3 algorithm using the given Challenge (RAND) and the KI residing in the SIM.



The authentication is based on a shared secret KI between the subscriber's home network's HLR and the subscriber's SIM.

The KI was generated and then write to the SIM card at a safer place when the SIM card is personalised, and a copy of the key is put to the HLR. When a new GSM subscriber turns on phone for the first time, it's the IMSI which is transmitted to the AuC on the network. Post this; a Temporary Mobile Subscriber Identity (TMSI) is assigned to the subscriber.

The IMSI is infrequently transmitted after this point except it is absolutely necessary.

Manuscript received on April, 2014.

Anshu Anand Jethi, Department of Computer Science and Engineering, Amity University, Noida (U.P) India.

Ajay Rana, Department of Computer Science and Engineering, Amity University, Noida (U.P) India.

This prevents a potential eavesdropper from identifying a GSM user by their IMSI.

B. *Subscriber Identity Protection*

The IMSI (International Mobile Subscriber Identity) is stored in the SIM card. In order to ensure confidentiality of subscriber identity uses the Temporary Mobile Subscriber Identity (TMSI).

Encryption of the data

GSM makes use of a ciphering key to protect both user data and signal on the vulnerable air interface. Once the user is authenticated, the RAND (delivered from the network) together with the KI (from the SIM) is sent through the A8 ciphering key generating algorithm, to produce a ciphering key (KC).

A8 algorithm stores on the SIM card. The KC created by the A8 algorithm which is then used with the A5 ciphering algorithm in order to encipher or decipher the data.

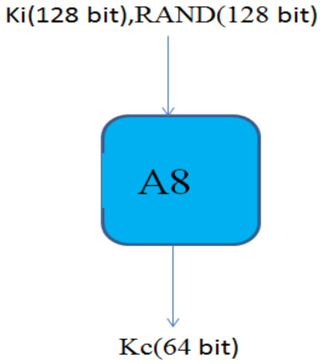


Fig:- 2 Generation of the Session Key

III. THE ALGORITHMS

A3: The MS Authentication Algorithm

The A3 is the authentication algorithm in the GSM security model. The A3 algorithm gets the RAND from the MSC and the secret key KI from the SIM as input to generate the 32-bit output which is the SRES response. The RAND and KI both secret are 128 bits long.

A8, The ciphering Key Generation Algorithm

The A8 algorithm is the session key generation algorithm in the GSM security model. The A8 algorithm takes two 128 bit inputs to generate 64 bit output. This output is 64 bit session key KC. As mentioned above, COMP128 is used for both the A3 and A8 algorithms in most GSM networks.

A5, the stream-ciphering algorithm

The A5 algorithm is used to encrypt over-the-air transmissions. There are three different possibilities for GSM, A5/0 (unencrypted one), use of the A5/1 algorithm or the A5/2 algorithm to secure the data.

IV. PROBLEMS WITH GSM SECURITY

- Security by anonymity, which means all of the algorithms used are not available to the public.
- Difficult to upgrade the mechanisms of cryptographic
- Lack of user visibility (e.g. doesn't know if encrypted or not)
- The flaw of the algorithms.

V. POSSIBLE IMPROVEMENT

Security could be improved in some areas with relatively simple measures. One solution is to use another cryptographically secure algorithm for A3 which would require issuing new SIM-cards to all subscribers and updating of HLR software which would effectively disable the attacker from making exact copies of SIM-cards, the most dangerous attack, which is discussed above. This solution is easy to be implemented because the network operators can make the changes themselves and do not need the support of hardware or software manufacturers or the GSM Consortium. There is now a new algorithms available called COMP128-2.[4]

The operator can employ a new A5 implementation with strong encryption as well. New A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm [7]. This improvement would require the co-operation of the hardware and software manufacturers because they will have to release new versions of their software and hardware that would comprise with the new algorithm.

Third solution would be to encrypt the traffic on the operator's backbone network between the components of network. This would restrict the attacker from wiretapping the backbone network.

This solution also could be implemented without the blessings of the GSM Consortium, but the co-operation of the hardware manufacturers would still be required.

VI. CONCLUSION

Although the GSM network was designed to be a secure mobile system and it did provide strong subscriber authentication and over-the-air transmission encryption, it is now exposed to some attacks targeted at different parts of an operator' s network. One of the main reasons is that some of the algorithms and specifications were accidently losed and studied and some critical errors were found. The A5 algorithm used for encrypting the over-the-air transmission channel is exposed against known-plain-text and divide-and-conquer attacks and the intentionally reduced key space are small enough to make a brute-force attack viable as well. The COMP128 algorithm used in most GSM networks as the A3/A8 algorithm has been proved to have some flaw either.

Although if security algorithms were not broken the GSM architecture still be exposed to attacks from inside which means the attack is targeting the operator's backbone network or HLR.

However, security can be improved in some areas by taking simple measures.

Acronyms

A3
Authentication Algorithm
A5
Ciphering Algorithm
A8
Ciphering Key Generating Algorithm
AUC
Authentication Centre
BS
Base Station
CEPT

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

European Conference of Post and Telecommunication Administrations
ETSI
European Telecommunications Standards Institute
GSM
Group Special Mobile
HLR
Home Location Register
IMSI
International Mobile Subscriber Identity
KC
Ciphering Key
KI
Individual Subscriber Authentication Key
MS
Mobile Station
MSC
Mobile Switching Center
RAND
Random Number
SRES
Signed Response
TMSI
Temporary Mobile Subscriber Identity
VLR
Visitor Location Register

REFERENCES

1. Friedhelm Hillebrand (editor): GSM and UMTS, the creation of Global Mobile Communication, Wiley 2001
2. European Telecommunications Standards Institute, Recommendation GSM 02.17,"Subscriber Identity Module".
3. European Telecommunications Standards Institute, Recommendation GSM 03.20, "Security Related Network Functions".
4. Marie-Bernadette Pautet, Thomas Haug (Foreword by), Michel Mouly, GSM System for Mobile Communication.
5. David Margrave, "GSM Security and Encryption", http://spyhard.narod.ru/phreak/gsmsecur.html.
6. Lauri Pesonen, "GSM Interception", http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/a5/Netsec/netsec.html.
7. Josyula R Rao, Pankaj Rohatgi, Helmut Scherzer and Stefan Tinguely Partitioning Attacks:Or how to rapidly clone some GSM cards", IEEE Symposium on Security and Privacy.