

PAPER ON GSM SECURITY

By Mathew Varghese

The purpose for security

All frauds result in a loss to the operator. It is important to recognize that this loss may be in terms of:

- No direct financial loss, where the result is lost customers and increase in use of the system with no revenue.
- Direct financial loss, where money is paid out to others, such as other networks, carriers and operators of 'Value Added Networks' such as Premium Rate service lines.
- Potential embarrassment, where customers may move to another service because of the lack of security.
- Failure to meet legal and regulatory requirements, such as License conditions, Companies Acts or Data Protection Legislation.

TYPES OF PROTECTION

- Protecting the network against unauthorized access.
- Protecting the privacy of the users.

First unauthorized access is achieved by means of authentication. ie, the subscriber identity provided by the mobile station corresponds to the inserted SIM (Subscriber Identity Module). From the point of view of the operator, this function is of paramount importance, in particular in conjunction with international roaming, where the visited network does not control the subscribers record... and his ability to pay.

Preserving the identity of the subscriber is achieved by different means. Transmission can be ciphered to prevent eavesdropping of communications on the radio path. Most of the signaling also be protected in the same way, preventing third parties from knowing who is being called. Finally the replacement of the subscribers identity by a temporary alias also does the same job. Since most of the calls involving a GSM user go through the fixed network, the designers of GSM did not aim at a level of security much higher than that of fixed trunk network. Mechanisms to ensure privacy have only been introduced for the radio path. Within the infrastructure, communications are transmitted in clear text, as they are in PSTN.

It is important to note that at this stage that all the security mechanisms of GSM are under sole control of operators:- the users have no possibility to affect the authentication.

AUTHENTICATION

The simple authentication method is the use of a password (PIN, Personal Identify Number). The level of protection achieved by such a method is very much minimal in radio environment since listening once to the PIN is enough to break the code. To overcome this issue the PIN is locally checked by the SIM. (Subscriber Identity Module). GSM uses a sophisticated method, consisting in a Layman's words, in asking a question that only the right subscriber equipment (SIM) may answer. The question takes a guise of a number called RAND in specifications of GSM, whose value is drawn randomly between 0 and $2^{128}-1$. The answer is called as SRES (Signed RESult) is obtained as the outcome involving a secret parameter specific to the user, called Ki. The secrecy of Ki is the cornerstone on which all security is based. It is stored in a very protected way, without the knowledge of even the subscriber. The algorithm which computes SRES from Ki and Rand is called as A3 in specifications, which is kept very secret by the GSM MoU. The operator can have their own A3 while allowing full inter PLMN roaming.

A3 is done as one way (or trap door) function. This means that the computation of SRES from RAND and Ki should be easy while knowing Ki from SRES and RAND should be as complex as possible. Even with a no SRES, RAND pairs for the same subscriber (same Ki) the computation should remain highly complex.

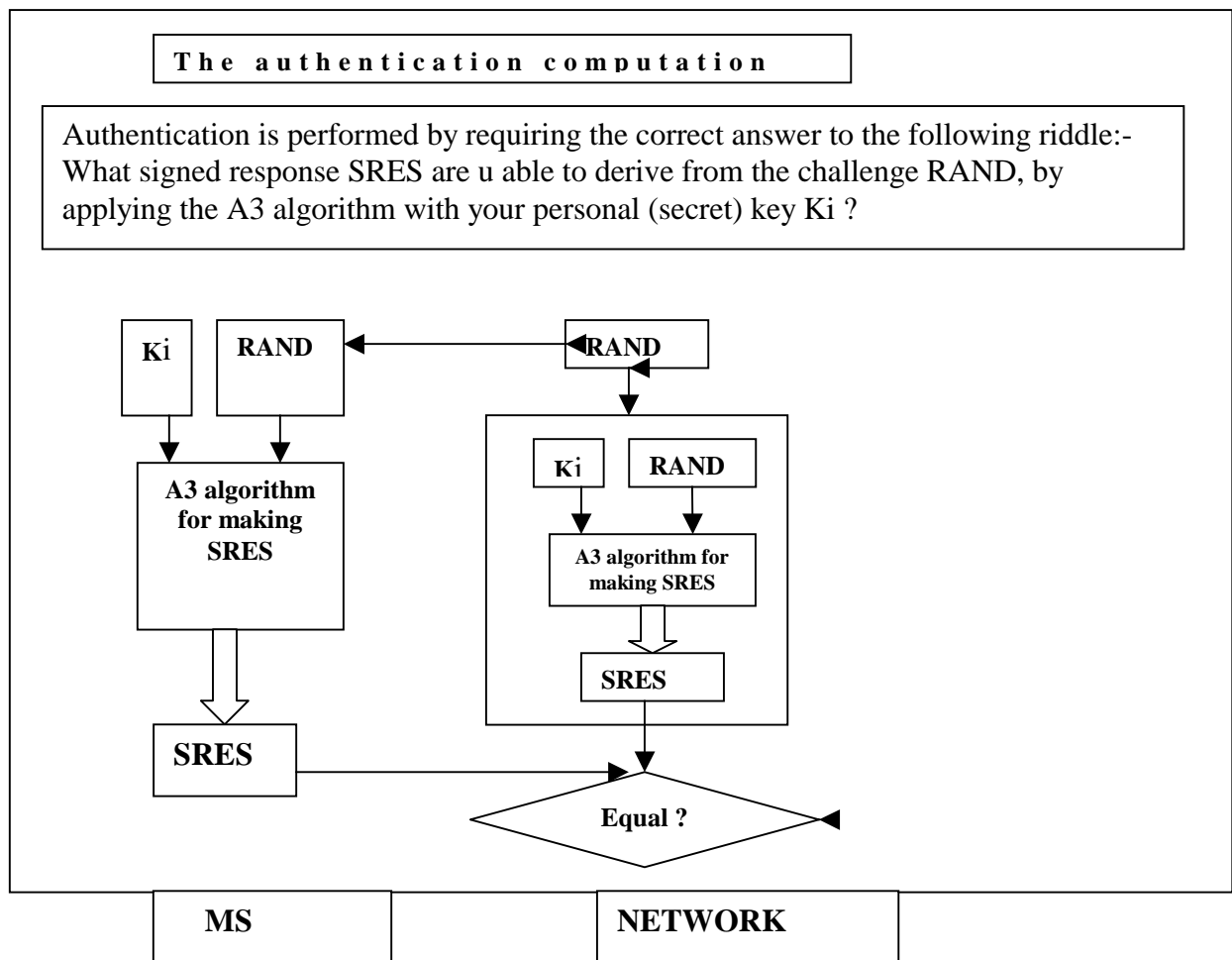
Sizes of keys:-

RAND ----- 128 Bit Long

SRES ----- 32 Bit Long

Ki ----- Operator Dependent, leaves operator good flexibility with a maximum limit of
128 Bits

The choice of A3 algorithm is given to the operator to give maximum security.



In General we can describe the authentication in the following way.

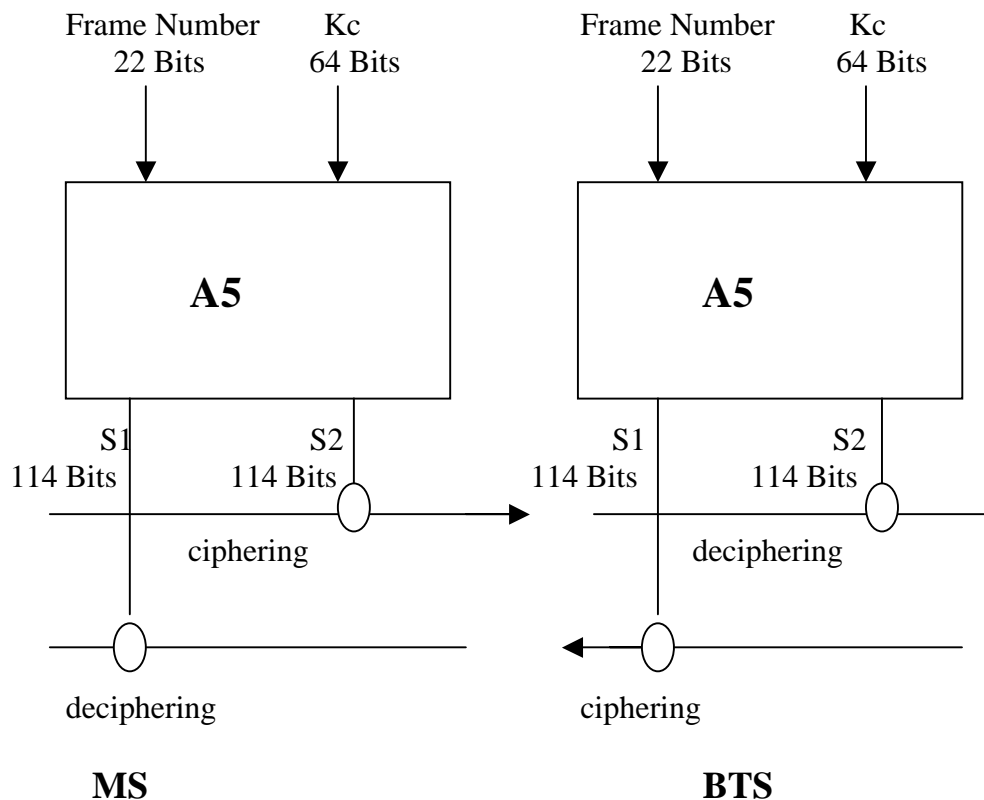
Authentication is initiated by the fixed network, and is based upon a simple challenge-response protocol. When a mobile subscriber (MS) attempts to access the system, the network issues it a random challenge RAND. The MS computes a response SRES to RAND using a one-way function A3 under control of a subscriber authentication key K_i . The key K_i is unique to the subscriber, and is shared only by the subscriber and an authentication center which serves the subscriber's home network. The value SRES computed by the MS is signaled to the network, where it is compared with a pre-computed value. If the two values of SRES agree, the mobile subscriber has been authenticated, and the call is allowed to proceed. If the values are different, then access is denied.

PROTECTING THE PRIVACY OF THE USERS .

In Analog transmission good protection against unauthorized listening is not an easy matter. But in digital transmission permits an excellent level of protection with relatively simple means, with digital cryptography methods. This has been taken advantage of in GSM, where the position of the encryption and deciphering process in the transmission chain allow a single method to be

used for protection of all transmitted data in dedicated mode, whether user information (speech, data...), user related signaling (eg., message carrying the called phone numbers) or even system related signaling (eg., the messages carrying radio measurement to prepare for handover) . So there are only two possibilities.

- 1 . Transmission is protected: everything is encrypted
2. Transmission is not protected: everything is sent in clear text.



A5 derives a ciphering sequence of 114 Bits for each burst independently taking into account the frame number and the ciphering key Kc

Both ciphering as well as deciphering are performed by applying an “Exclusive – Or” function between the 114 coded bits of a radio burst and a 114 bits ciphering sequence generated by a specific algorithm called A5. In order to derive the ciphering sequence for each burst, A5 performs a computation with two inputs, one is the frame number and other with a key named Kc, agreed between mobile station and network. The uplink and downlink directions use two different sequences : for each burst one sequence is used for ciphering in the mobile station and for deciphering in BTS , whereas another one is used for ciphering in the BTS and deciphering in the mobile station. Algorithm A5 must be specified in International level since for achieving MS roaming it must

be implemented in every base station, as well as in every mobile equipment. For the time being as per the GSM MoU a single A5 algorithm is used in all countries. The algorithm is a GSM MoU property and it is tightly copyright protected. It's external specifications are public and it can be described as a black box.

Input of A5 algorithm

Kc ---- 64 Bits
 Frame Number ----- 22 Bits

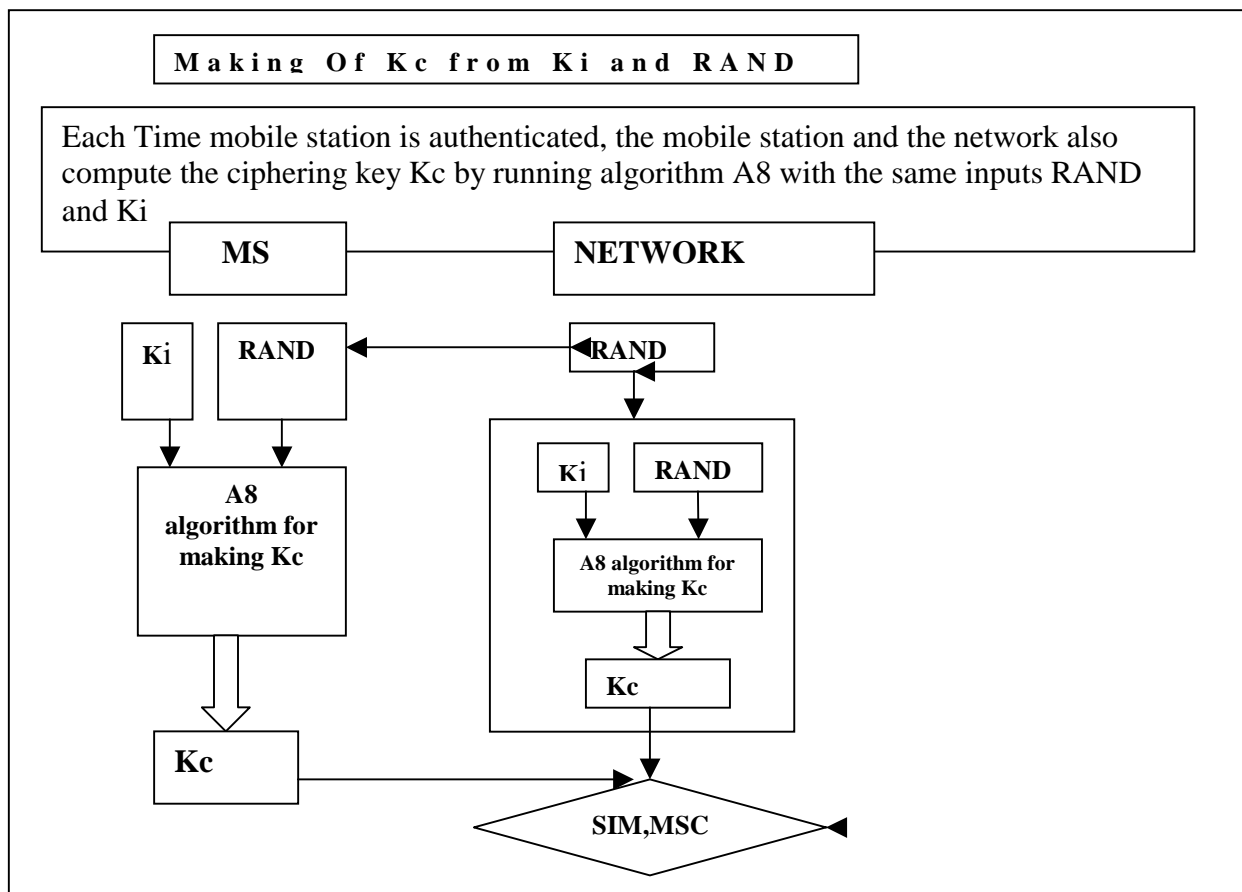
Output of A5 algorithm

S1 --- 114 Bits
 S2 --- 114 Bits

KEY CREATION AND MANEGEMENT

The key Kc must be agreed by the mobile station and the network prior to the start of encryption. The choice in GSM is to compute the key Kc independently from the effective start of encryption, during the authentication process. And then stored in the non volatile memory inside SIM remembered ever after a switch off phase. This dormant key is also stored in the visited MSC/VLR on the network side, and is ready to be used for a start of encryption. When authentication happens while the transmission is ciphered, then the active key Kc being used for ciphering/deciphering is not affected, but the new Kc is stored.

The algorithm used to compute Kc from RAND and Ki is called as A8 in specifications.



The pre-computed triples (RAND, SRES, K_c), held by the fixed networks for a particular subscriber, are passed from the home network's authentication centre to visited networks upon demand. The challenges are used just once. Thus the authentication centre never sends the same triple to two distinct networks, and a network never re-uses a challenge

In practice the two functions A3 and A8 are combined into a single algorithm, called A38 which is used to simultaneously compute SRES and K_c from RAND and K_i . This combined algorithm is referred to as the authentication algorithm. The protocol described above makes it quite clear that this algorithm need only be available to an authentication centre and the mobile subscribers which that authentication centre serves. In particular, there is no need for a common GSM authentication algorithm and different networks may use different algorithms. (The algorithms do, however, need to have the same input and output parameters; in particular, the length of K_c is determined by the GSM cipher algorithm). Never-the-less it is desirable that there is a GSM standard authentication algorithm which may be used by all networks which do not wish to develop a proprietary algorithm. There is just one candidate for such an algorithm; it was proposed by the German administration.

USER IDENTITY PROTECTION

Ciphering with K_c applies only when the network knows the identity of the subscriber it is talking to. Ciphering cannot be applied to common channels. When a mobile moves to a dedicated channel there is some time during which the network does not know the identity of the subscriber. So it is not possible to hide the subscriber's identity at the first authentication process.

Afterwards, protection is obtained by using an identity alias called TMSI (Temporary Mobile Subscriber Identity) which is used instead of the Subscriber Identity (IMSI).

SECURITY FOR THE MOBILE EQUIPMENT MS

(IMEI) International Mobile Equipment Identifier

In GSM the customer subscription and authentication capability is contained within a smart card (SIM, Subscriber Identity Module). Any mobile will take on the identity of a subscriber by insertion of a smart card. The mobiles now become attractive items to steal, as they can be used with another SIM card.

To prevent this, GSM has specified an International Mobile Equipment Identifier (IMEI). Although to an operator, at first evaluation, it may seem as the stolen mobiles have no effect, as

they do not affect a subscription, there will be problems with an increase in customer facing staff to handle esquires, and a possibility that GSM handsets are expensive to insure.

An Equipment Identity Register (EIR) exists in each network, with Black, White and Grey Lists for stolen or non type approved mobiles, valid mobiles and mobiles that need tracking respectively. Grey lists are for local tracking of mobiles within a network.

GSM has defined a procedure so that approved, lost or stolen mobile IMEIs can be communicated to all other operators. A Central Equipment Identity Register has been (CEIR) proposed. Type approval authorities issue white list numbers (random ranges of valid IMEIs) to mobile manufacturers, and manufacturers inform the CEIR when the mobiles are released to market. All operators are able to post their black lists to the CEIR, and in return collect a consolidated list of all operators black and white lists.

By this method stolen or invalid mobiles can be quickly barred throughout the world.

ARCHITECTURE AND PROTOCOLS IN SECURITY MANEGEMENT

The main parts of security management are SIM on the mobile station side, Authentication center AUc which can be seen as part of HLR on the network side. The SIM and AUc are the repositories of Ki of the subscriber. They do not transmit these keys but perform the a3 and a8 algorithms themselves. The AUC is usually implemented as a separate module of HLR because of the security reasons and all of these mechanisms depend upon the secrecy of Key Ki. The AUc is a means to build another layer of protection for the key Ki.

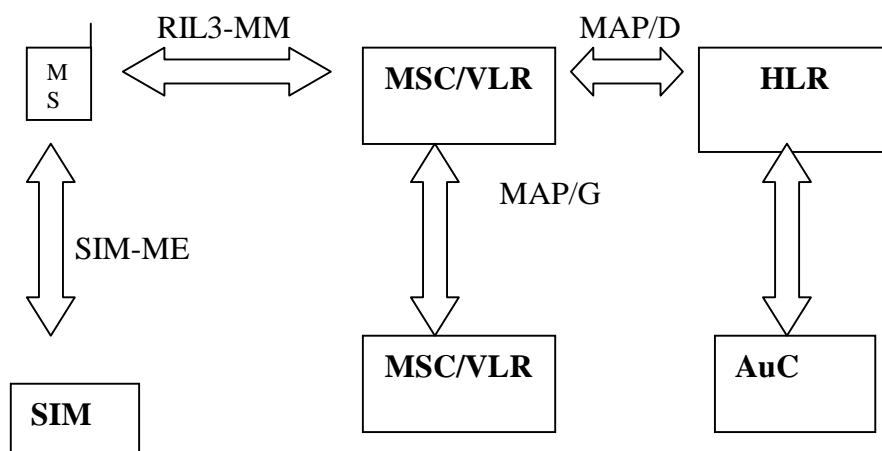
The SIM takes cares of most of the security functions at the Mobile Station side. It stores Ki , it implements the operator dependent A3/A8 and stores the dormant Key Kc. The existence of SIM as a separate physical equipment is indeed one of the elements which gives flexibility in the choice of A3 and A8. The mobile equipment manufactures need not know about this algorithms at all. On the other hand the SIM card manufactures should implement different types of algorithms for each of their operator customers. But completion, mass market production and distribution is entirely different in the SIM manufacturing case since the first level customer is the operator.

The Ki is burnt into the SIM in the initial personalization of the SIM card. Because of the smart card technology it is not easy to read the Ki from the SIM and initial phase is done in the SIM card manufacturing place. So the Ki is given a high level of security. Later Ki is accessed only internally when it has to compute SRES from Ki and RAND. Another advantage of SIM is

that if security requires the operator can issue a new SIM and there by the A3 and A8 algorithms gets updated.

The MSC/VLR plays several small roles. It initiates authentication, it decides to switch to ciphered mode, it checks the SRES provided by the SIM, it stores the dormant key Kc in the network side, and it manages the IMSI.

The security functions are supported by same protocols as location management. The RIL3-MM protocol supports the dialogue between mobile station and the MSC/VLR. Whereas MAP/D is used between MSC/VLR and the HLR.



Security Management Protocols

Security management is coupled with location management and makes use of the same protocols, with two additions. A small protocol to transfer the subscriber Data between MSC/VLR 's called MAP/G. and the connection of AuC to the HLR.

SIGNALLING MECHANISAMS

There are mainly two sections of signaling are done which are MS-MSC and MSC-HLR sections.

MS-MSC procedure.

The authentication procedure between visited MSC/VLR and mobile station consists of two messages. , The RIL3-MM AUTHENTICATION REQUEST from MSC to Mobile station and RIL3-MM AUTHENTICATION RESPONSE from mobile station to MSC giving the SRES for checking in the MSC.

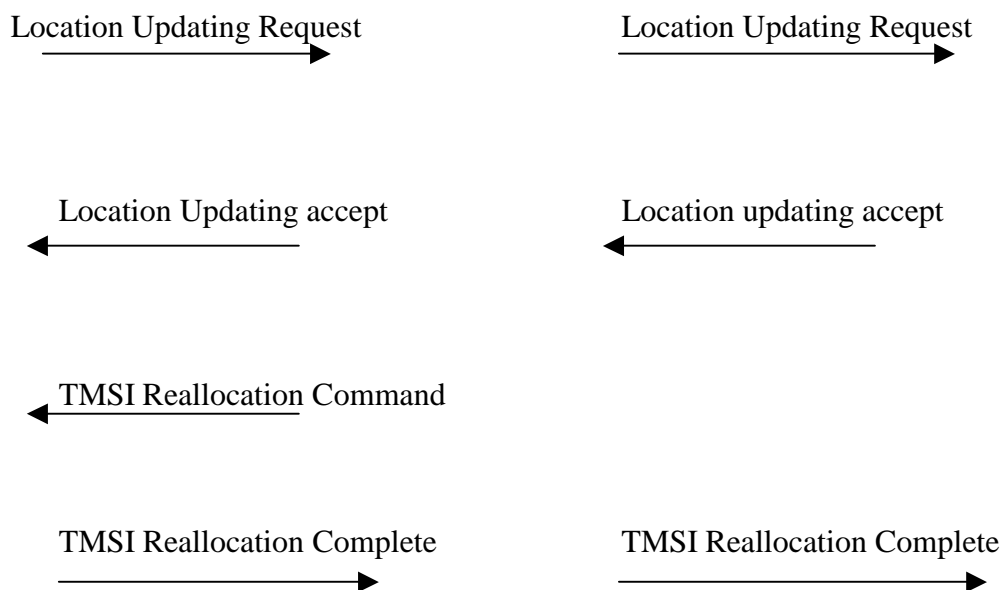
MSC-HLR procedures

The computation of SRES and Kc on the network side, requiring the knowledge of both Ki and A3 and A8 must be performed so that its result is made available in the visited MSC/VLR.

Usually the operators MSC/VLR 's are connected by dedicated high secure lines which can be used for the transmission of keys.

USER IDENTITY PROTECTION DETAILS

The Temporary Mobile Subscribers Identity is an alias for the subscribers identity used in order to avoid sending the IMSI clear on radio path. The TMSI is allocated by the network on a location area basis at a given movement it refers non ambiguously to a subscriber when used in conjunction with the location area identity (LAI). A usual way of updating the TMSI is given below.



TMSI Allocation

A new TMSI can be allocated to a Mobile station through a Standalone procedure consisting of two messages.

Summary

GSM provides a basic range of security features to ensure adequate protection for both the operator and customer. Over the lifetime of a system threat and technology change, and so the security is periodically reviewed and changed. The technical security features must be properly supported by procedures to ensure complete security. The security provided by GSM is well in advance of similar mobile radio systems, and should ensure that it remains at the front of the field for some time to come.

However, it is vitally important that these capabilities are designed in from the start, as they will have an impact on the system requirements. Business cases should show the effect of fraud and the costs of protection.

BIBLIOGRAPHY

Books:

1. **The GSM System for Mobile Communications** :- Michel Mouley & M.B Pautet
Sys 1992
2. **GSM System Security Study** 10-1617-01 10th June 1988 **Racal Research Ltd**
Worton Drive, Worton Grange Industrial Estate, Reading, Berks, England.

Web Sites GSM and Security settings:

1. <http://jya.com/gsm-cloned.htm>
2. [Www.iec.org/gsm](http://www.iec.org/gsm)
3. www.gsmworld.com
4. <http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html>
5. <http://ccnga.uwaterloo.ca/~jscouria/GSM/index.html>

Web Sites GSM algorithms

1. <http://jya.com/crack-a5.htm>
2. www.crackerstown.com/gsm/index.html

Copyright © Mathew Varghese 2001-2005

Written by [Mathew Varghese](#)

Last modified 12/12/01 3:18:18 PM.