

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

Security of GSM System

By Priyanka Agarwal

Security of GSM System by Priyanka Agarwal

By Priyanka Agarwal
<http://M6.net>

Introduction

Every day millions of people use cellular phones over radio links. With the increasing features, the mobile phone is gradually becoming a handheld computer. In the early 1980's, when most of the mobile telephone system was analog, the inefficiency in managing the growing demands in a cost-effective manner led to the opening of the door for digital technology (Huynh & Nguyen, 2003). According to Margrave (n.d), "With the older analog-based cellular telephone systems such as the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS)", cellular fraud is extensive. It's very simple for a radio hobbyist to tune in and hear cellular telephone conversations since without encryption, the voice and user data of the subscriber is sent to the network (Peng, 2000). Margrave (n.d) states that apart from this, cellular fraud can be committed by using complex equipment to receive the Electronic Serial Number so as to clone another mobile phone and place calls with that. To counteract the aforementioned cellular fraud and to make mobile phone traffic secure to a certain extent, GSM (Global System for Mobile communication or Group Special Mobile) is one of the many solutions now out there. According to GSM-tutorials, formed in 1982, GSM is a worldwide accepted standard for digital cellular communication. GSM operates in the 900MHz, 1800MHz, or 1900Mhz frequency bands by "digitizing and compressing data and then sending it down a channel with two other streams of user data, each in its own time slot." GSM provides a secure and confidential method of communication

Security provided by GSM

The limitation of security in cellular communication is a result of the fact that all cellular communication is sent over the air, which then gives rise to threats from eavesdroppers with suitable receivers. Keeping this in account, security controls were integrated into GSM to make the system as secure as public switched telephone networks. The security functions are:

1. Anonymity: It implies that it is not simple and easy to track the user of the system. According to Srinivas (2001), when a new GSM subscriber switches on his/her phone for the first time, its

Security of GSM System

International Mobile Subscriber Identity (IMSI), i.e. real identity is used and a Temporary Mobile Subscriber Identity (TMSI) is issued to the subscriber, which from that time forward is always used. Use of this TMSI, prevents the recognition of a GSM user by the potential eavesdropper.

2. Authentication: It checks the identity of the holder of the smart card and then decides whether the mobile station is allowed on a particular network. The authentication by the network is done by a response and challenge method. A random 128-bit number (RAND) is generated by the network and sent to the mobile. The mobile uses this RAND as an input and through A3 algorithm using a secret key Ki (128 bits) assigned to that mobile, encrypts the RAND and sends the signed response (SRES—32 bits) back. Network performs the same SRES process and compares its value with the response it has received from the mobile so as to check whether the mobile really has the secret key (Margrave, n.d). Authentication becomes successful when the two values of SRES matches which

enables the subscriber to join the network. Since every time a new random number is generated, eavesdroppers don't get any relevant information by listening to the channel. (Srinivas, 2001)

3. User Data and Signalling Protection:

Srinivas (2001) states that to protect both user data and signalling, GSM uses a cipher key. After the authentication of the user, the A8 ciphering key generating algorithm (stored in the SIM card) is used. Taking the RAND and Ki as inputs, it results in the ciphering key Kc which is sent through. To encipher or decipher the data, this Kc (54 bits) is used with the A5 ciphering algorithm. This algorithm is contained within the hardware of the mobile phone so as to encrypt and decrypt the data while roaming.

Algorithms used to make mobile traffic secure

Authentication Algorithm A3: One way function, A3 is an operator-dependent stream cipher. To compute the output SRES by using A3 is easy but it is very difficult to discover the input (RAND and Ki) from the output. To cover the issue of international roaming, it was mandatory that each operator may choose to use A3 independently. The basis of GSM's security is to keep Ki secret (Srinivas, 2001)

Ciphering Algorithm A5: In recent times, many series of A5 exists but the most common ones are A5/0(unencrypted), A5/1 and A5/2. Because of the export regulations of encryption technologies there is the existence of a series of A5 algorithms (Brookson, 1994).

A8 (Ciphering Key Generating Algorithm): Like A3, it is also operator-dependent. Most providers combine A3 and A8 algorithms into a single hash function known as COMP128. The COMP128 creates KC and SRES, in a single instance (Huynh & Nguyen, 2003).

GSM security flaws

·Security by obscurity. According to (Li, Chen & Ma) some people asserts that since the GSM algorithms are not publicized so it is not a secure system. "Most security analysts believe any system that is not subject to the scrutiny of the world's best minds can't be as secure." For instance, A5 was never made public, only its description is divulged as part of the GSM specification.

Security of GSM System

·Another limitation of GSM is that although all communication between the Mobile station and the Base transceiver station are encrypted, in the fixed network all the communication and signalling is not protected as it is transmitted in plain text most of the time (Li, Chen & Ma).

·One more problem is that it is hard to upgrade the cryptographic mechanisms timely.

·Flaws are present within the GSM algorithms. According to Quirke (2004) " A5/2 is a deliberately weakened version of A5/1, since A5/2 can be cracked on the order of about 216".

Security breaches

Time to time, people have tried to decode GSM algorithms. For instance, according to Issac press release (1998) in April 1998, the SDA (Smartcard Developer Association) along with two U.C Berkeley researchers alleged that they have cracked the COMP128 algorithm, which is stored on the SIM. They claimed that within several hours they were able to deduce the Ki by sending immense numbers of challenges to the authorization module. They also said that out of 64 bits, Kc uses only 54 bits with

zeros padding out the other 10, which makes the cipher key purposefully weaker. They felt government interference might be the reason behind this, as this would allow them to monitor conversations. However, they were unable to confirm their assertion since it is illegal to use equipment to carry out such an attack in the US. In reply to this assertion, the GSM alliance stated that since the GSM network allows only one call from any phone number at any one time it is of no relevant use even if a SIM could be cloned. GSM has the ability to detect and shut down duplicate SIM codes found on multiple phones (Business press release, 1998).

According to Srinivas (2001), one of the other claims was made by the ISAAC security research group. They asserted that a fake base station could be built for around \$10,000, which would allow a "man-in-the-middle" attack. As a result of this, the real base station can get deluged which would compel a mobile station to connect to the fake station. Consequently, the base station could eavesdrop on the conversation by informing the phone to use A5/0, which is without encryption.

One of the other possible scenarios is of insider attack. In the GSM system, communication is encrypted only between the Mobile station and the Base Transceiver station but within the provider's network, all signals are transmitted in plain text, which could give a chance for a hacker to step inside (Li, Chen & Ma).

Measures taken to tackle these flaws

According to Quirke (2004), since the emergence of these, attacks, GSM have been revising its standard to add newer technologies to patch up the possible security holes, e.g. GSM1800, HSCSD, GPRS and EDGE. In the last year, two significant patches have been implemented. Firstly, patches for COMP 128–2 and COMP128–3 hash function have been developed to address the security hole with COMP 128 function. COMP128–3 fixes the issue where the remaining 10 bits of the Session Key (Kc) were replaced by zeroes. Secondly, it has been decided that a new A5/3 algorithm, which is created as part of the 3rd Generation Partnership Project (3GPP) will replace the old and weak A5/2. But this replacement would result in releasing new versions of the software and hardware in order to implement

Security of GSM System

this new algorithm and it requires the co-operation of the hardware and software manufacturers. GSM is coming out of their "security by obscurity" ideology, which is actually a flaw by making their 3GPP algorithms available to security researchers and scientists (Srinivas, 2001).

Conclusion

To provide security for mobile phone traffic is one the goals described in GSM 02.09 specification, GSM has failed in achieving it in past (Quirke, 2004). Until a certain point GSM did provide strong subscriber authentication and over-the-air transmission encryption but different parts of an operator's network became vulnerable to attacks (Li, Chen, Ma). The reason behind this was the secrecy of designing algorithms and use of weakened algorithms like A5/2 and COMP 128. One of other vulnerability is that of inside attack. In order to achieve its stated goals, GSM is revising its standards and it is bringing in new technologies so as to counteract these security holes. While no human-made technology is perfect, GSM is the most secure, globally accepted, wireless, public standard to date and it can be made more secure by taking appropriate security measures in certain areas.

Bibliography

Business Wire Press release (1998). GSM Alliance Clarifies False & Misleading Reports of Digital Phone Cloning. Retrieved October 26th, 2004 Web site: <http://jya.com/gsm042098.txt>

Brookson (1994). Gsm doc Retrieved October 24th, 2004 from gsm Web site: <http://www.brookson.com/gsm/gsm doc.pdf>

Chengyuan Peng (2000). GSM and GPRS security. Retrieved October 24th, 2004 from Telecommunications Software and Multimedia Laboratory Helsinki University of Technology Web site: <http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf>

Epoker Retrieved October 27th, 2004 from Department of Mathematics Boise State University, Mathematics 124, Fall 2004 Web site: <http://math.boisestate.edu/~marion/teaching/m124f04/epoker.htm>

Huynh & Nguyen (2003). Overview of GSM and GSM security. Retrieved October 25th, 2004 from Oregon State university, project Web site: http://islab.oregonstate.edu/koc/ece478/project/2003RP/huynh_nguyen_gsm.doc

Li, Chen & Ma (n.d). Security in gsm. Retrieved October 24th, 2004 from gsm-security Web site: <http://www.gsm-security.net/papers/securityingmsm.pdf>

Quirke (2004). Security in the GSM system. Retrieved October 25th, 2004 from Security Website: [http://www.ausmobile.com/downloads/technical/Security in the GSM system 01052004.pdf](http://www.ausmobile.com/downloads/technical/Security%20in%20the%20GSM%20system%2001052004.pdf)

Margrave (n.d). GSM system and Encryption. Retrieved October 25th, 2004 from gsm-secur Web site: <http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html>

Press release (1998). Smartcard Developer Association Clones Digital GSM (1998). Retrieved October 26th, 2004 from is sac Web site: <http://www.isaac.cs.berkeley.edu/isaac/gsm.html>

Srinivas (2001). The GSM Standard (An overview of its security) Retrieved October 25th, 2004 from papers Web site:<http://www.sans.org/rr/papers/index.php?id=317>

Stallings (2003). Cryptography and Network Security: Principles and practices. USA: Prentice Hall.

A novice trying to create her niche on network of networks

Intruder Alarm Monitoring

By Antony Christie

For complete peace of mind, many people choose to have their intruder alarms monitored. If an alarm is monitored, then, when it detects an intruder it automatically sends a signal via the phone line and/or cellular network to an ARC (Alarm Receiving Centre – these used to be referred to as Central Stations or Monitoring Stations) and the appropriate action is taken. CIA uses Southern Monitoring Services (SMS) Ltd -

New Police/Constabulary Service guidelines (the ACPO Policy on Response to Security - ACPO are the Association of Chief Police Officers of England, Wales and Northern Ireland) state that the Police will now only attend monitored alarms that confirm alarm activations (unless installed pre October 2002).

Confirmation is received when a second detection device is triggered during the same intrusion; therefore, something is definitely on site and moving around.

On receiving the first activation, the ARC will notify a keyholder but if a second detection device is triggered in the same activation, this confirms to the ARC that 'something' is definitely on site and moving around, and the Police are instantly alerted.

If an intruder is detected, a signal is sent from the alarm system using either a standard digital communicator, BT RedCare, BT RedCare GSM or CSL DualComm, via the phone line and/or a cellular network.

A standard digital communicator works by sending signals via the ordinary analogue telephone network, as does BT RedCare, however, with RedCare the ARC are alerted if the phone line fails, either through attack or a genuine line fault, as the line is constantly monitored.

BT RedCare GSM and CSL DualComm send alarm activations via the phone line and a cellular network to for increased security. These forms of signalling are ideal if your insurance company requires your alarm to transmit 'confirmation' signals after a line cut.

Your home is your greatest asset. Why leave it vulnerable when it clearly pays to have your house protected by security professionals.

Christie Intruder Alarms (CIA) Ltd are always delighted to advise on any security related issues from their headquarters in Waterlooville, Portsmouth, Hampshire.

The UK's leading independent security company and the very first to be awarded the prestigious NSI NACOSS Gold Medal. CIA install and service Intruder and Fire Alarms, CCTV, Access Control and Physical Security (Safes, Locks, Fire Extinguishers, Car Park Barriers, etc) for home and business. Visit



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!