Security in GSM Networks

Masum Bakaul
Department of CSE
Britannia University,
Cumilla, Bangladesh

Md. Ashikul Islam
Department of CSE
Britannia University,
Cumilla, Bangladesh

H. M. Abdul Ahad
Department of CSE
Britannia University,
Cumilla, Bangladesh

Shayma Rahman
Department of CSE
Britannia University
Cumilla, Bangladesh

ABSTRACT
Wireless medium is open to all. Hence it is always acceptable to threats and attacks. GSM being a wireless network is always prone to the unauthorized access to the network and entrustment to the privacy and confidentiality of the users. Therefore, the GSM provides security measures to ensure the privacy and confidentiality of the users to ensure that only registered and authorized users get the access to the network. This paper briefly presents the security measures of GSM technology. The study is enriched with a general overview of GSM protection and the algorithms that are mainly used in A3, A5 and A8. Author's also discussed the authentication and encryption methods provided by GSM. A3 for MS authentication algorithm. A5 for powerful over wind voice privacy algorithms. A8 for voice privacy key generation algorithm.

Keywords
GSM Security, Algorithm, Anonymity, Authentication, Encryption

1. INTRODUCTION
The most secure system available today for cellular telecommunications. GSM ensures user's security by protecting the GSM subscribers call privacy and anonymity. In order to protect user's privacy a temporary identification number is given to the subscriber's number. Temporary identification numbers are assigned to the subscriber's number to maintain the privacy of the user. GSM uses narrowband and TDMA for giving voice and context base administration over cell phones. The 1st GSM network was deployed in Finland in Dec 1993. At the starting of 2007, the worldwide number of mobile users reached to 2.83 billion people where 2.28 billion users out of them (i.e. 80.5%) were using the GSM [4]. GSM 900 / GSM1800 MHz are mostly used in country like Europe, Australia, Asia, Middle East and Africa whereas the GSM 850 / GSM 1900 MHz are used in the United States, Canada, Mexico and most countries of South America. GSM uses wireless medium, encrypted communication between user phone and the cellular telephone base station. User's voice is decrypted at base station and sent over the telephone network. A suitably motivated attacker can crack A5 algorithm which is known as encryption algorithm in GSM. GSM system provides security controls [2]. Since GSM is a wireless medium always acceptable to attacks. GSM offers different security services using confidential information stored in the SIM and AUC [2]. To provide GSM securities at first ensure two sided security such as one in subscriber side and other in operator side. At the subscriber side, the security measures need to be promising and precise. Its aim at maintaining privacy and anonymity and mechanism's for strong access control so that only authorized users should be able to access the network. At operator side, it follows mechanisms to avoid fraud and service protection from threats and attacks. GSM security controls achieved using the four primary security mechanisms which provides strict security measures to ensure the privacy and confidentiality of the users as well as to ensure that only authorized and registered users are capable to access the network. Goals of the security features of GSM is security namely access control, anonymity authentication and encryption mechanism offered by GSM via A3, A5, A8 algorithm [3]. Strong algorithm and encryption techniques were introduced in GSM for protecting user's security.

2. LITERATURE REVIEW
In 2003, J. H. Schiller published the book "Mobile communications"; where author described the fundamental concepts of GSM security used to protect all mobile systems during data transmission [3]. M. Toorani and A. Beheshti researched on Solutions to the GSM Security Weaknesses and published The Second International Conference on Next Generation Mobile Applications, Services and Technologies in September 2008[4]. In 2001, Suraj Srinivas published the paper "The GSM Standard (An overview of its security)" from the SANS Institute Information Security Reading Room site [6]. In 2005, Thomas Stockinger focused on basic mechanisms of the GSM network to protect security and privacy based on A5 stream cipher with a short introduction of the A8 cipher and the similar A3 cipher [1]. Yong LI, Yin CHEN and Tie-Jun MA., reviews the existing limitation and problems with GSM security; also describe some possible improvements for the next GSM network [5]. In 2004, Jeremy Quirke published the updated edition of the paper "Security in the GSM system" where authors explore the security features offered by GSM [7]. Chengyuan Peng published "GSM and GPRS Security" in Tik-110.501 Seminar on Network Security where author gives an overview of the security features provided in a GSM PLMN and GPRS network and also discusses the SIM module, which plays an important role in GSM security [2].

Ihtesham ul Haq, Zia Ur Rahman, Shahid Ali and Muhammad Faisal published "GSM Technology: Architecture, Security and Future Challenges" on International Journal of Science Engineering and Advance Technology where author's reviews the whole GSM system and its security [8]. Giuseppe Cattane, Giancarlo De Maio and Umberto Ferraro Petrillo researched on Security Issues and Attacks on the GSM Standard: a Review1 and published Journal of Universal Computer Science in October 2013[9]. In 2011, Christian Kröger published the paper "GSM security" where author gives an overview of GSM security and the practicality of an attack on the A5/1 algorithm used for encrypting 2G GSM communication [10]. In November 2012, Opu Narcisse published the paper "Security in the Global System for Mobile Communications (GSM)" where author reviews the security features and architecture of GSM [11]. In 2000, Juha Mynttinen published "'End-to-end security of mobile data in GSM" in Tik-110.501 Seminar on Network Security where author discusses Security requirements for end-to-end security of mobile data in GSM [12].

3. TERMINOLOGY

SIM *(Subscriber Identity Module*) is implemented on a smart card which stores identification information that determines a smartphone to a specific mobile network.

PIN (*Personal Identification* Number) is a security code used for verifying user identity.

PUK (*Personal Unblocking Key*) is the code necessary to unlock a *GSM* SIM card that has disabled itself after an incorrect PIN code was entered 3-5 times.

AuC (*Authentication Center*) is a secure database. It offers authentication parameters for the authentication process.

IMSI (*International Mobile Subscriber Identity*) is a number that uniquely identifies every user of a GSM network. It is used for identification of user, when he is accessing the GSM network.

TMSI (*Temporary Mobile Subscriber Identity*) is a temporary identification number that is used in the GSM network instead of the IMSI to ensure the privacy of the users.

VLR (*Visitor Location Register*) is a database which contains the exact location of all mobile users right now present in the service area of the MSC.

RAND is 128-bit random challenge produced by the authentication center.

SRES is the 32-bit signed response produced by the mobile station and the authentication center.

Ki is the 128-bit individual subscriber authentication key utilized as a secret key shared between the mobile station and the GSM operator.

Kc is the 64-bit ciphering key used as a session key for encryption of the over-the-air channel.

4. GSM SECURITY MECHANISM

GSM security procedures are generation and distribution of keys, exchange information between operators, confidentiality of algorithm etc. GSM has given concern on operator and user side. Billing to the right person, method to avoid fraud and protecting services from attacks was maintained at the operator side. Privacy maintenance and anonymity and methods for strong access control were accused at user side.

4.1 Experiencing Security Problems in GSM

GSM are vulnerable to various kinds of attacks. To discuss GSM security features at first analyze the problems GSM faces. Facing problems are:

- Implicit data integrity means no integrity algorithms have provided for this problem [5].
- Unilateral Authentication means only user authentication to the network has provided and no accomplishment of network identification to the users. [5].
- Increasing computation speed with smaller key length makes a weak encryption algorithm. A break down might occur in COMP128 algorithm due to increased computational speed. Weak encryption algorithms are quite difficult to replace due to increasing speed [5].
- Unsecured Terminal means IMEI is an unsecured identity. Integrity mechanisms for IMEI are introduced late that makes it unsecured.

4.2 Possible Improvements for GSM Security

To solve these existing problems the paper, present some prediction to improve the GSM security features. The author's recommended to use cryptographically secure algorithm for A3 [5]. Secondly, the operator can employ a new A5 implementation with strong encryption too. Thirdly, Due to some weakness in A8 algorithm researchers have suggested to use their own algorithm for security purposes [5].

4.3 Access Control to SIM

The first step includes access control to SIM. SIM stores confidential information that might be personal or network specific [3]. It stores IMSI number which is used to access the account of the subscriber. It stores 128 bit root encryption key. It contains A3 and A8 algorithm which is used for authentication and generation of cipher keys [3]. Therefore, it is very necessary to protect the SIM card. GSM provides a provision of SIM card by PIN. The user needs to know the PIN number to lock the SIM card. The SIM card automatically locked out after three unsuccessful attempts by feeding the wrong PIN have been made. In this case, A PIN and locking key that is PUK is provided to the operator [7]. A PUK code is required to unblock a GSM SIM card that has been locked after entering the wrong PIN code three times [7]. If the PUK code entered incorrectly (normally 10 times) the access to information is refused permanently and SIM becomes useless [7]. A3 and A8 algorithm ensures the security of user's personal information. Both A3 and A8 performed this task by authentication and cipher keys generation [3]. The purpose of an access control system is to provide quick and convenient access to those users who are authorized. At the same time unauthorized access to information is also protected.

4.4 Anonymity

Anonymity of the user means hiding the identity and location of the user. It is followed by using TMSI in place of IMSI number. TMSI has provided by the AuC after submitting application for authentication and valid encryption procedures [3, 6]. TMSI contains (4*8bits) is consists of 4 octets but all 32 bits cannot be made 1 because all 32 bits 1 indicates that there is no TMSI. The VLR should be able to correlate the TMSI with the IMSI of the mobile station to which it is allocated [3, 6]. That means there should be a provision to create the TMSI number for which IMSI number. Anonymity is used to protect the privacy of users during communication.

4.5 Authentication and Encryption

Authentication and encryption have been treated as a precaution to security and user's confidential information. Authentication is simply one-sided. Authentication ensures that only authorized user's is allowed to access the network. A3 algorithm is used for authentication purposes [3]. Encryption ensures the confidentiality of data and signal maintenance. In encryption, A8 algorithm is used for generating cipher key and A5 algorithm is used for encrypting data transmitted from mobile station to base station [3].

5. GSM SECURITY ALGORITHMS

The GSM specification for security has designed secretly by GSM consortium. The consortium used "Security by Obscurity" principles. It means protects anything by hiding. So, the GSM consortium used "Security by Obscurity" for the algorithms A3, A5 and A8 initially which said that algorithm will be difficult to crack if they are not publically available [6]. Therefore, these algorithms are available to only hardware and software manufacturers and GSM network operators. But slowly these algorithms are also made public.

5.1 A3 and A8 Algorithm

Both A3 and A8 algorithm are one-way algorithms. They are implemented in SIM cards and GSM network Authentication Centers. A3 and A8 are not strong enough therefore the network provider can use their own algorithms or user can use their created algorithm for encryption. But A5 algorithm which is used for encryption is implemented on the device therefore it should be identical for all the service providers. It should change from service provider to service provider or from one user to another user. Only A3 and A8 algorithms can be made properly by the service providers or by the users and they can bring changes accordingly to make the algorithms strong. A3 and A8 algorithm used symmetric encryption techniques where keys are shared and loaded in the SIM card. Both are one-way function which means that output can be found if the inputs are known but it is impossible to find inputs if outputs is known. Both A3 and A8 algorithms used COMP128 which is keyed hash function [5, 6].

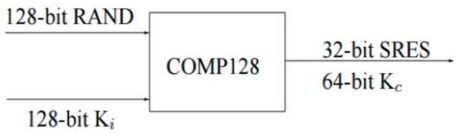

Fig 1: COMP 128 algorithm

It takes 128 bit key and 128 bit RAND number as input and produces 128 bit output. The first 32 bits of 128 form SRES and next 54 bits from the cipher key which are used for authentication and encryption [5]. It resolves the key length problems and COMP128 algorithm not supposed to broken while speed increased. A3 is used for the authentication in the GSM. An A3/A8 algorithm is used to authenticate the customer and generate a key for encrypting voice and data traffic.

5.2 Authentication via Challenge Response Technique

Authentication method checks the validity of the user's SIM card and then decides whether the mobile station is allowed on a particular network. Authentication requires following the entities and uses a technique which is known as “challenge response technique or method”. The entities required A3 algorithms used for authentication which is stored in the SIM card as well as also made available at the AuC and the network [7]. Entities require Ki which is 128 bit key stored at the SIM card and AuC. The key ki correlated with the IMSI number and looking at the IMSI number the key can be automatically retrieved. It requires RAND which is automatically generated by AuC known as “Challenge” [7].

Authentication follows following steps:

- Mobile station sends IMSI to the network.
- Network accepts IMSI and finds corresponding Ki which is 128 bit secret key stored on the SIM card as well as available with the authentication center [7].
- The AUC generates 128 bit random number RAND and sends to the mobile station. This is called "Challenge” [7].
- SIM card accepts this challenge and used the random number and key Ki as input to A3 algorithm. It produces 32 bit output called SRES.
- Network also calculates output (SRES) using same inputs and algorithm.
- MS sends SRES to the network.
- Network matches both SRES, if matched subscriber is authenticated.

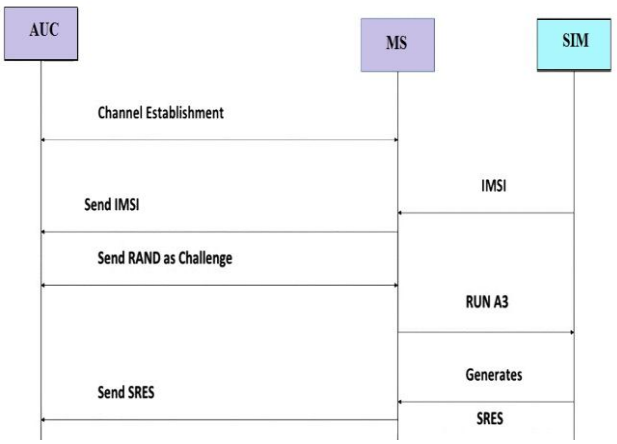

Fig 2: Authentication process

This method ensures that only authorized user can access the network. There is no possibility of unsecured data transmission. It is also used to prove the identity of a user or other entity requesting access to a computer, network or other network resource.

It points that, how GSM encrypts data and signals. The encryption is always happening between the mobile station and base station only. There is no end to end encryption that is the data and signal will transmit encrypted format from the Mobile station to Base station.

The algorithm A5 and A8 are used for encryption. For encryption it needed a cipher key Kc. This cipher key is not statically available. It is dynamically generated using A8 algorithm. Actually, SRES and Kc both are generated at the same time. A8 uses Ki and RAND as input and generates 64 bit cipher key (Kc) [5, 7]. A5 algorithm is used for encryption of plain text.

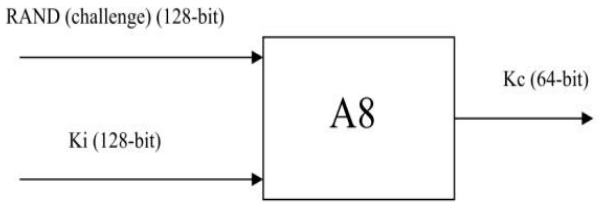

Fig 3: A8 algorithm

5.3 A5 Algorithm

A5 algorithm stored on device. A5 algorithm is implemented on the hardware of the device. It is a stream cipher. It is used to encrypt over the air transmissions and works on bit by bit basis. It uses Kc (cipher key) that is 64 bits where 22 bits used as function key. It generates 114 bits cipher text from the same number of plaintexts [1].

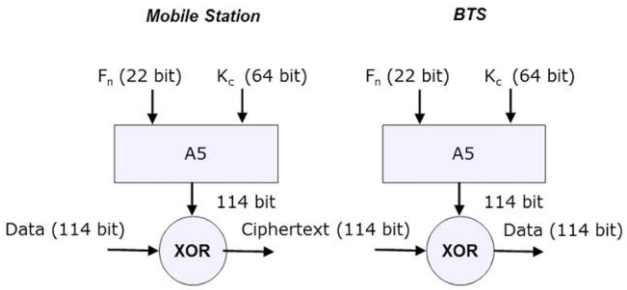

Fig 4: A5 algorithm

The various implementation of A5 algorithms are available most common ones are A5/0, A5/1, A5/2, and A5/3[6]. A5/1 is the strongest one and A5/0 is literally no encryption [1]. So, authors recommended to use the A5/1 algorithm during data transmission because it has provided strong security compared to other versions of A5.

6. GSM SECURITY LIMITATIONS

The important problem of algorithms in GSM is that they are example of: "Security *by Obscurity*".

- Design only provides access security in communication and signaling in the fixed network portion are not protected [5].
- Design does not address active attacks, whereby network elements may be impersonated.
- Design goal was only ever to be as secure as the fixed network to which GSM system connect.
- Short key size of kc (64 bits) makes it more vulnerable to various attacks [5].

7. CONCLUSION

GSM security algorithms are used for secure communication in mobile network. In this paper, the security of the GSM network is estimated and a complete and brief review of its security problems is presented. It is proved that the GSM network has many inherent security errors that can be distorted for duplicitous purposes. GSM is the dominant mobile technology. Main reason for GSM to become vulnerable that some of the algorithms and specifications were oozed out and some critical errors were found. Security can be enhanced in some areas with relatively simple measures. The security mechanisms specified in the GSM network made it most secure mobile communication system. The use of AuC, encryption and TMSI number ensure the privacy and anonymity of the users. To building strong a security in GSM it is essential to use A3, A5 and A8 algorithm because they provided stronger security in GSM encryption and data transmission.

8. REFERENCES

[1] T. Stockinger, "GSM network and its privacy- the A5 stream cipher," CiteSeerX, Nov-2005. [Online]. Available:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.465.8718.

[2] C. Peng, "GSM and GPRS Security."

[3] J. H. Schiller, Mobile communications. Reading, MA: Addison-Wesley, 2003.

[4] M. Toorani and A. Beheshti, "Solutions to the GSM Security Weaknesses," 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, Sep. 2008.

[5] Y. LI, Y. CHEN, and T.-J. MA, "Security in GSM," pp. 2–11.

[6] [https://pdfs.semanticscholar.org/3aac/d711ae891c9a1ad70f3be26be4ab9de090a1.pdf]

[7] S. Srinivas, "The GSM Standard (An overview of its security)," SANS Institute Information Security Reading Room, pp. 2–7, 20-Dec-2001.

[8] J. Quirke, "Security in the GSM system," pp. 2–13, 01-May 2004.

[9] [https://pdfs.semanticscholar.org/b0c8/493e0c6b6e5e08d870a1b318401236e07e82.pdf]

[10] Ihtesham ul Haq, Zia Ur Rahman, Shahid Ali and Engr. Muhammad Faisal (2017) 'GSM Technology: Architecture, Security and Future Challenges', International Journal of Science Engineering and Advance Technology, 5(1).

[11] Giuseppe Cattaneo,Giancarlo De Maio,Umberto Ferraro Petrillo (2013) 'Security Issues and Attacks on the GSM Standard: a Review1', Journal of Universal Computer Science, 19(16).

[12] Christian Kröger (2011) 'GSM security'.

[13] Opu Narcisse (2012) 'Security in the Global System for Mobile Communications (GSM)'.

[14] Juha Mynttinen (2000) 'End-to-end security of mobile data in GSM'.