Encryption Algorithm Addressing GSM Security Issues- A Review

Mandar M. Kulkarni
Department of Electronics and Communication Engineering
S.S.G.B.C.O.E & T Bhusawal, Maharashtra, India

Prof. A. S. Bhide
Department of Electronics and Communication Engineering
S.S.G.B.C.O.E & T Bhusawal, Maharashtra, India

Prafull P. Chaudhari
Department of Electronics and Communication Engineering
S.S.G.B.C.O.E & T Bhusawal, Maharashtra, India

Abstract- GSM bears numerous security vulnerabilities. Although GSM's architecture is designed in such a way to provide various security features like authentication, data/ signaling confidentiality, and secrecy of a user yet the GSM channel is susceptible to replay, interleaving and man-in-the middle attacks. The GSM speech service is secure up to the point where speech enters the core network. However to achieve end-to-end security it is desired that the GSM subscriber, not the network operator controls the encryption on the speech channel. In this paper we have discussed the best algorithm suited for securing speech in GSM networks.

Keywords- Global System for Mobile Communication (GSM), Data Encryption Algorithm (DES), General Packet Radio Services (GPRS), Advanced Encryption Algorithm (AES).

I. INTRODUCTION

Mobile phones are used on a daily basis by hundreds of millions of users, over radio links. Emerging wireless networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and hence many security issues with the wire-line networks also apply to the wireless environment. The GSM system doesn't provide end-to-end security and lacks in provision of traffic confidentiality to its subscribers. Anonymity, authentication, and confidentiality are the security services which are offered by the world's largest mobile telephony system. Still this system is defenseless against many attacks and fails to ensure taut safety of the user's telephone conversations and data transfer sessions. Confidentiality of transmitted data is achieved by encrypting the information flow between the communicating parties. In GSM networks, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is not sufficient for attaining end-to-end security. As a result, a need for investigating mechanisms for implementing absolute confidentiality of traffic arises [6].

Cryptography is the art of communicating with secret data. In voice communication, cryptography refers to the encrypting and decrypting of voice data through a possibly insecure data line. The goal is to prevent anyone who does not have a "key" from receiving and understanding a transmitted message. GSM employs many cryptographic algorithms for security like A5/1, A5/2 and A5/3. Even so, these algorithms do not provide sufficient level of security for protecting the confidentiality of GSM. Therefore, it is desirable to increase security by additional encryption methods. The modern field of cryptography can be divided into several areas of study. Cryptosystem is a system in which the information is made unintelligible to all but the intended receiver. The process of disguising a message, often referred as plaintext, in such a way as to hide its substance is called encryption. An encrypted message is called cipher text. The process of turning cipher text back into plaintext is called decryption. A cryptographic algorithm, also called a cipher, is a mathematical function for encryption and decryption. The security of algorithm is based on secret key. A cryptosystem consist of an algorithm, all possible plaintexts, cipher texts and keys.

II. GLOBAL SYSTEM FOR MOBILE COMMUNICATION (GSM)

GSM was originally developed in Europe as a replacement for their existing pan- European Cellular phone system. A committee was formed in 1982 to develop a roaming network that provides capacity and privacy. By 1987, eighteen nations made commitments to implement cellular networks based on GSM. Four years later, commercial networks were in place. GSM is now made up of over 745.5 million subscribers in 184 countries. The GSM family is now composed of EDGE, 3GSM, and GPSR [1].

Mobile phones are used on a daily basis by hundreds of millions of users, over radio links. Emerging wireless networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and hence many security issues with the wire-line networks also apply to the wireless environment. Risks in wireless networks are equal to the sum of the risk of operating a wired network plus the new risks introduced by weaknesses in wireless protocols. Thus, wireless mobile communication technology is more vulnerable to security risks than fixed wired technology as monitoring airwaves is a much easier thing to do. Establishment of protective measures that guarantee a state of inviolability from antagonistic acts is an important requirement of wireless communication. Therefore a major concern regarding the safeguard of the subscriber's privacy arises [6].

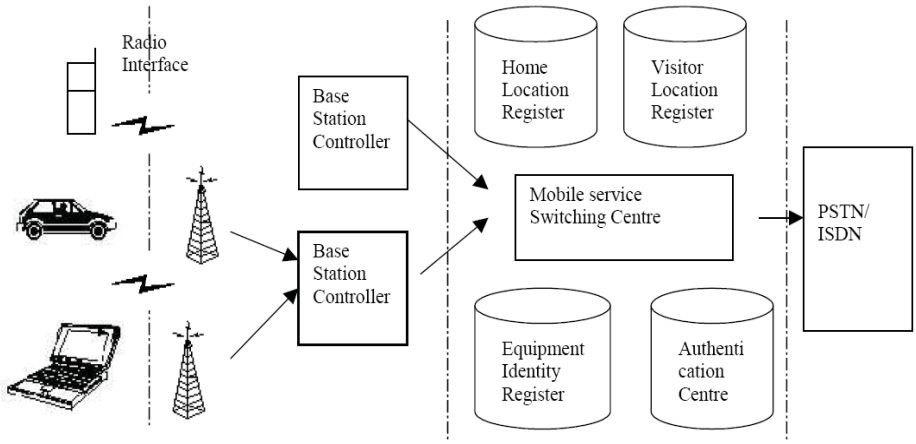

Figure 1. Architecture of GSM

The constraints of security include issues like, the weaknesses and limitations of mobile and communications, the architecture limitations, the user requirements, the contents of provided services, and the evolution of hacking techniques.

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world. According to a press release by the GSM Association recently, there are more than 747.5 million subscribers in over 184 countries today by the time of September 2002, accounting for 71.2% of the World's digital market and 69% of the World's wireless market.

The number of subscribers worldwide is expected to surpass one billion by the end of 2003. The name GSM first comes from a group called Group Special Mobile (GSM), which was formed in 1982 by the European Conference of Post and Telecommunications Administrations (CEPT) to develop a pan-European cellular system that would replace the many existing incompatible cellular systems already in place in Europe. But when GSM service started in 1991, the abbreviation "GSM" was renamed to Global System for Mobile Communications from Group Special Mobile. The typical architecture of GSM network was shown in figure 2.1 The GSM network can be divided into three parts. The Mobile Station carries the subscriber; the Base Station Subsystem controls the radio link with the Mobile Station; the Network Subsystem, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. Not shown is the Operations and Maintenance center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the air interface or radio link. The Base Station Subsystem and the Network Subsystem are also called the fixed network [5].

2.1 What is Necessity?

All frauds result in a loss to the operator. It is important to recognize that this loss may be in terms of:
1) No direct financial loss, where the result is lost customers and increase in use of the system with no revenue.
2) 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.
3) Potential embarrassment, where customers may move to another service because of the lack of security.
4) Failure to meet legal and regulatory requirements, such as License conditions, Companies Acts or Data Protection Legislation.

2.2 Descriptions of the functions of the security services-

1) Anonymity: So that it is not easy to identify the user of the system. Anonymity is provided by using temporary identifiers. When a user first switches on his radio set, the real identity is used, and a temporary identifier is then issued. From then on the temporary identifier is used. Only by tracking the user is it possible to determine the temporary identity being used.

2) Authentication: So the operator knows who is using the system for billing purposes. Authentication is used to identify the user (or holder of a Smart Card) to the network operator. It uses a technique that can be described as a "Challenge and Response", based on encryption. Authentication is performed by a challenge and response mechanism. A random challenge is issued to the mobile, the mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, the response to the challenge is correct. Eaves dropping the radio channel reveal no useful information, as the next time a new random challenge will be used. Authentication can be provided using this process. A random number is generated by the network and sent to the mobile. The mobile use the Random number R as the input (Plaintext) to the encryption, and, using a secret key unique to the mobile *Ki,* transforms this into a response Signed Response (SRES) (Cipher text) which is sent back to the network. The network can check that the mobile really has the secret key by performing the same SRES process and comparing the responses with what it receives from the mobile.

3) Signaling Protection: So that sensitive information on the signaling channel, such as telephone numbers, is protected over the radio path.

4) User Data Protection so that user data passing over the radio path is protected [16].

2.3 Objectives of security services

The objective of security for GSM system is to make the system as secure as the public switched telephone network. The use of radio at the transmission media allows a number of potential threats from eaves dropping the transmissions. It was soon apparent in the threat analysis that the weakest part of the system was the radio path, as this can be easily intercepted. The GSM MOU Group produces guidance on these areas of operator interaction for members. The technical features for security are only a small part of the security requirements [16].

III. SYSTEM DESIGN

Figure shows our proposed system. Security has become an essential topic in current mobile and wireless networks. As the security procedures for such networks elevates, the tools and techniques used to attack such networks also increases. Wireless communications security is the measures or methods used to protect the communication between certain entities. To protect the entity from any third party attacks, such as revealing a particular identity, data modification or data-hijacking, eavesdropping, impersonating an identity, Protection mechanisms are used.

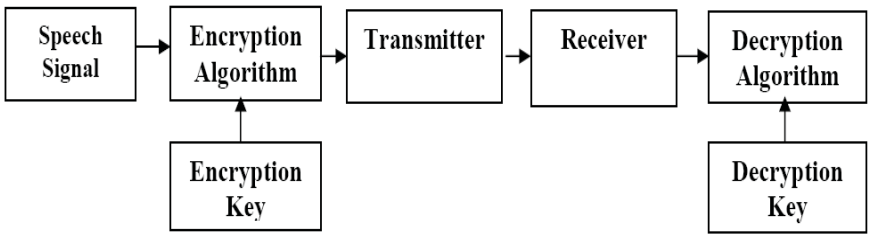

Figure 2. Block diagram of proposed system.

There are several ways of classifying cryptographic algorithm. Since IT security became a growing market in the past, there are a lot of different standards to choose from. Here is a list of some famous ones:

1. DES (Data Encryption Standard)
2. AES (Advanced Encryption Standard) / Rijndael
3. FEAL (Fast Data Encryption Algorithm)
4. IDEA (International Data Encryption Algorithm)
5. SAFER (Secure and Fast Encryption Routine)
6. RC5 (Rivest's Code 5) and RC6 (Rivest's Code 6)

3.1 Data Encryption Standard (DES)-

It is a block cipher with key length 56 bits. It was designed by IBM in 1976 for the National Bureau of Standards (NBS), with approval from the National Security Agency (NSA). It had been used as a standard for encryption until 2000. From 2001 the AES will replace DES. After 25 years of analysis, the only security problem with DES found is that its key length is too short. DES uses a 56 bit key which can be broken using brute force methods, & is now considered to be insecure for many application. This is chiefly due to the 56 bit key size being too small. DES keys have been broken in less than 24 hours. A 16 cycle Feistel system is used, with an overall 56 bit key permuted in to 16, 48 bit sub key, one for each cycle. To decrypt the identical algorithm is used, but the order of sub key is reversed. DES was up for a 5 year review by NIST in 1992 and the decision was made to keep it as a standard (to the surprise of many), but at its next review in 1997 it was clear that it was going to be replaced. Some expected it not to remain a standard after this review, but due to NIST's activities concerning the new AES (Advanced Encryption Standard) the decision was made to keep DES as the standard (but only triple DES was to be considered secure). On Dec. 4, 2001, Secretary of Commerce Don Evans announced the approval of AES as the new standard, replacing DES. Products implementing the AES are now available in the marketplace. [7], [8].

3.2 Fast Data Encryption Algorithm (FEAL)-

In cryptography, FEAL is a block cipher proposed as an alternative to the Data Encryption Standard (DES), and designed to be much faster in software. The Feistel based algorithm was first published in 1987 by Akihiro Shimizu and Shoji Miyaguchi from NTT. The cipher is susceptible to various forms of cryptanalysis, and has acted as a catalyst in the discovery of differential and linear cryptanalysis. There have been several different revisions of FEAL, though all are Feistel ciphers, and make use of the same basic round function and operate on a 64-bit block. One of the earliest designs is now termed FEAL-4, which has four rounds and a 64-bit key. It was designed for implementation on 8 bit or 16 bit microprocessor [19].

3.3 International Data Encryption Algorithm (IDEA)-

International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991. It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem. IDEA was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies. It is also interesting in that it entirely avoids the use of any lookup tables or S-boxes. It operates on 64 bit blocks using 128 bit key, common method to break IDEA is checking for weak key IDEA is immune under certain assumptions against differential cryptanalysis attack. No successful linear or algebraic weaknesses have been reported. As of 2004, the best attack which applies to all keys can break IDEA reduce to 5 rounds only. A brute force attack is as well possible, but since it uses a longer key, 128 bit, brute force is less time efficient. A very common method to break IDEA is, checking for weak keys, which exist because of the way how IDEA works. IDEA encrypts a 64-bit block of plaintext to 64-bit block of cipher text. It uses a 128-bit key. The algorithm consists of eight identical rounds and a "half" round final transformation [17].

3.4 Secure and Fast Encryption Routine (SAFER)-

SAFER is based on the existing SAFER family of ciphers, which comprises the ciphers SAFER K-64, SAFER K-128, SAFER SK-64, SAFER SK-128, and SAFER SK-40. The block size of all the ciphers in the existing SAFER family is 64 bits, while the key length is 40 or 64 or 128 bits as indicated in the name of the cipher. The ciphers in the existing SAFER family are non-proprietary ciphers and were designed by Prof. James L. Massey of the ETH Zurich (Swiss Federal Institute of Technology, Zurich) at the request of Cylink Corporation. The first of these ciphers, SAFER K-64, was publicly announced at the Dec. 9--11, 1993, Fast Software Encryption workshop in Cambridge, England. The other ciphers in the SAFER family differ from SAFER K-64 only in their key schedules and in the number of rounds used. The 8 rounds of SAFER (with a 128-bit key) provide an enormous margin of

safety against an attack by linear cryptanalysis. No proof of complete security & Encryption/Decryption Dissimilarity [18].

3.5 Advanced Encryption Standard (AES) / RIJNDAEL-

The Advanced Encryption Standard (AES), the block cipher ratified as a standard by National Institute of Standards and Technology of the United States (NIST), was chosen using a process lasting from 1997 to 2000 that was markedly more open and transparent than its predecessor, the aging Data Encryption Standard (DES). AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits 8 called AES-128, AES-192, and AES-256, respectively. AES- 128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds [21].

The most successful attack on AES to date is the "Square Attack" based on the Square Cipher, which was also created by the authors of Rijndael. It "exploits the byte-oriented structure of Square cipher. This attack is also valid for Rijndael, as Rijndael inherits many properties from Square."The Square Attack is faster than a brute force attack for AES using six rounds or less. For seven rounds or more, brute force attacks are the fastest known attacks. AES uses 10–14 rounds, based on the key length. Brute forcing AES-128 (smallest key length) is unlikely to be practical in the foreseeable future. According to NIST, "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key."[21]

3.6 Rivest's Code 5 (RC 5) and Rivest's Code 6 (RC 6)-

RC5 is a block cipher notable for its simplicity. Designed by Ronald Rivestin 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.RC5 encryption algorithm, a fast symmetric block cipher suitable for hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a variable-length secret key. RC5 should be a symmetric block cipher. The same secret cryptographic key is used for encryption and for decryption. The plaintext and cipher text are fixed-length bit sequences (blocks). RC5 should be suitable for hardware or software. This means that RC5 should use only computational primitive operations commonly found on typical microprocessors. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive. RC5 also consists of a number of modular additions and exclusive OR (XOR)s. The general structure of the algorithm is a Feistel-like network. The encryption and decryption routines can be specified in a few lines of code. The key schedule, however, is more complex, expanding the key using an essentially one-way function with the binary expansions of both e and the golden ratio as sources of "nothing up my sleeve numbers". The tantalizing simplicity of the algorithm together with the novelty of the data-dependent rotations has made RC5 an attractive object of study for cryptanalysts 12-round RC5 (with 64-bit blocks) is susceptible to a differential attack using 244 chosen plaintexts. 18-20 rounds are suggested as sufficient protection [20].

IV. Discussion Regarding Proposed Work

The Advanced Encryption Standard (AES- Rijndael) is a symmetric-key cipher with a simple and elegant algebraic structure, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the key length can be 128, 192, or 256 bits and the number of rounds N_r is 10, 12 or 14 respectively. The 128-bit data block is divided into 16 bytes that are mapped to a 4 × 4 array called the State, and all the internal operations of the Rijndael algorithm are performed on the State. In the encryption of the AES-Rijndael algorithm, each round except the final round consists of four iterative transformations: the Sub Bytes, the Shift Rows, the Mix-Columns, and the Add Round Keys, while the final round does not have the Mix Columns transformation. The data are placed in an $4\times N_b$ block length array of elements of $GF(2^8)$ which is Galois Field defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. The encryption of each block of data involves an initialization phase, (N_r-1) iterations of the basic encryption processing and a finalization round: Sub Bytes is a non-linear byte substitution, operating on each of the state bytes independently, composed by the multiplicative inverse in $GF(2^8)$ (0 mapped onto itself) and a fixed affine transformation over $GF(2^8)$; Shift Rows cyclically shifts the elements of the i^{th} row of the state C_i elements to the right, where C_i are fixed constants; In Mix Columns the columns of the state are considered as polynomials over $GF(2^8)$ and multiplied modulo $x^4 +1$ by a fixed polynomial; and Add Round Key is a XOR of the key (after the scheduling) with the array. The key schedule for AES-Rijndael is a simple expansion using XOR and cyclic shifts, and consists of two components: Key Expansion and round key

selection. The application in the scheduling scheme of Sub Bytes ensures the non-linearity, without adding much more space requirements on an 8-bit processor. Key Expansion depends on the value of N_k (key length/32) [22].
AES-Rijndael is suitable on all aspects and future research in optimization techniques will definitely make it the de facto encryption for resource constrained wireless networks. RC5 is good on the code point of view, but the key schedule consumes more time [22].

V. CONCLUSION

In this paper, we focus on the security of the Global System for Mobile communication (GSM) networks. 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. GSM is the most commonly used system for mobile communications. Lack of security and privacy are the major issues of GSM that need to be addressed. Various encryption techniques exist that aim to make the GSM system secure and confidential.
Now days there are many situations to keep voice secret in voice communication. This can be achieved by voice encryption by using different encryption algorithms. In the proposed architecture, we use Symmetric Ciphers for speech encryption and decryption. AES-Rijndael is suitable on all aspects and future research in optimization techniques will definitely make it the de facto encryption for resource constrained wireless networks.

REFERENCES

[1] Mohsen Toorani & Ali Asghar Beheshti Shirazi "Solutions to the GSM Security Weaknesses" The Second International Conference on Next Generation Mobile Applications, Services, and Technologies.
[2] Tuan Huynh and Hoang Nguyen "Overview of GSM and GSM Security".
[3] Hongyu Lei, Yu Zhao, Yuewei Dai, Zhiquan Wang "A Secure Voice Communication System Based on DSP" 2004 8th International Conference on Control, Automation, Robotics and Vision Kunming, China, 6·9th December 2004.
[4] Chi-Chun Lo and Yu-Jen Chen" Secure Communication Mechanisms for GSM Networks" IEEE.
[5] Rekha. A. B, Umadevi B, Yogesh Solanke and Snnivasa Rao Kolli End-to-End Security for GSM Users."
[6] Saad Islam and Fatima Ajmal "Developing and Implementing Encryption Algorithm for Addressing GSM
[7] B.Rajesh "Real Time Implementation of DES Algorithm By Using TMS3206713 DSK"
[8] Khaled Merit and Abdelazziz Ouamri "Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.
[9] Cryptography & Network Security by "William Stallings" 4th Edition.
[10] Eric Conrad "Types of Cryptographic Attacks
[11] Daniel J. Bernstein "Understanding brute force"
[12] Hannes Kruppa & Syed Umair Ahmed Shah "Differential & Linear Cryptanalysis in Evaluating AES Candidate Algoritms".
[13] Pascal Junod "Linear Cryptanalysis of DES".
[14] Kazuo Ohta and Kazumaro Aoki Linear Cryptanalysis of the Fast Data Encipherment Algorithm.
[15] John Kelsey Bruce Schneier & David Wagner "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES.
[16] Charles Brookson GSM (and PCN) Security &Encryption.
[17] M. BramhajiRao "Classification of RSA & IDEA Ciphers".
[18] James L. Massey "SAFER K-64 A Byte Oriented Block-Ciphering Algorithm."
[19] Akihiro Shimizu & Shoji Miyaguchi "Fast Data Encryption Algorithm FEAL."
[20] Ronald L. Rivest MIT Laboratory for Computer Science 545 Technology Square, Cambridge, Mass. 02139 "The RC5 Encryption Algorithm."
[21] Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the Advanced Encryption Standard.
[22] "Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security" by M. Razvi Doomun and KMS Soyjaudah International Journal of Network Security, Vol.9, No.1, PP.82–94, July 2009