Opu Narcisse,
Graduate student,
Department of Mathematical Information Technology,
University of Jyväsjylä – Finland.

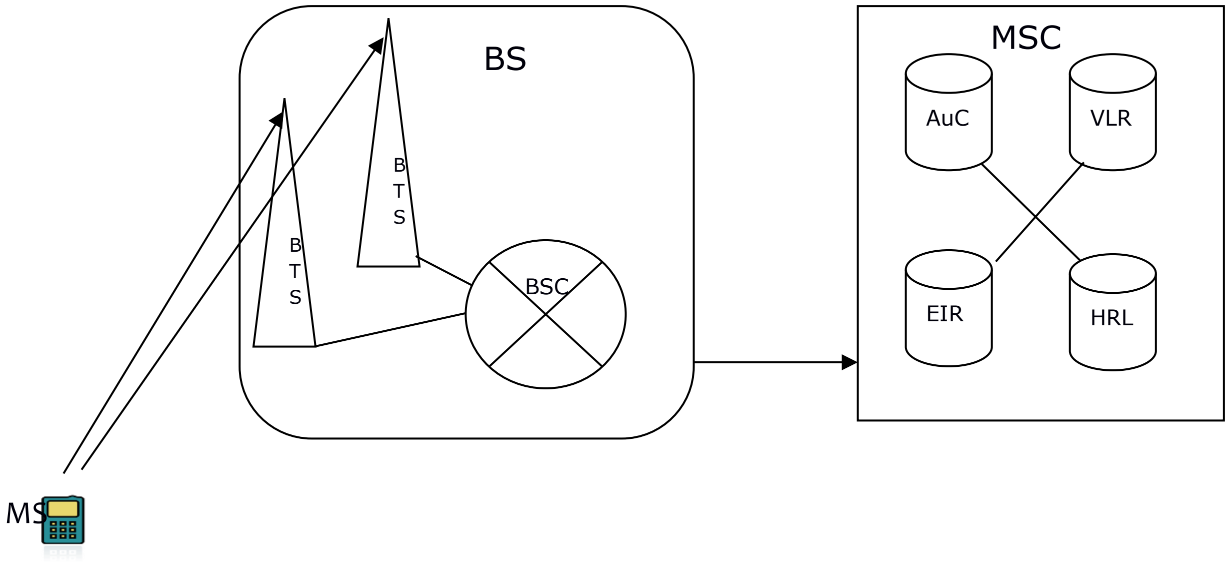
11 November 2012

Security in the Global System for Mobile Communications (GSM)

The Global System for Mobile Communications (GSM) signal was first powered on in Finland in radiolinja's network at 900 MHz in 1991. There were plans since the 1982 by the Conference of European Post and Telecommunication Administrators (CEPT) to develop a pan-European compatible cellular system. Although the CEPT created the Group Special Mobile (GSM) standard, the development was continued by the European Telecommunications and Standards Institute (ETSI) which published the first phase of the GSM standards in 1989 (Gold, 2011). Over the years, the GSM has won the minds and souls billions; it is in use in over 200 countries worldwide and accounts for over 70% of the world's digital market (Gold, 2011).

The architecture of the GSM is hierarchic simple and consists of four main components namely;

- The Mobile Station (MS),
- The Base Station (BS),
- Mobile Switching Centres (MSC)



Mobile Station (MS)

This is the mobile terminal which connects to the Base Station (BS) to let the end user make a call or send data. It uses the International Mobile Equipment Identity (IMEI) to identify every MS. It also uses the Subscriber Identity Module (SIM) card to connect to the network. For security reasons the MS cannot make and receive calls without the SIM. The SIM stores the International Mobile Subscriber Identity (IMSI), the secret key and other user information. This information is protected by the Personal Identity Number (PIN) (Yong, Yin &Tie).

Base Station (BS)

This marks the borderline between the GSM operator's network and the MS. The BS is usually constituted of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BTS is composed of transceiver station which is mounted on poles. BTS define the radio signals and coverage cells through which the MS connects. The BSC controls the BTS, radio-channels and *handoff.* The BSC controls frequency hopping, it may control one or more BTS and connects to the MSC. The BSC modulates the voice channel of the radio link to the standard channel used in the PSTN or ISDN (Yong, Yin &Tie).

Mobile Switching Centre (MSC)

The MSC is the core of the GSM system. It is performs many critical task such as; connects to the Public Switch Telephone Network or Integrated Switch Digital Network, authenticates, registers, update location, handoff and call routing to roaming MS. These critical tasks are processed by subsystems of the MSC, these subsystem are; Home Location Register (HLR), Equipment Identity Register (EIR), Visitor Location Register (VLR) and Authentication Centre (AuC) (Pagliusi, 2002).

All administrative information of registered mobile subscriber within the network such as phone number and IMSI are saved in the HLR. Every GSM network can have one HLR only. The EIR handles all registration of MS within the network by using their IMEI. When a MS is reported stolen or not registered it will be marked invalid, and will not be granted access to the network. The AuC is responsible for granting or revoking access rights to every mobile subscriber. It holds the PIN codes and K1 secret keys. The VLR holds almost identical data as the HLR; some additional dynamic data is collected and stored. This is because the VLR is updated frequently. Additional information held includes the current location and the BS through which the MS is connected. Every MCS has one VLR (Pagliusi, 2002).

GSM Authentication

When a MS with a SIM card wants to connect to a GSM network, it uses only the information which was pre-saved into the SIM card by the GSM operator. The MS sends the IMSI to the BS, the BS forwards it to the VLR, from VLR to the HLR and finally to the AuC. The AuC response with the IMSI, a 128bit random number RAND, 32bit signed response SRES and a secret key K1. This response is forwarded to the VLR by the HLR and only the K1 and RAND are sent to the MS and stored in the SIM card. The MS uses this response to compute the A3 algorithm and generates a signed response SRES which is sent to the VLR. The VLR compares the SRES from the MS and that from HLR, if there is a match, access is granted else revoked. After authentication, the VLR generates an assigns a unique Temporal Mobile Subscriber Identity (TMSI) to the MS and stored in the SIM card. For security reasons, the TMSI is used in the place of IMSI even though not identical. The TMSI will prevent eavesdropper from identifying, tracking MS and be used in used for an identity response within the network (Pagliusi, 2002).

GSM Encryption

Algorithms are used to generate keys and these keys to secure the mobile phone communications and are saved in the SIM card. Algorithms used in mobile phones are A3, A5 and A8 and keys include a ciphering or session key, RAND encipher and secret key (Yon, Yin & Tie). The A8 algorithm uses the RAND and secret keys which had been saved in the SIM card to generate a 64bit session key (Kc) and saved in the SIM card. The A5 algorithm takes the Kc as input and produces the encipher, which is composed the Kc and the number of the frame to be encrypted. Added to this, the A5 algorithm has sub-classes, these sub-classes are A5/0, A5/1, A5/2 and A5/3 algorithms (Pagliusi, 2002).

Before communication begins with the BS, the mobile phone will specify the encryption algorithms it computes, the BS chooses one of the encryption algorithms and secure traffic commences. It is worth noting here that, as the A5 algorithm uses the Kc and the frame to generate the encipher; the key-stream is different for every frame. The Kc might remain same for days, even if the mobile phone is turn off and on. It might only change when the MSC authenticate the MS gain; which is not usually done. GSM networks on the other hand uses the COMP-1228 algorithm for decryption and encryption. The COMP-128 uses both the A3 and A8 algorithms to generate a SRES response and a session key (Yon, Yin & Tie).

A5 Algorithms

There are four sub-sets of the A5 algorithm used in mobile phones today. They have different characteristics and encryption levels; the most secure is the A5/3 followed the A5/1 then the A5/2 and finally the A5/0 which means no encryption. The A5/1 was first developed for the European market and has a time complexity level of 2^54 while the A5/2 which is mostly used in the rest of the world has a time complexity of 2^16 (Yon, Yin & Tie). The A5/3 has been developed already and is part of the 3G specification. The algorithm of the A5/3 encryption has not yet leak, it is pretty secured (Pagliusi, 2002).

GSM Security Breaches

There is no doubt that the GSM is the most secure mobile communication system in recent times. Nevertheless, it has some short comings and security problems. In this section some of these security loop holes in the air interface will be exposed and possible solutions outlined. There has been a number research which have looked at the opposing views on GSM security; whist some researchers focused on the exposing the loop holes in GSM security others concentrated on closing these loop holes. In this section, the security failures of the GSM air interface will be examined and possible solutions brought forth.

One of the most common GSM security problems in the air interface is the one way authentication. This is a fundamental design in the GSM architecture; the GSM network authenticates the MS but the MS does not authenticate the GSM network (Gold, 2011).

Another GSM security problem is the "black box security"; security by obscurity. The specification of the A5 algorithm has never been published. Officially nobody knows how their communication traffic is being encrypted and this is not very good. People like to know what and how their communication traffic is made secured (Yon, Yin & Tie).

It is illegal to clone a mobile phone in many countries, but the practise is still widely common. Mobile phone cloning is a practise where a mobile phone's SIM "A" data is copied into another SIM "B" (Potter, 2004). As the keys and most identifiers are saved in the SIM, the new SIM "B" can now use the network masquerade as SIM A (Goldberg & Briceno, 1989).

There is also the use of the IMSI catcher; commercially called the Virtual Base Transceiver Station (VBTS). This instrument was initially develop to test GSM networks and mobile phones, hackers reversed engineered it and now it can be used to bridge the GSM air interface security. The VBTS has a SIM slut; thus it can use as a MS or Virtual BS or both simultaneously (Deahyun, 2007).

MS have an optimisation feature in their design which allows them to connect to the BS with the highest signal strength. When VBTS is setup in an area where GSM operator's BS are further away, most MS in that area will be induce to connect through the VBTS; this is because it has masqueraded as a BS and has the highest signal strength. The VBTS will then trigger a procedure that will induce the MS to authenticate by sending their IMEI. The IMEI of the MS who had connected through the VBTS will be collected and saved. The VBTS can now be taken offline and the hacker can use the IMEI for eavesdropping or masquerade as the original MS (Deahyun, 2007).

Another scenario with the use of the VBTS is the middle-man attack. This is when the VBTS is fitted with a SIM card; functions simultaneously as MS network and a VBTS. This is a very dangerous situation because it goes undetected for a very long time; MS will continue to communicate normally. While the BTS use A5/1 for encryption, the VBTS will use A5/0 encryption in the air interface with the MS connected through it; encryption levels are decided by the BS. The hacker will collect huge data which he could use as he pleases (Deahyun, 2007).

There is also a problem with COMP-128 algorithm and in 1998 it was announced by Wagner and Goldberg that they had cracked the A3 and A8 algorithms (Potter, 2004). They argued that the session key is only 54bits long as the last 10bits of the 64bits key are not used (Yon, Yin & Tie). It has also been published that A5/2 has been cracked and that A5/1 may have been cracked by Israeli scientists (Pagliusi, 2002).

The android platform also possesses a real security thread, Gold 2011. He continued by stating that over 50 applications were infected by malware in the android market. These malwares are used to steal IMEI (Gold, 2011).

Effects of GSM Security Breaches

As everyone knows, security is one of the most important aspects of our existence and survival. The same notion applies to the GSM security; the air interface is the most vulnerable section of the GSM architecture. One of the most obvious effects will be very huge phone bills for your phone number; for calls made by someone else. Eavesdropping will also be very common in an unsecured GSM network; your communications will be listened to and saved. Another point is that you might be tracked; your movements will be noticed and even save. This is illegal in many countries but because someone got into your phone, tracking will be very easy. Crimes may be committed and they will link to you because the IMEI of your hone was used (Goldberg & Briceno, 1989). There are some ill effects from these loop holes of GSM security; which has triggered researched to make the GSM safer.

Possible GSM Security Fixes

It is word noting that these GSM security loop holes were commonly noticed in the 2G networks. With the coming of the 3G networks, most of these loop holes have been addressed (Deahyun, 2007). Nevertheless, some new GSM security loop holes have emerged and researchers are constantly working to make the GSM saver; it is a constant cycle.

The A5/1 and A5/2 cryptography has been proven not as secure as it is claim. This has led to the development of the A5/3 cryptography standard which uses a 128bit long key (Pagliusi, 2002).

There has also been the development of the Universal Mobile Telecommunications System (UMTS) which gave the MS better security, faster data transfer rates and better coverage. By migrating from the 2G to 3G networks and smart phones, the GSM air interface is made better. The one-way authentication was addressed with the coming of the UMTS. This is because the MS also authenticates the BS. The attacks with the use of the VBTS has been brought under control, nevertheless, smart hackers have developed a smarter version of the VBTS. It can still be use but with less effects (Deahyun, 2007).

Added to this, some smart phones display an orange coloured padlock on the top of their screens. This padlock will indicate when the A5 encryption level being use. The user can now control what is communicated in a secured or unsecured environment (Deahyun, 2007).

The COMP-128 has also been revised; the new version is name the COMP-128-2. The COMP-128-2 was developed to address the security short comings of the COMP-128 which generated session keys which were 54bit long instead of 64bit (Yon, Yin & Tie).

Conclusion

The GSM has been, still is the widely use and the most secure standard for mobile communication. In this paper, the beginnings, architecture and functioning of the GSM were covered; the security problems and possible solutions of the GSM network were also addressed. It is worth noting that with the introduction of smart phones and the android market, the security of mobile phones has risen to a new level. Android applications are compiled and uploaded unto the android market by anybody; this could be potentially infected (Gold, 2011).

A bulk of the literature was concentrated on the air interface security of the GSM network. The most vulnerable section of the GSM network with regards GSM security is the air interface. Many researches and concrete steps has been undertaken to ensure that the GSM security standards are always a step ahead of the hacker.

References

1. European Telecommunications and Standards Institute (2011), “How we work”, available: http://www.etsi.org/WebSite/AboutETSI/HowWeWork/Howwework.aspx [Nov. 09, 2012]
2. Y. Li , Y. Chen, T. Ma, “Security in GSM”, India Institute of Technology Bombay, available: http://www.it.iitb.ac.in/~kavita/GSM_Security_Papers/securityingsm.pdf, [Oct. 01, 2012] .
3. S. Pagliusi (2002), “A Contemporary Foreword on GSM Security”, University of London, available: http://jazi.staff.ugm.ac.id/IC3-Royal%20Holloway/GSM_Security_v4.pdf [Oct. 02, 2012] .
4. D. Strobel (2007 July), “IMSI Catcher”, Chair for embedded security, available: http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf [Oct. 02, 2012]
5. S. Gold (2011 April), “GSM Cracking”, Science Direct, available: http://www.sciencedirect.com/science/article/pii/S1353485811700393, [Oct. 01 2012] .
6. B. Potter (2004 May), “GSM Security”, Science Direct, available: http://www.sciencedirect.com/science/article/pii/S1353485804000777 [Sep. 28, 2012].
7. Goldberg & Briceno (1989 April), “GSM Cloning”, University of California, available: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html [Oct. 01, 2012]
8. S. Deahyun (2007 July), “IMSI Catcher”, Seminararbeit Ruhr-Universit¨at Bochum, available: http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf [Oct. 01, 2012]