Security Enhancement in GSM using A3 algorithm

Arpita Gupta
Computer Engineering
Nirma University
Sarkhej Gandhinagar Highway
Ahmedabad, India

Prateek Singh Chandel
Computer Engineering
Nirma University
Sarkhej Gandhinagar Highway
Ahmedabad, India

ABSTRACT
The GSM (Global System for Mobile Communications) is widely used cellular standard in the world. Recently, the mobile industry has experienced an extreme increase in the number of its users. Thus the GSM network with the greatest worldwide number of users succumbs to several security vulnerabilities. Security is a burning and intelligent issue. GSM security flaws have been identified several years ago. Many algorithms are used for making the GSM secure. The algorithms mainly used are A3, A5 and A8 algorithms. Algorithm A3 is used for authentication, A5 is used for encryption, and A8 is used for the generation of a cipher key. This paper presents an enhanced scheme of A3 algorithm to improve the level of security provided by the GSM. Proposed scheme is implemented at some level and analyzed thoroughly to show that the proposed scheme provides better security in the GSM. The above said algorithm is implemented using C#.NET in Microsoft Visual Studio 2012 with the help of socket programming. In this paper, encryption is introduced in the Authentication phase during the A3 algorithm of the GSM security.

General Terms
Security, Algorithm, Authentication, GSM, Response, Service, Phase, Mobile station

Keywords
GSM, Security, A3 algorithm, SRES, VLR, HLR

1. INTRODUCTION
Mobile communications offer people the facility to communicate with each other at anywhere at any time. GSM is much more than an abbreviation for Global System for Mobile Communications. It signifies an extremely successful technology and bearer for mobile communication system for second generation cellular technology. It offers digitalized voice. It covers over 71% of the digital wireless market [3]. Hence it has become the most successful digital mobile telecommunication system in the world today. It is used in more than 190 countries by over 800 million people. The ubiquitous infrastructure, while dramatically increasing the functionality levels, has posed significant security concerns on cellular mobile networks [9].

However the openness of the mobile communication poses serious security threats to the sensitive information. The security solutions in the mobile communications generally rely on the cryptographic techniques [1]. But anybody who can get hold of a radio receiver can access GSM signal or data [2] [8]. Hence, as the growth of cryptographic attacks has increased, there is a need for advanced security solution, especially in the mobile communication [4]. Therefore, it is necessary that the communication over the wireless radio media is secured. The first step in the GSM security is the authentication of a valid user for the SIM (Subscriber Identity Module) [SIM stores all user-specific data that is relevant to GSM.]. The user needs a PIN to access the SIM. PIN is the Personal Identification Number. The next step is the subscriber authentication. This step is based on the challenge-response scheme. Later steps are encryption and cipher key generation.

This paper deals with the first step of the security of GSM i.e. the authentication. The authentication is done to ensure that the user is really the person who he claims is. Authentication involves two functional entities: the SIM card in the mobile phone and the Authentication Centre (AuC) [3]. GSM employs A3 algorithm for the authentication of the user. Algorithm A3 is located on the SIM and in the AuC and can be proprietary. This algorithm employed is not very strong but is susceptible to danger.

In this paper, an enhanced version of A3 algorithm is proposed to improve the level of security offered by the GSM standard. To improve the security during the authentication, the basic idea is to include the encryption during the authentication phase. The generated signed response (SRES) as the result of the A3 algorithm is encrypted on the SIM or the mobile station (MS) and it is decrypted at the mobile services switching centre (MSC). Then, if the SRES generated at the MSC is same as the SRES generated at the mobile station and encrypted by the MSC, the user is authenticated. The proposed scheme is coded in C#.NET in Microsoft Visual Studio 2012. The paper is organized as follows: Section II gives the brief introduction to the A3 algorithm. Section III describes the proposed version of the A3 security algorithm. Finally section IV gives the conclusion for the paper.

2. A3 ALGORITHM: A BRIEF INTRODUTION
Algorithm A3 is used for the authentication in the GSM cellular standard. Before a subscriber can use any service provided by the GSM network, he/she must be authenticated [2]. This authentication is based on the SIM (Subscriber Identity Module), which stores the authentication key K_i, the user identification IMSI (International Mobile Subscriber Identity), and the algorithm used for this authentication i.e. A3.

The authentication uses a challenge-response mechanism [3]. The mobile station (MS) signs into the network. The access control (AC) generates a random number RAND as challenge, and the SIM within the MS answers with the SRES (Signed Response) as the response. The AuC (Authentication Centre) generates the random values of RAND, the signal response SRES and the cipher key K_c. This information is forwarded to the HLR (Home Location Register). The VLR (Visitor Location Register) requests the values of RAND, SRES and K_c from the HLR [7].

The VLR sends the RAND value generated to the SIM. On both sides, the network and the subscriber module, same operation is performed between the 128 bit RAND and 128 bit K_i, called A3. SRES of 32 bit is generated on both the sides. MS sends the SRES generated by the SIM to the VLR [3]. Now VLR can compare both the SRES generated. If both are same, the user or the subscriber is authenticated, otherwise rejected [3]. The following diagrams (Fig 1 and Fig 2) depict the above mentioned algorithm:

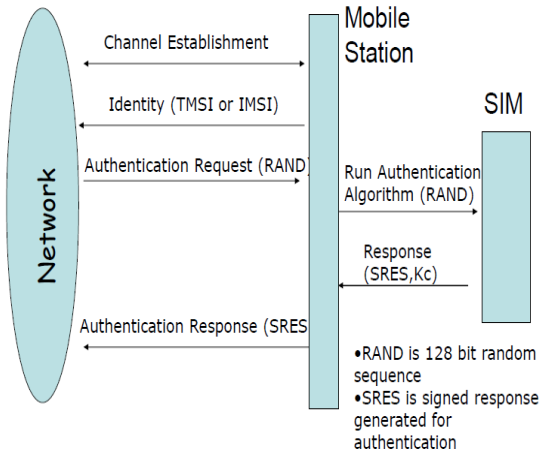

Fig 1: A3 Algorithm flow

3. PROPOSED SCHEME

The proposed algorithm of security enhances the authentication of the user who is trying to communicate via the mobile device. The 128 bit RAND and the 128 bit K_i are present at both ends i.e. on the SIM as well as in the mobile network.

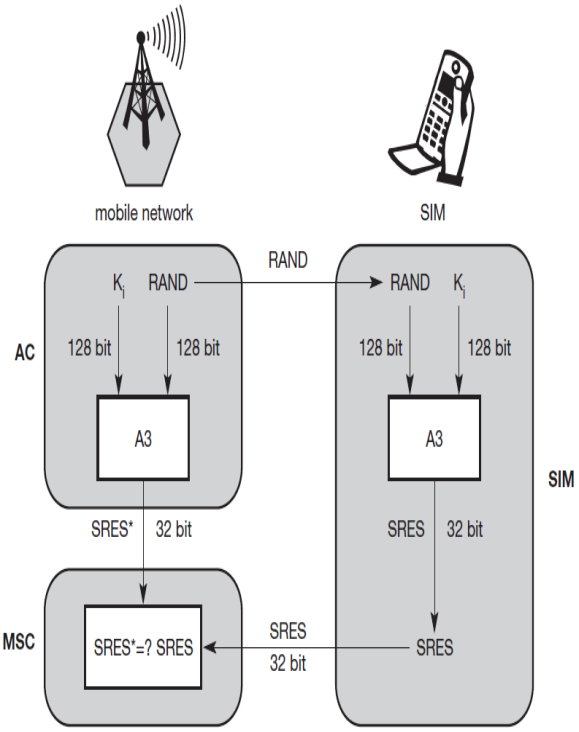

Fig 2: A3 Algorithm Block Diagram

The signed response generated (SRES) by A3 algorithm as shown below in Fig 3.

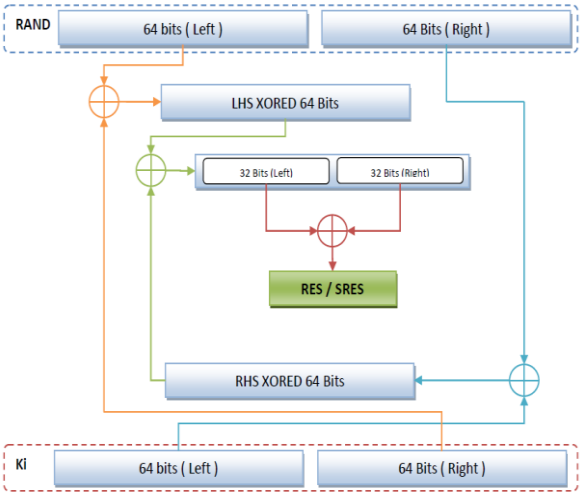

Fig 3: A3 Algorithm generated SRES

As shown in the figure above, the upper 64 bits of the RAND are XORed with lower 64 bits of K_i to produce the LHS 64 bits. Similarly the lower 64 bits of the RAND are XORed with the upper 64 bits of K_i to produce RHS 64 bits. The results produced (LHS and RHS 64 bits) are XORed to get a 64 bit number. In this number the upper 32 bit is XORed with the lower 32 bit to form a 32 bit SRES (signed response).

Now, in our proposed scheme, this SRES generated is encrypted by the AC (access control) using some scheme of encryption. This SRES goes to the MSC which decrypts it and compares it with the SRES that is generated by the SIM. If they are equal, the user is authenticated otherwise not.

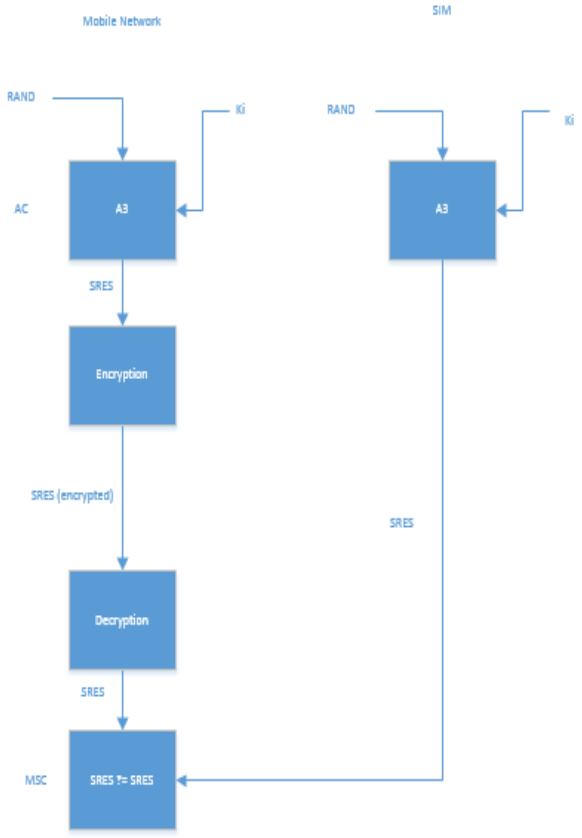

Fig 4: Flow diagram

The above flow chart (Fig 4) is the flow chart of the proposed scheme. This ensures a better security in the GSM.

4. CONCLUSION

In this paper we presented an enhanced version of the authentication algorithm used in GSM cellular standard. The additional encryption is done during the authentication phase to improve the security so that only the authenticated users can be subscribed. The implementation is done in C#.NET in Microsoft Visual Studio 2012. The security analysis is carried out by this proposed scheme. It can be concluded that the addition of the encryption in the authentication during the A3 algorithm increases the security in the GSM network. This is because the original A3 algorithm that is being implemented currently in the GSM is not very strong. Hence enhancements of the security algorithms are very much required for better mobile security and for the protection of data over the wireless communication network. As the security in mobile communication is very fragile, these kinds of enhancements are required. Still the security is not at the level that is required but it is just a step forward to reach that level. In future, further enhancements can be done or new algorithms can be proposed and mobile communications can be made more secure.

5. ACKNOWLEDGEMENT

We would like to thank our faculty Prof. Vishal U. Parikh to give us such an opportunity to prepare this research paper. This really helped us improve our ability in understanding the subject of Mobile Computing. Also big thanks to our university for providing us with such a platform where we can indulge in this kind of research work.

6. REFERENCES

[1] Musheer Ahmad and Izharuddin, Security Enhancements in GSM Cellular Standard, 978-1-4244-3328-5/08/$25.00 ©2008 IEEE.

[2] Asoke K. Talukder and Rupa R. Yavagal, Mobile Computing – Technology, Applications and Service Creation, 137-165.

[3] Jochen Schiller, Mobile Communications Second Edition, 96-122.

[4] Yong Ll, Yin Chen, Tie-Jun Ma, Security in GSM.

[5] Prof. Noureddine Boudriga, Security of Mobile Communications, 2007 IEEE International Conference on Signaling Processing and Communications (ICSPC 2007), 24-27 November, Dubai, United Arab Emirates.

[6] A. Jaganath Swamy and D. Dinesh Reddy, WAP Collaboration and Security Issues in Mobile Communication, 0-9785699-1-1/07/$25.00 ©2007 IEEE.

[7] Billy Brumley, Special Course on Cryptology, A3/A8 & COMP128.

[8] M Walker, Security Issues in Future Mobile Communications, © Vodafone Printed and published by the lEE, Michael Faraday House, Six Hills Way, Stevenage. Herts SG12AY, UK.

[9] Bo Sun, Xing Jin, Yang Xiao, Ruhai Wang, Enhancing Security using Mobility Profile for Cellular Mobile Networks, 1-4244-0357-X/06/$20.00 © 2006 IEEE.