International Journal of Engineering and Advanced Technology Studies
Vol.2,No.3,pp.13-19, September 2014
Published by European Centre for Research Training and Development UK (www.eajournals.org)

ALGORITHM-THE EPITOME OF GLOBAL SYSTEM FOR MOBILE COMMUNICATION SECURITY

Miss Asmita Satpute, Miss Snehalata Nampalli
Orchid college of Engineering & Technology (E & TC dept.), Solapur University, Maharashtra, India

Prof. Rahul Bhandari
Orchid college of Engineering & Technology (Mechanical dept.), Solapur University, Maharashtra, India

ABSTRACT— *Global system for mobile communication (GSM) is the largest used operator network. The early phase of this paper deals with the gigantic ken of GSM provided services and various security aspects in order to prevent the services from being deteriorated. But with great power comes great responsibility to be persistent about its level of performance, for the same the GSM association evolved with algorithms. Also the need for security in telecommunication has a shared view in this paper. Nevertheless this paper sets a glance on each of these developed algorithms. Algorithms being a strictly private affair they were never exposed to public, yet the paper makes an effort least to have an informative approach about them.*

KEYWORDS—GSM, Authenticaton, Encryption, Ciphering

INTRODUCTION

The security methods standardized for the GSM System make it the most secure cellular telecommunications standard[1] currently available. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to-end security. The subscriber's anonymity is ensured through the use of temporary identification numbers. The GSM Security is concerned for its responsibilities at both operator as well as customer level; this is done in order to have a seamless service throughout. At the Operator's end, it bills right people in order to avoid fraud and to have protected services. On the other hand at the customers end privacy and anonymity is maintained. Certain precautions are also taken care of like, system does not add significant overhead on call set up, in any scenario increases bandwidth of the channel. This leads to have a network of minimum error rate along with cost effective scheme.

SERVICES BY GSM

The popularity of GSM is due to its services provided.
1) Voice communication
2) Voice mail
3) Short message transmission
4) Data transmission
5) Supplementary services such as call forwarding.

The GSM subscribers are million's in number and significantly increasing, reason being the comfort and compatibility provided to its subscriber. With this, GSM becomes responsible for providing seamless and error free service which gave rise for the implementation of several

algorithms. When the consideration of system elements is established the security mechanisms of GSM are performed in three distinct level of implementation. First Subscriber Identity Module (SIM) wherein the SIM contains the International Mobile Subscriber Identity (IMSI), the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN) [4]. This is followed by the GSM handset containing the ciphering algorithm (A5). And later part is the GSM network wherein the encryption algorithms (A3, A5 and A8) are present.

GSM SECURITY CONCERN

A. Prerequisites maintained are:

1) **Authentication [2] of the registered subscribers only:** the validation of only those users is subscribed who are authorized ones. And this legitimation is done by means of registration wherein the user's need to select a service provider who they think satisfy their communication needs and the usage of services is in budget. A verification task would be performed. Further a positive result of this task connects the subscriber with service provider where he can make use of all services provided.
2) **Subscriber identity protection:** when a service provider has an authorized subscriber by means of some valid documentation few preventive measures are taken to keep his identity a private matter, this is again done by taking into account the security aspect.
3) **Mobile phones are inoperable without a SIM:** a Subscriber Identity Module (SIM) defines the company of service provider which is card shape of 25mm*15mm. These are active only after inserting in reserved in-built structure of handset. There are certain handset also available in market which are reserved for only one specific kind of SIM and do not respond if any other SIM is inserted in them. Until and unless these SIM is inserted inside the phone the communication won't proceed further as there will be null connection between Mobile station (MS) and Base Transceiver Station (BTS).
4) **Duplicate SIMs are not allowed on the network:** when an subscriber gets authenticated, an unique SIM number is allocated to him as a result there would be no two subscribers having same SIM number. If under any circumstances such case exists then, on safety measures the services on both the SIMs are blocked.
5) **Securely stored Ki:** it is the subscriber authentication key which is generated at the beginning of process which usually is a 128 bit key used for authentication of subscriber by the operator. This key is stored in Subscriber's SIM. Further during processing it gets acquainted into Operator's Home Locator Register (HLR)

GROUND LEVEL SECURITY

Subscriber Identity Protection

This is done by Temporary Mobile Subscriber Identity (TMSI) which is preferred over IMSI [5] as a temporary subscriber identifier. TMSI prevents an eavesdropper from identifying the subscriber. TMSI is assigned when IMSI is transmitted to Authentication center (AuC) on the first phone switch on. Every time a location update (new MSC) occurs the network assigns a new TMSI. MS uses TMSI to report to the network during a call initialization, in other words network uses TMSI to communicate with MS. On MS switch off; TMSI is stored on SIM card to be reused next time. In GSM architecture, the Visitor Location Register (VLR) performs assignment, administration and update of the TMSI.

Equipment identity and protection

This is done by International Mobile Equipment Identifier (IMEI) which is independent of SIM and is used to identify stolen or compromised equipment. Also there is Equipment Identity Register (EIR) which is listed as black list, white list and gray list. The equipment's labeled under white list are valid mobiles for which the subscribers are gifted with all the available services. The ones under Gray list are local tracking mobiles for which the service provider keeps a track of their actions. But the things are not as simple for the Black listed equipment's as they indicate stolen or non-type mobiles for which strictly no services are provided.

Central Equipment Identity Register (CEIR)

It gives Approval of mobile type (type approval authorities) and consolidates the black list.

SCHEME'S OF SECURITY

Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (RAND) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber. Note that the individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AuC, HLR and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS. In order to achieve this, there are certain Authentication goals as:

1) Subscriber (SIM holder) authentication this is done to keep a track of secure user's on, an account to test their loyalty towards the service provider. Every SIM can be protected by a Personal Identification Number (PIN). For the security purpose, a four digit code is established which usually gives three attempts before the phone is blocked. Also for bypassing the PIN, the prerequisite is a Pin Unblocking Key (PUK) [6] which is an eight digit code and is set by manufacturer. To unlock this PUK maximum ten attempts are given for the next one the SIM gets permanently blocked.

2) Protection of the network against unauthorized use wherein a strict provision is made for not allowing any services to an unauthenticated subscriber. The last measure of authentication is to create a session key. The architecture of GSM itself has an Authentication center (AuC) whose function is to provide parameters for authentication and encryption functions (RAND, SRES, K_c)

Encryption and Decryption

Further the prime phenomenon involved in security is Encryption. The entire security handling revolves around this term. In technical terms encryption means the process wherein encoding of message, data, information is done. Further a precaution is taken that these encoded bits are received and read only by authorized receiver. Also being advantageous, the encrypted data bits do not intercept. In this encryption the message bits are termed to be plaintext, which is processed by means of encryption algorithm giving rise to cipher text. On majority, the usage of pseudo random encryption key generation algorithm is observed. The cipher text can only

be read after decryption. The details about decryption are discussed further currently. Dealing with encryption has been classified in two prime terms as- Private Key encryption and Public key encryption.

a) **Private Key encryption**: It is also called as Systematic key encryption. In this type the keys allocated for encryption and decryption are same. This provision makes the communication process very easy, the only precaution necessary would be two different entities involved in secret communication must beforehand make sure of having same keys to make the process simplified and error free.

b) **Public key encryption**: This was first evolved in 1973 until then all encryption schemes used were private type. As the name suggests, in this type the encryption keys were made public to all who wish to encrypt message but, only the receiving entity had the decryption key and was eligible to read the encrypted message bits.

Decryption: After encryption we are left out with the cipher text. The process of converting cipher text back to plaintext is nothing but decryption. A measure must be taken that to decrypt a particular piece of cipher text; the key that was used to encrypt the data must only be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.
Dealing with the algorithm prospect, A5 is a stream cipher consisting of three clock-controlled linear feedback shift register (LFSRs) [7] of degree 19, 22 and 23. The clock control is a threshold function of the middle bits of each of the three shift registers. The sum of the degrees of the three shift registers is 64. The 64-bit session key is used to initialize the contents of the shift registers. The 22-bit TDMA frame number is fed into the shift registers. Two 114-bit key streams are produced for each TDMA frame, which are XOR-ed with the uplink and downlink traffic channels.

C. Key Generation: This section focuses on key length as a figure of merit of an encryption algorithm. A machine capable of testing one million keys per second is possible by today's standards. In considering the strength of an encryption algorithm, the value of the information being protected should be taken into account. It is generally accepted that data encryption standard (DES)[8] with its 56-bit key will have reached the end of its useful lifetime by the turn of the century for protecting data such as banking transactions. Assuming that the A5 algorithm has an effective key length of 40 bits (instead of 64), it currently provides adequate protection for information with a short lifetime. A common observation is that the "tactical lifetime" of cellular telephone conversations is on the order of weeks.

Ciphering

When it comes to GSM security Ciphering [3] is one of the most prominent security procedures which are designed with a motive of protecting the subscriber's identity and data bits. When ciphering is active, all information exchanged between the mobile and the network on the dedicated radio channels is encrypted as by means of key wherein this same key is common for both encryption and decryption procedure

GSM ALGORITHMS

The GSM has three distinct algorithms named as A3, A5 and A8. The Confidentiality of these algorithms is a must; their privacy is maintained as much as possible in order to keep their importance sustained.

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 KI) from the output parameters. Remember the key to GSM's security is keeping KI unknown. To summarize its operation one can say, it does generation of SRES response to MSC's random challenge RAND.

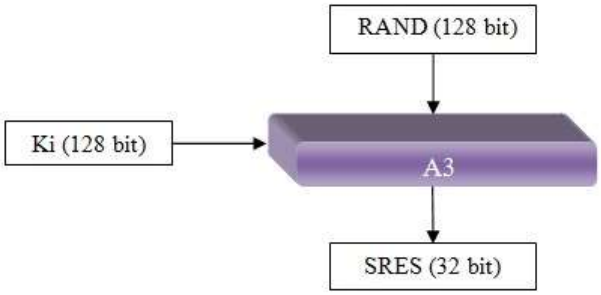

Fig 1. A3 Algorithm

Ciphering Key Generating Algorithm A8

Unlike A3, it is also operator-dependent. In most providers the A3 and A8 algorithms are combined into a single hash function known as COMP128. The COMP128 creates KC and SRES, in a single instance. It does generation of session key Ks. A8 is never a public approach.

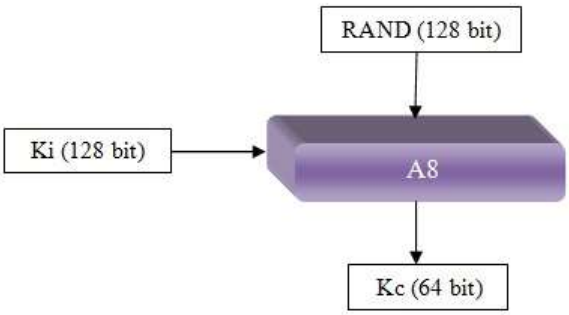

Fig 2. A8 Algorithm

Both A8 and A3 are implemented on SIM. It is the operator who decides which algorithm to use. Hence algorithm implementation is independent of hardware manufacturers and network operators. The logical implementation of A8 and A3 can be represented as:

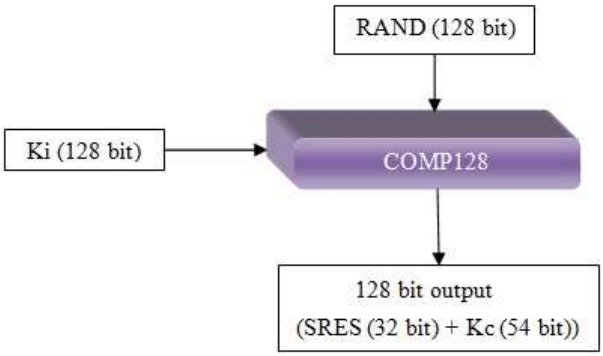

Fig 3. Logical implementation

Comp128

The heart which runs these algorithms is referred as Comp128. Although this algorithm is not revived to public it lags much needed peer review. In spite of keeping it secure, the algorithm went through certain attacks. By certain analysis, the attempts of these attacks occurred to be the first public attack, collision attack and partitioning attack.

Comp128 is the reference algorithm for the task pointed out by GSM consortium. A point to be noted here is, it generates both SRES response and session key Kc on one run. This output gets connected to A5. But if noticed the input to A5 is 64 bits and the key length generated by comp128 is of 54 bits. Hence in order to establish this compatibility there are ten auxiliary zero's appended at the end making it a 64 bit input data. Also in comp128 where security meets mathematics, cryptography comes into picture. The mathematical operations are performed involving compression mechanism. The explanation goes as: There is a 16 bit data which gets compressed and becomes merely of 12 bit. For ψ is the number of bits represented. Then the total number of values present in the stream would be calculated as $(2)^{(9-\psi)}$ (i.e. two to the power $(9-\psi)$). Where as to calculate the total number of bits in each value, divide the $2^{9-\psi}$ resultant by 2 and then compare it with the power of 2. The suitable power represents the number of bits in each value.

Example- For $\psi = 0$.

The total values present $= 2^{9-\psi}$
$= 2^{9-0}$
$= 512$

The number of bits present
in each value $= 512/2$
$= 216$ …… (1)
Power of 2 $= 2^8 = 216$ ……..... (2)

Hence from (1) and (2) we compare and get the number of bits as 8 bits/value.

Ciphering Algorithm A5

Currently, there exist several implementations of this algorithm though the most commonly used are A5/0, A5/1, A5/2 and A5/3. The reason for the different implementations is due to the 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. The A5/3 is its latest variant owned by GSM Association Security Group and 3GPP design and is based on Kasumi algorithm used in 3G mobile systems. The A5 output is 228 bits.

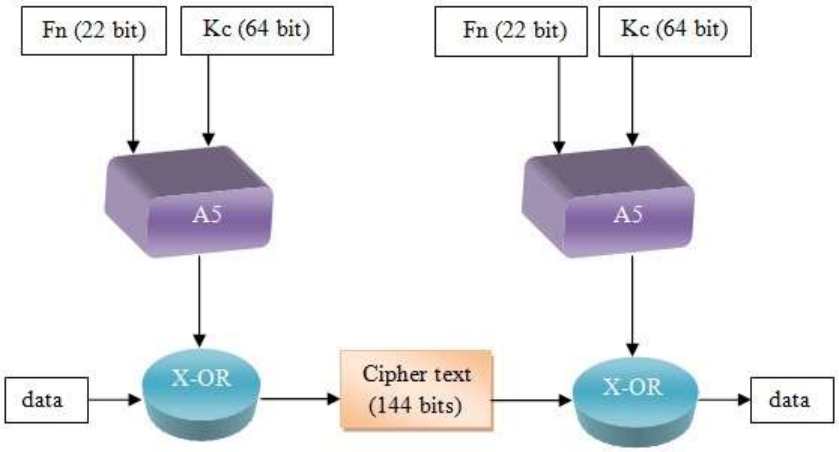

Fig 4. A5 algorithm.

CONCLUSION

In GSM, the security key management is independent of equipment wherein the subscribers can change handsets without compromising security. Also subscriber identity protection is done due to which it is not easy to identify the user of the system intercepting a user data. Nevertheless GSM still serves its legitimated subscribers with seamless services all across the globe.

ACKNOWLEDGMENT

We feel privileged to seek support from our fellow companions, who helped and guided us regarding the pros and cons of the subject, also our guardians for their constant upliftment regarding the work.

REFERENCES

[1] Mobile and personal communication services and sytems, Raj Pandaya
[2] www.teletopix.org/gsm/how-authentication-center-auc-works-in-gsm
[3] www.telecomsource.net › NSN › GSM-EDGE
[4] www.gsmarena.com/glossary.php3?term=pin-code
[5] www.techopedia.com/.../international-mobile-subscriber-identity-imsi
[6] www.phonescoop.com/glossary/term.php?gid=285
[7] www.eng.auburn.edu/~strouce/class/elec6250/LFSRs.pdf
[8] searchsecurity.techtarget.com/definition/Data-Encryption-Standard