IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

An Analysis of Global System for Mobile Communication Security and Encryption

Tushar Mehrotra, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- tushar.cs17@nitp.ac.in

ABSTRACT: ***The Global System for Mobile Communication (GSM) is riddled numerous security flaws, and although it was built with authenticating, signaling confidentiality, and user seclusion as encryption techniques, the GSM channel is still vulnerable to relay, interleaving, and man-in-the-middle attempts. Prior to voice accessing the core network, the GSM communication service is secure. To provide end-to-end security, it is preferable that the GSM subscriber, rather than with the network operator, controls your voice channel's encrypting. At the user's perspective, a new method of encryption is introduced. In this paper, the author uses DSP-Starter-Kit (DSK) to demonstrate our cryptographic techniques on the GSM communication system in real-time. With our technology, the speech is scrambled before it reaches the GSM device, increasing safety and confidentiality. Given that the communicating GSM subscribers' encrypted message is personal to them, the GSM channel will indeed be secret to them. The system's DSK board served as a standalone product that carried out the encryption system. To assess the system's performance in terms of its own performance and latency frequency, real-time tests have been carried out.***

KEYWORDS: ***Ciphering, Data Encryption, GSM Security, Mobile Communication, Network System.***

1. INTRODUCTION

Hundreds of thousands of people use mobile phones every day during radio connections. Many of the other features of existing wire-line networks, including public switch telephone/data networks, that emergent wireless networks share also pertain to the wireless environment, including several security challenges. The risk of maintaining a wired network and other hazards brought on by weaknesses in wireless protocols are equivalent the risk in wireless networks. Therefore, however to the ease of monitoring airwaves, wireless digital communication is more subject to security issues than fixed cable technologies [1]. An essential need for wireless communication is the development of safeguards and provide an environment free from hostile actions. As a consequence, there is a serious issue concerning protecting consumer privacy. The restrictions of infrastructure, the user needs, the substance of the services offered, and the progression of hacking methods are now only a few examples of the variables that impact security. End-to-end security and indeed the provision of traffic anonymity to subscribers are both inadequate in the GSM system [2]. The biggest mobile telephone system in the world combines the security services comprising anonymity, verification, and secrecy. Still, this system is ineffective against several threats therefore falls short of providing full protection for user phone calls and information transmission sessions.

The communication process between the sender and recipient is encrypted to maintain the confidentiality of the sent data. In GSM networks, communication has been sent in clear-text

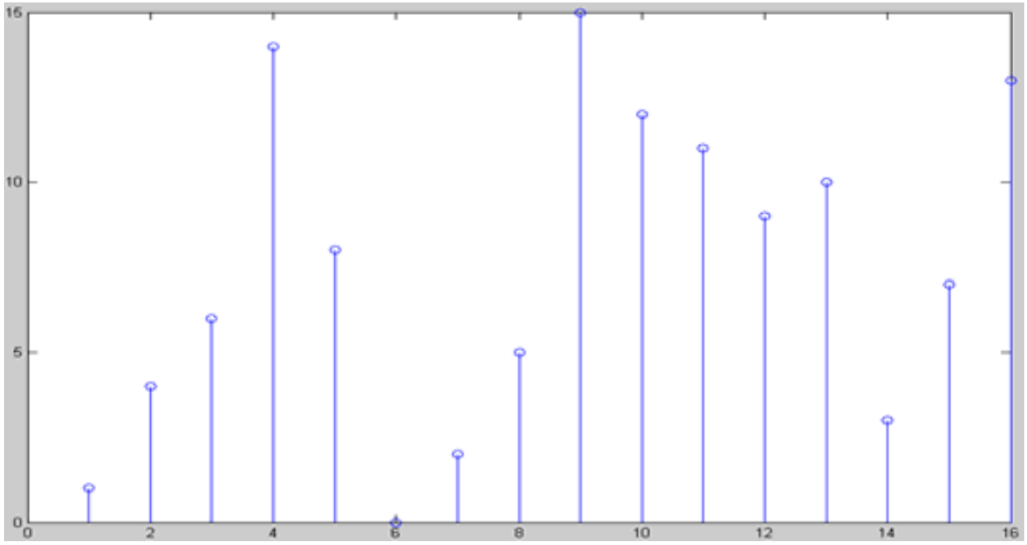
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

across the remainder of the network; just one radio connection here between smartphone and the base station is encrypted [3]. End-to-end security in GSM cannot be guaranteed with only radio link secrecy. As a conclusion, there is a need to look into ways to establish intelligent traffic secrecy. In this writing, we have put out some very workable and tempting fix for the security breaches in the GSM system. The voice signals are classified using an embedded hardware component, the TMS320C6713 DSK, and simulation code produced in Code Composer Studio (CCS). Test was performed to determine how encryption affected describes the methodology over GSM-to-GSM connections [4]. Two very different transmission with encryption and transmission sans encryption scenarios of the GSM system were examined, and the outcomes were collected for comparison. Compared to overall processors, DSPs are tailored for signal processing applications (GPP) [5]. The allure of DSP lies in the fact that something that requires fewer instructions to process signals effectively. As a result, the DSP-boards' specialized computers and quick ADCs and DACs made the system sensitive. With desktop computers' painfully slow CPUs, that wouldn't have been feasible to analyze data at this power and precision.

1.1. Embedded Encryption Algorithm:

The goal of our encryption scheme was to randomize the voice command while preserving its speech-like amplitude, making the scrambled speech signal impossible to comprehend. We developed a method that modifies the signal to make it entirely undetected. Using 8-bit quantization, the microphone analysis it shows the voice signal to 256 levels [6]. We increase each sample's level using our C++ implementation using these quantized samples. So, Level 0 was assigned Level 128, Level 1 was assigned Level 129, and so on. The opposite mappings, from Level 129 to Level 0, is performed similarly via the decryption process. The efficiency of our method can be seen from the following figures, which highlight the distinction across unencrypted and encrypted communication. Instead of 256 levels, 16 quantization thresholds are put into consideration for simplicity [7]. The samples in Figure 1; are quantized into 16 levels, meanwhile the samples in variable continuous improvement as a result of the use of our cryptography approach. In this scenario, a difference of 8 is added to all the samples' levels in addition to adding the largest amount of randomized.



ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

Figure 1: Illustrates that the Original Unencrypted Signal Quantized into 16 Levels.

Our proposed methodology is distinctive in that it offers encrypted communications while delving into the realm of bits. In just about all GSM systems, stream cyphers have been used for cryptography [8]. Bit by bit or byte by byte, stream cipher encrypts and decrypts audio signal. The use of exclusive OR (XOR) function required that the input speech data be more in binary format. On the other token, since our encryption system operates on speech samples, the computations is reduced to binary 0s and 1s [9]. Faster processing and ultra-low latency are the end outcomes, which are also much desired in real-time audio transmissions. Our method is extremely productive, simpler, and quicker since that handles non-binary data to encrypt/decrypt language and requires less mathematics.

1.2. Use of DIP Switches:

During operation, the asymmetric encryption was changed employing DIP switches. More cryptographic techniques were devised and implemented by altering the criterion for replacement the statistical parameters with different ones [10]. Stream cyphers and a few other regularly used bit-level procedures were also put to the test. The DSK for the TMS320C6713 has 4 DIP switches. As a result, Table 1 lists the 16 possible combinations that the person who wrote this article has in total.

0000	**0001**	**0010**	**0011**
0100	**0101**	**0110**	**0111**
1000	**1001**	**1010**	**1011**
1100	**1101**	**1110**	**1111**

Table 1: Illustrates that DIP Switches Combinations.

- 0000 was the key for our previous encryption scheme, which had been previously described.
- Five different configurations of the numbers 0001-0101 were utilised to create algorithms that were adjusted from their original.
- Three different configurations between 0110 and 1000 were adopted for popular cryptographic algorithms.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

- The communication was done without protection using port 1001.
- Six more permutations between 1010 and 1111 were not utilized.

The TMS320C6713 DSK's DIP switches provides us the opportunity to evaluate several techniques in real time. The receiver side utilized the identical switch combination to decrypt using the associated decryption method [11]. This process gives us a platform to experiment with various algorithms and examine the results.

1.3. Description of GSM Security Features:

GSM Specifications 02.09, "Security Aspects," 02.17, "Subscriber Identification Modules," 03.20, "Security Related Network Functions," and 03.21, "Security Related Algorithms," will have to go into depth on the security features of GSM. The components of GSM security are user data confidentially, signaling data secrecy, subscriber identification confidentiality, and subscriber's identity authentication [12]. The International Mobile Equipment Identity uniquely identifies the customer. These details make up unique identifying credentials similar to the Electronic Serial Number in power amplifiers like AMPS and TACS, combined with the people who are interested authentication key. This sensitive information has never been communicated over the communication system thanks to the way the GSM verification and encryption systems are constructed [13]. Instead, certification is accomplished via the deployment of a challenge-response process. With the use of a transitory, randomly generated ciphering key, the real talks are secured. The Temporary-Mobile-Subscriber-Identity which is supplied by the network and might even be altered on occasion, such as during hand-offs for added security, is how the MS identifies itself.

The Subscriber Identification Module, the GSM handset or MS, and the GSM network are the three separate system components where another GSM security procedures are accomplished. The SIM includes the IMSI, the subscription identity module, the individual subscriber authenticating key, the ciphering key expansion method, and the certification algorithm. The algorithm for ciphering was included in the inside the GSM device [14]. The GSM network employs use of the cryptographic techniques as well. A database holds subscriber identity and confirmation data is kept at the authenticating center, which is a subsystem of the GSM network's construction and operation subsystem. The IMSI, TMSI, Location Area Information, and unique subscriber authentication key for each user make up this data. All three parts (SIM, device, and GSM network) must be present for the identity verification and security processes to operate. The above distribution between security credentials and cryptographic algorithms adds an extra layer of protection for both the confidentiality of wireless phone conversations and indeed the avoidance of mobile telephone fraud.

1.3.1. Authentication:

Using a challenge-response procedure, the GSM network verifies the subscriber's authentication. The MS receives a different value of 128 bits. The MS uses the people who are interested authentication key to calculate the 32-bit signed response (SRES) due to the random number's encryption using the authentication algorithm (A3) (Ki). The GSM technology repeats the computation to confirm the user's authenticity after receiving the subscriber's signed response (SRES). The unique subscriber authentication key (Ki) should be noted never before being sent via the communication system. It may be found in the subscriber's SIM, the AUC, HLR, and VLR databases, as well as other places. If the predicted value and the received SRES match, the MS has

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

successfully authorized and may proceed. If the values do not equal, the communication is cut off and the MS is informed that now the identification failed.

1.3.2. Signaling and Data Confidentiality:

The 64-bit ciphering value is encrypted using the ciphering essential generation method which is included in the SIM. Applying the same different value used in the authentication mechanism to the ciphering key generating technique with the unique subscriber verification key results in the derivation of the ciphering key. The ciphering key to encrypt and decode the data sent between the MS and BS, as should be shown in following sections. The ability to alter the cryptographic functions key adds another element of security, strengthening the platform's anti-eavesdropping defenses. The network architecture and safety concerns may call for temporal variation to the ciphering key.

1.3.3. Subscriber Identity Confidentiality:

The Temporary Mobile Subscriber Identifier (TMSI) is used to maintain subscriber identification secrecy. Following the encryption and other security processes, the TMSI is transmitted to the mobile station. The access point replies by verifying TMSI transmission. The TMSI is enforceable in the region where it was issued. The Unique-Identification (LAI), in addition to the TMSI, is required during communications far beyond location area.

2. DISCUSSION

The security of the GSM network is evaluated in this study, and a thorough and succinct summary of its security issues is presented. It has been shown that the GSM network does have several inherent security weaknesses that may be exploited for illegal activities or to confuse consumers. There are also some doable changes proposed to increase the security of 2G networks that are already in use. Though some solutions focus on end-to-end security, others prefer to concentrate on enhancing infrastructure confidentiality. The best and most lucrative approach for the 2G systems now are in use is inferred to be end-to-end protection or security at the protocol stack. To evaluate the applicability of our suggested method, experiments were conducted on both encrypted and unencrypted speech. Prior to transmitting and promptly after receipt, encrypted speech was accessible to test the effectiveness of the encryption system. Our suggested encryption scheme was unable to decrypt the encrypted voice stream. This pronunciation, which had been encrypted, was unrecognizable and significant differences from the original speech. However, the introduction of decryption somewhere at receiving end allowed for the reconstruction of the original signal. Plot lines of the waveforms of the original and encrypted voice signals were produced in order to visualize the effectiveness of the suggested system. The following screenshots demonstrate how entirely different the voice waveforms is after cryptography.

3. CONCLUSION

Although not particularly simple to accomplish, the huge number of attacks that have been created to recently would appear to indicate that security should be a main consideration for GSM users. This is especially relevant for anybody who uses such network to do private issue, such making money transactions or sharing the information about the troops. Several technologies for encrypting GSM-based communications have now been offered in the scientific papers and are now on the market, which bears witness to the fact that GSM carriers seem to have miscalculated

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

these risks. Although added and the solution for authentication, decryption, and data integrity are supplied by next generation mobile communications networks like UMTS and LTE, their familiarity with GSM protocols renders these improvements effectively useless. In actuality, impersonation attempts that take use of GSM's intrinsic design flaws will be impossible to control as long as the network continues to support outmoded protocol.

REFERENCES:

[1] M. Ramadan, G. Du, F. Li, and C. X. Xu, "EEE-GSM: End-to-end encryption scheme over GSM system," *Int. J. Secur. its Appl.*, 2016, doi: 10.14257/ijsia.2016.10.6.22.

[2] S. Eshwarage and A. Gunesekara, "Web-Based Expert System for Personalized Psychotherapeutic Counselling," *Int. Res. Conf. Artic.*, 2017.

[3] S. Morsalin, A. M. J. Islam, G. R. Rahat, S. R. H. Pidim, A. Rahman, and M. A. B. Siddiqe, "Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application," in *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, iCEEiCT 2016*, 2017. doi: 10.1109/CEEICT.2016.7873048.

[4] E. M. Cho and T. Koshiba, "Secure SMS transmission based on verifiable hash convergent group signcryption," in *Proceedings - 18th IEEE International Conference on Mobile Data Management, MDM 2017*, 2017. doi: 10.1109/MDM.2017.54.

[5] R. Elin Thomas, G. Chandhiny, K. Sharma, H. Santhi, and P. Gayathri, "Enhancement of A5/1 encryption algorithm," in *IOP Conference Series: Materials Science and Engineering*, 2017. doi: 10.1088/1757-899X/263/4/042084.

[6] N. Saxena and N. S. Chaudhari, "Secure algorithms for SAKA protocol in the GSM network," in *Proceedings - WMNC 2017: 10th Wireless and Mobile Networking Conference*, 2017. doi: 10.1109/WMNC.2017.8248853.

[7] V. R. G. Dubey, V. Jain, S. Agrawal, A. Das, and R. S. Gamad, "Automated Security and Rider Safety System for Two Wheelers," in *Proceedings - 2014 Texas Instruments India Educators Conference, TIIEC 2014*, 2017. doi: 10.1109/TIIEC.2014.012.

[8] L. s. L. Baraka W.Nyamutiga,Anael Sam, "Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania | Baraka William - Academia.edu," *Int. J.*, 2016.

[9] H. M., A. E., and A. Hussein, "Implementation of an Encryption Scheme for Voice Calls," *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016910116.

[10] A. Wightwick and B. Halak, "Secure communication interface design for IoT applications using the GSM network," in *Midwest Symposium on Circuits and Systems*, 2016. doi: 10.1109/MWSCAS.2016.7870010.

[11] C. Naveen and V. R. Satpute, "Image encryption technique using improved A5/1 cipher on image bitplanes for wireless data security," in *International Conference on Microelectronics, Computing and Communication, MicroCom 2016*, 2016. doi: 10.1109/MicroCom.2016.7522451.

[12] Z. Chen, L. Yin, Y. Pei, and J. Lu, "CodeHop: physical layer error correction and encryption with LDPC-based code hopping," *Sci. China Inf. Sci.*, 2016, doi: 10.1007/s11432-015-5452-1.

[13] S. Jadhav and A. M. Rawate, "A new audio steganography with enhanced security based on location selection scheme," *Int. J. Performability Eng.*, 2016.

[14] D. Upadhyay, P. Sharma, and S. Sampalli, "Enhancement of GSM stream cipher security using variable taps mechanism and nonlinear combination functions on linear feedback shift registers," in *Smart Innovation, Systems and Technologies*, 2016. doi: 10.1007/978-3-319-30927-9_18.