Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The GSM Standard (An overview of its security)

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world, accounting for 70% of the world's digital mobile phones. According to a press release by the GSM Association in May 2001, there are more than half a billion GSM mobile phones in use in over 168 countries today. The phenomenal success in mobile telecommunications is due in large to GSM. One of its key strength is its international roaming capability, giving consumers a seamless service in over 168 countries.

Copyright SANS Institute
Author Retains Full Rights

AD
Embed Security Into the Software Development Lifecycle
Sponsored By VERACODE
Download the Report by Securosis

The GSM Standard (An overview of its security)

Introduction

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world, accounting for 70% of the world's digital mobile phones. According to a press release by the GSM Association in May 2001, there are more than half a billion GSM mobile phones in use in over 168 countries today. The phenomenal success in mobile telecommunications is due in large to GSM. One of its key strength is its international roaming capability, giving consumers a seamless service in over 168 countries.

History of GSM

In 1982, the European Conference of Post and Telecommunications Administrations (CEPT) formed a group called Group Spéciale Mobile (GSM) to develop a pan-European cellular system that would replace the many existing incompatible cellular systems already in place in Europe.

In 1987, a milestone was achieved with the signing of the GSM Memorandum of Understanding (MoU) by GSM-operators-to-be, agreeing to implement cellular networks, based on the GSM specifications. While it was clear from the start that GSM would be a digital system, it was officially announced in 1987.

GSM service started in 1991. In the same year, GSM was renamed to Global System for Mobile Communications from Group Spéciale Mobile.

Although GSM was initially developed as a European digital communication standard to allow users to use their cellular devices seamlessly across Europe, it soon developed into a standard that would see unprecedented growth globally. Here in North America, the GSM standard is often referred to as PCS 1900 and elsewhere as DCS 1800. The number relates to the operating frequency of the system.

Key features of GSM

1) International Roaming - single subscriber number worldwide
2) Superior speech quality - better than existing analog cellular technology
3) High level of security - user's information is safe and secure
4) Universal and Inexpensive Mobile handsets
5) Digital Convenience - talk time is doubled per battery life and digital networks can handle higher volume of calls at any one time that analog networks
6) New services - such as call waiting, call forwarding, Short Message Service (SMS), GSM Packet Radio Service (GPRS)
7) Digital compatibility - easily interfaces with existing digital networks i.e. Integrated Services Digital Network (ISDN)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

GSM Architecture

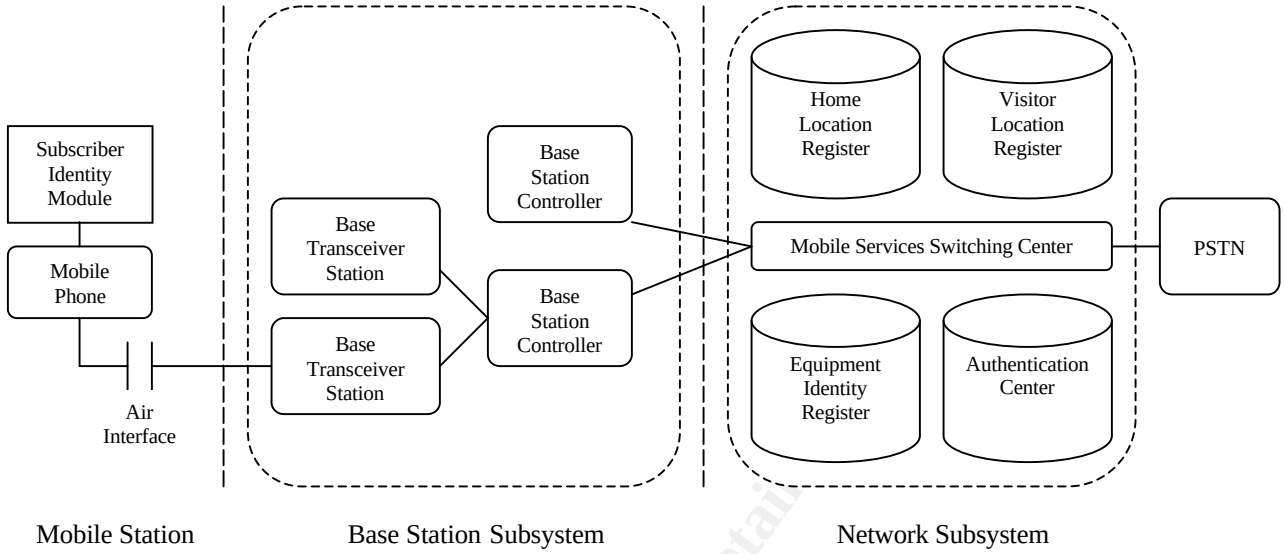

Figure 1: GSM Architecture[1]

Mobile Station

Every GSM mobile phone has a Subscriber Identity Module (SIM). The SIM provides the mobile phone with a unique identity through the use of the International Mobile Subscriber Identity (IMSI). The SIM is like a key, without which the mobile phone can't function. It is capable of storing personal phone numbers and short messages. It also stores security related information such as the A3 authentication algorithm, the A8 ciphering key generating algorithm, the authentication key (K_I) and IMSI. The mobile station stores the A5 ciphering algorithm.

The SIM is removable, which allows users to travel abroad taking with them only their SIM card. They would need to inform their local provider, which countries they would be visiting, prior to their departure. At their destination, they can simply plug the SIM into a rental cellular phone and make use of the mobile unit. The SIM can be protected with a Personal Identification Number (PIN) chosen by the subscriber. The PIN is stored on the card and if entered incorrectly thrice, the card blocks itself. At this point, you'll have to contact your cellular provider who can unblocked your mobile phone, by entering an eight digit Personal Unblocking Key (PUK), which is also stored on the card.

Base Station Subsystem (BSS)

The role of the Base Station Subsystem (BSS) is to connect the user on a mobile phone with other landline or mobile users. The Base Transceiver Station (BTS) is in direct contact with the

[1] Scourias, John "GSM - Global System For Mobile Communications - Figure 1. General architecture of a GSM network" (Static information on website) URL: http://www.smarthomeforum.com/gsm.shtml

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

mobile phones via the air interface and can be thought of as a complex radio modem. The Base Station Controller (BSC) is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manage radio frequencies allocated for the calls through the BTS.

Network Subsystem (NSS)

It is a complete exchange, capable of routing calls from a fixed network via the BSC and BTS to an individual mobile station. The Mobile Services Switching Center (MSC) interconnects the cellular network with the Public Switched Telephone Network (PSTN). The MSC also serves to co-ordinate setting up calls to and from GSM users.

The Home Location Register (HLR) stores information of all subscribers belonging to an area served by a MSC. It stores permanent data such as the IMSI, services subscribed by the user, subscriber's number from a public network, K_I and some other temporary data. The HLR has to provide the MSC with all the necessary information when the call is coming from a public network.

The Visitor Location Register (VLR) contains relevant information for all mobiles currently served by a MSC. The permanent data stored in the VLR is also stored in the HLR. In addition, it also stores the Temporary Mobile Subscriber Identity (TMSI), which is used for limited intervals to prevent the transmission of the IMSI via the air interface. *(See section on GSM Security: Anonymity)* The VLR has to support the MSC during call establishment and authentication when the call originates from a mobile station.

The Equipment Identity Register (EIR) stores all the International Mobile Equipment Identities (IMEI) of mobile equipment and their rights on the network. The EIR maintains a white, gray and black list. Those on the white list are permitted on the network while those on the black list are blocked from the network. The gray list consists of faulty equipment that may pose a problem on the network but are still permitted to participate on the network. The IMEI reveals the serial number of the mobile station, manufacturer, type approval and country of production.

The Authentication Center (AuC) is a protective database that houses the K_I, the A3 authentication algorithm, the A5 ciphering algorithm and the A8 ciphering key generating algorithm. It is responsible for creating the sets of random numbers (RAND), Signed Response (SRES) and the Cipher key (K_C), though the created sets are stored in the HLR and VLR.

GSM Security

As all cellular communications are sent over the air interface, it is less secure than a wired network, as it opens the door to eavesdroppers with appropriate receivers. Several security functions were built into GSM to safeguard subscriber privacy. These include:

- Authentication of the registered subscribers only
- Secure data transfer through the use of encryption
- Subscriber identity protection

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Mobile phones are inoperable without a SIM
- Duplicate SIMs are not allowed on the network
- Securely stored K_I

Authentication

The authentication procedure checks the validity of the subscriber's SIM card and then decides whether the mobile station is allowed on a particular network. The network authenticates the subscriber through the use of a challenge-response method.

Firstly, a 128 bit random number (RAND) is transmitted to the mobile station over the air interface. The RAND is passed to the SIM card, where it is sent through the A3 authentication algorithm together with the K_I. The output of the A3 algorithm, the signed response (SRES) is transmitted via the air interface from the mobile station back to the network. On the network, the AuC compares its value of SRES with the value of SRES it has received from the mobile station. If the two values of SRES match, authentication is successful and the subscriber joins the network. The AuC actually doesn't store a copy of SRES but queries the HLR or the VLR for it, as needed.

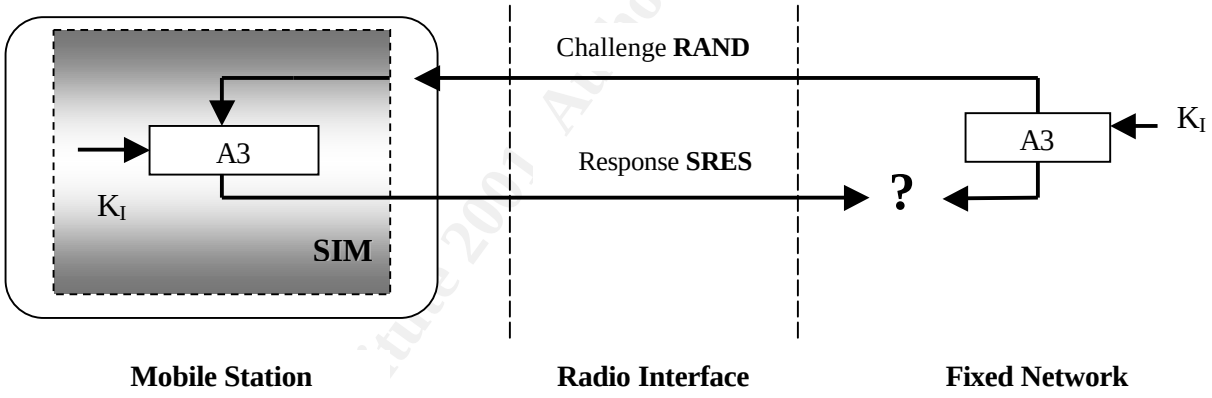

Figure 2: Authentication in GSM [2]

Anonymity

When a new GSM subscriber turns on his phone for the first time, its IMSI is transmitted to the AuC on the network. After which, a Temporary Mobile Subscriber Identity (TMSI) is assigned to the subscriber. The IMSI is rarely transmitted after this point unless it is absolutely necessary. This prevents a potential eavesdropper from identifying a GSM user by their IMSI. The user continues to use the same TMSI, depending on the how often, location updates occur. Every time a location update occurs, the network assigns a new TMSI to the mobile phone. The TMSI is stored along with the IMSI in the network. The mobile station uses the TMSI to report to the

[2] Brookson, Charles "GSM (and PCN) Security and Encryption - Figure 1. Encryption for GSM"
URL: http://www.brookson.com/gsm/gsmdoc.doc

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

network or during call initiation. Similarly, the network uses the TMSI, to communicate with the mobile station. The Visitor Location Register (VLR) performs the assignment, the administration and the update of the TMSI. When it is switched off, the mobile station stores the TMSI on the SIM card to make sure it is available when it is switched on again.

Encryption and Decryption of Data

GSM makes use of a ciphering key to protect both user data and signaling on the vulnerable air interface. Once the user is authenticated, the RAND (delivered from the network) together with the K_I (from the SIM) is sent through the A8 ciphering key generating algorithm, to produce a ciphering key (K_C). The A8 algorithm is stored on the SIM card. The K_C created by the A8 algorithm, is then used with the A5 ciphering algorithm to encipher or decipher the data. The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data on the fly.

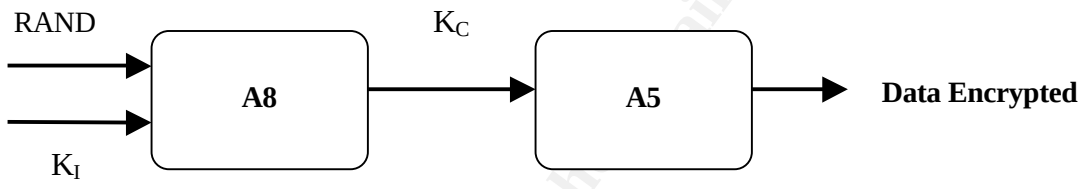

Figure3: Encrypting data using a ciphering key

GSM Algorithms

A consequence of international roaming is the exchange of information between providers in different countries. All countries have strict regulations against the export of encryption algorithms and thus GSM works around it. When a user tries to use his phone in say another country, the local networks request the HLR of the subscriber's home network for the RAND, SRES and K_C which is sufficient for authentication and encrypting data. Thus the local network does not need to know anything about the A3 or A8 algorithms stored in the SIM.

Authentication Algorithm A3 – It is operator-dependent and is an operator option. The A3 algorithm is a one-way function. That means it is easy to compute the output parameter SRES by using the A3 algorithm but very complex to retrieve the input parameters (RAND and K_I) from the output parameter. Remember the key to GSM's security is keeping K_I unknown. While it may sound odd that each operator may choose to use A3 independently, it was necessary to cover the case of international roaming.

Ciphering Algorithm A5 – Currently, there exists several implementations of this algorithm though the most commonly used ones are A5/0, A5/1 and A5/2. The reason for the different implementations is due to export restrictions of encryption technologies. A5/1 is the strongest version and is used widely in Western Europe and America, while the A5/2 is commonly used in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Ciphering Key Generating Algorithm A8 – It is operator-dependent. In most providers the A3 and A8 algorithms are combined into a single hash function known as COMP128. The COMP128 creates K_C and SRES, in a single instance.

Security by Obscurity

Some argue that GSM is not as secure, as publicized. The GSM standard was created in secrecy and all of the algorithms used are not available to the public. Most security analysts believe any system that is not subject to the scrutiny of the world's best minds can't be as secure.

In April 1998, the Smartcard Developer Association (SDA) together with two U.C. Berkeley researchers claimed to have cracked the COMP128 algorithm stored on the SIM. By sending large number of challenges to the authorization module, they were able to deduce the K_I within several hours. They also discovered that K_C uses only 54 bits of the 64 bits. The remaining 10 bits are replaced by zeros, which makes the cipher key purposefully weaker. They feel this is due to government interference. A weaker ciphering key, could potentially allow governments to monitor conversations.

The SDA did have the SIM in their physical presence when they cracked the algorithm. However they fear "an over the air attack" is not far fetched. Unfortunately, they are unable to confirm their suspicions, as the equipment required to carry out such an attack is illegal here in the US.

The GSM Alliance responded to the incident, stating even if a SIM could be cloned it would serve no purpose, as the GSM network would only allow only one call from any phone number at any one time. GSM networks are also capable of detecting and shutting down duplicate SIM codes found on multiple phones.

In August 1999, an American group of researchers claimed to have cracked the weaker A5/2 algorithm commonly used in Asia, using a single PC within seconds.

In December 1999, two leading Israeli cryptographers claimed to have cracked the strong A5/1 algorithm responsible for encrypting conversations. They admit the version they cracked may not be the exact version used in GSM handsets, as GSM operators are allowed to make small modifications to the GSM algorithms. The researchers used a digital scanner and a high end PC to crack the code. Within two minutes of intercepting a call with a digital scanner, the researchers were able to listen to the conversation. Here in the US, digital scanners are illegal. The GSM Alliance of North America has claimed that none of its members use the A5/1 algorithm, opting for more recently developed algorithms.

The ISAAC security research group claims it is technologically possible to build a fake base station for roughly $10,000. This allows a "man-in-the-middle" attack. Essentially, the fake base station can flood the real base station and force a mobile station to connect to it. The base station could then inform the phone to use A5/0 (no encryption) and eavesdrop on the conversation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

An insider attack is another possible scenario. All communication between the Mobile Station and the Base Transceiver Station are encrypted. Beyond that point, all communications and signaling is generally transmitted in plain text within the provider's network. While a strong defense has been put upfront to deter hackers, the inner core is wide open.

Live and Learn

Since the inception of these attacks, the GSM body has been working to patch up the possible security holes. Over the past 12 months, there have been two significant results. Firstly, the compromised COMP128 hash function has been replaced with a patched COMP128-2 hash function. Secondly, a new A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm. While they have chosen not to disclose any pertinent information regarding the currently used algorithms, they have taken a step in the right direction with GSM's replacement, 3GPP. They have moved away from their "security by obscurity" ideology with 3GPP (3rd Generation Partnership Project). All the algorithms being used in 3GPP are available to security researchers and scientists.

Conclusion

Despite the recent security breaches, GSM is by far more secure than previous analog cellular systems and continues to be the most secure public wireless standard in the world.

References:

Business Wire Press release "GSM Alliance Clarifies False & Misleading Reports of Digital Phone Cloning" (April 10, 1998) URL: http://jya.com/gsm042098.txt

Savage, Annaliza "Cell-Phone Security Far From Airtight" (April 13, 1998)
URL: http://www.wired.com/news/technology/0,1282,11630,00.html

Press release "Smartcard Developer Association Clones Digital GSM Cellphones" (April 13, 1998) URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-press.html

Pesonen, Lauri "GSM Interception" (November 21, 1999)
URL: http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/a5/Netsec/netsec.html

McCullagh, Decian "Cell Phone Crypto Penetrated" (December 6, 1999)
URL: http://www.wired.com/news/politics/0,1283,32900,00.html

Goodwins, Rupert "Digital cellphone security broken" (December 7, 1999)
URL: http://news.zdnet.co.uk/story/0,,s2075699,00.html

Robinson, Sara "Cell phone flaw opens security hole" (September 18, 2000)
http://news.zdnet.co.uk/story/0,,t269-s2081469,00.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Robinson, Sara "Design flaw in mobile phone protocol opens security hole" (September 25, 2000) URL: http://www.zdnet.co.uk/itweek/analysis/2000/36/client/gsm

Press release "GSM Mobiles Reach Half A Billion Landmark" (May 11, 2001)
URL: http://www.gsm.org/news/press_2001/press_releases_18.html

3GPP/OP#6 Meeting "ETSI position on A5/3 funding and ownership" (October 9, 2001)
URL: http://www.3gpp.org/ftp/Op/OP_06/Docs/OP6_10.pdf

Webmaster "GSM - Frequently Asked Questions" (Static information on website)
URL: http://www.gsm.org/technology/faq.html

Webmaster "GSM Technology" (Static information on website)
URL: http://www.mobileworld.org/gsm_about.html

Scourias, John "GSM - Global System For Mobile Communications" (Static information on website) URL: http://www.smarthomeforum.com/gsm.shtml

Brookson, Charles "GSM (and PCN) Security and Encryption" (Static information on website)
URL: http://www.brookson.com/gsm/gsmdoc.doc

Webmaster "GSM Security and Encryption" (Static information on website)
URL: http://www.keralaconnect.com/gsm_security_encryption.htm

Wagner, David "GSM Cloning" (Static information on website)
URL: http://www.isaac.cs.berkeley.edu/isaac/gsm.html

Webmaster "GSM - Global System For Mobile Communications" (Static information on website) URL: http://www.iec.org/online/tutorials/gsm/topic03.html

Webmaster "Introduction to GSM" (Static information on website)
URL: http://www.pt.com/products/gsmintro.html

Webmaster "How does a GSM network work?" (Static information on website)
URL: http://www.bryte.net/gsm-hoe.asp

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced