Security Management System of Cellular Communication: Case Study

Othman O. Khalifa, Abdulrazzag Aburas, A. Al Bagul, Meftah Hrairi, Muhammad Shahril bin Shahbuddin, and Harman bin Mat Kasa

***Abstract*—**Cellular communication is being widely used by all over the world. The users of handsets are increasing due to the request from marketing sector. The important aspect that has to be touch in this paper is about the security system of cellular communication. It is important to provide users with a secure channel for communication. A brief description of the new GSM cellular network architecture will be provided. Limitations of cellular networks, their security issues and the different types of attacks will be discussed. The paper will go over some new security mechanisms that have been proposed by researchers. Overall, this paper clarifies the security system or services of cellular communication using GSM. Three Malaysian Communication Companies were taken as Case study in this paper.

***Keywords*—**GSM, Security systems, SIM CARD, IMSI, Authentication.

I. Introduction

SOME of the cellular communication systems nowadays are using GSM where it is a common world wide standard. GSM stands for *"global system for mobile communications"* [1][2]. Practically, the GSM standard is currently used in the 900 MHz and 1800 MHz bands. The technique uses by GSM to transmit signals are using Frequency Division Multiplexing (FDD). It allows full roaming from operator to operator if mutual bilateral agreement. In theory, GSM network contains cells with a base station (BS) at the center of each cell. Mobile stations (MS) are connected to base stations. If mobile station moves between two cells the network performs a handover and the call is not dropped. GSM network is divided into location areas, each containing a certain number of cells. Mobile station can be reached trough paging when it moves within location area; otherwise it cannot be reached before it performs a location update [3][4]. According to the GSM Association, GSM technology is in use by more than one in ten of the world's population and is available in almost over all world [5]. Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries. For instance, we can contact our friends outside Malaysia because Maxis's and Celcom's have using this GSM system networking. Furthermore, The General Packet Radio Service (GPRS) [6] is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks, e.g., to the Internet. It applies a packet radio principle to transfer user data packets in an efficient way between mobile stations and external packet data networks [7].

II. GSM Security Measures

There are four security measures in GSM. The four security measures are the PIN code, Authentication of SIM CARD; this is a local security measure. Then, the User authentication performed by network, encrypting of information sent over radio interface and the last one is the usage of TMSI instead of IMSI over radio interface. The IMSI means international mobile subscribers identity which is globally unique and the TMSI means temporary mobile subscriber identity which is local and temporary identity. By referring to introduction statement, we had explained the GSM network. Now, we are going to explain about the networking. Network uses subscriber authentication key (Ki) and International Mobile Subscriber Identity (IMSI) for identifying the mobile. Ki and IMSI are stored in the mobile and in a network element called AUC. AUC uses Ki and IMSI to calculate an identification parameter called signal response (SRES). SRES is calculated as a function of Ki and a random number generated by the AUC. RAND and SRES are stored in the HLR (home location register). Registration to the network will not be accepted until the authentication has been performed. Using the mobile's IMSI, RAND and SRES are fetched from HLR [5][7]. RAND is sent to the mobile, which uses the stored Ki to calculate SRES.

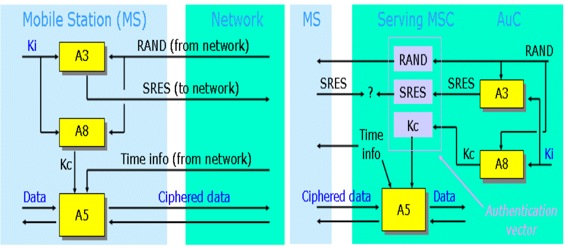


Fig. 1 Signaling between the MSC and the MS

Authors are with International Islamic University Malaysia, Faculty of Engineering (e-mail: khalifa@iiu.edu.my).

The calculated SRES is returned to the MSC, where it is compared with the SRES value received from HLR as shown in Fig. 2. The objective of the security system is to make the system as secure as the public switched telephone network. The use of radio at the transmissions medium allows a number of potential threats from eavesdropping the transmissions. Eavesdropping refers to an intruder being able to interact with the communication channel so that information can be extracted from the channel, possibly without the knowledge of any of the communicating parties. Eavesdropping can compromise the network and allow an intruder to obtain restricted information.

III. Description of the Functions of the Security Systems

In GSM, there are four security services or systems provided that we have discovered. The four security services are:

1. Anonymity: So that is not easy to identify the user of the system.
2. Authentication: So the operator knows who is using the system for billing purposes.
3. Signaling protection: So that sensitive information on the signaling channel, such as telephone numbers, is protected the radio path.
4. User Data Protection: So that user data passing over the radio path is protected.

A. Anonymity

Anonymity is provided by using temporary identifiers. When user first switches on his radio set, the real identify is used, and a temporary identifier is then issued. From then on the temporary identifier is used. Only by tracking the user is possible to determine the temporary identify being used. In analog cellular security, the anonymity is none, IMSI (International Mobile Subscribers Identity) transmitted in the clear. Besides, the desired security attributes has protected the users from identification. The anonymity has functioning for end users use real IMSI to obtain a temp IMSI and all subsequent operations use the temp IMSI.

B. Authentication

Authentication uses a technique that can be described as a “Challenge and Response”, based on encryption. The encryption is the process by which information is encoded so that only an unauthorized user has access to that information. A user needs the key that will unlock the encoded information and change it back to its original form. Actually, authentication is used to identify the user (or holder of a Smart Card) to the network operator. It 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. Eavesdropping the radio channel reveals no useful information, as the next time a new random challenge will be used. As mentioned before, eavesdropping refers to an intruder being able to interact with the communication channel so that information can be extracted from the channel, possibly without the knowledge of any of the communicating parties. Eavesdropping can compromise the network and allow an intruder to obtain restricted information. 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 R as the input (Plaintext) to the encryption, and using a secret key unique to the mobile Ki, transform into a response Signed Response (SRES), which is sent back to the network. The diagram below shows “Challenge response mechanism for Authentication and Key Agreement” where A3 algorithm is used to compute Response from Challenge using a shared, secret key. In summary, the authentication is a complex process with mutual verification is desirable, but not always achievable.

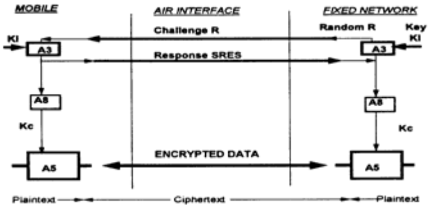


Fig. 2 GSM Authentication and Key Agreement

C. User Data and Signaling Protection

Actually, the signaling protection is protected the radio path of the sensitive information on the signaling channel and user data protection is protected user data passing over the radio path. By referring to the Fig. 1, after the authentication process, the response is then passed through an algorithm A8 by both the mobile and the network to derive the key Kc used for encrypting the signaling and messages to provide privacy (A series algorithms). In wired telephony, for signal protection, it requires physical access to wire or SS7 and for user data protection, it physical access to wire.

The attribution of the security for signaling protection is secure signaling and protected from interception. Also, the user data protection is protected for privacy of conversations.

D. GSM Security Implementation

In theory, A3 implemented within a Smart Card. It is “Tamper proof” smart card containing the key. Furthermore, A5 is in the data path and must be fast (in the phone hardware). The difference between A5/1 and A5/2 are A5/1 is “strong” encryption and A5/2 for “export”-level encryption.

IV. Implementation

In this section, we are going to clarify about the implementation and roaming of the GSM network. The authentication algorithm A3 is an operator option, and is implemented within the smart card (known as the Subscriber Interface Module or SIM). So that the operators may inter-work without revealing the authentication algorithms and mobile keys (Ki) to each other, GSM allows triplets of challengers (R), responses (SRES) and communications keys

(Kc) to be sent between operators over the connecting networks. The A series algorithms are contained within the mobile equipment, as they have to be sufficiently fast and therefore hardware. There are two defined algorithms used in GSM known as A5/1 and A5/2.

The enhanced Phase 1 specifications developed by ETSI allows for inter-working between mobiles containing A5/1, A5/2 and unencrypted networks. These algorithms can all be built using a few thousand transistors, and usually takes a small area of a chip within the mobile.

V. Techniques for Privacy and Authentication in Personal Communication Systems

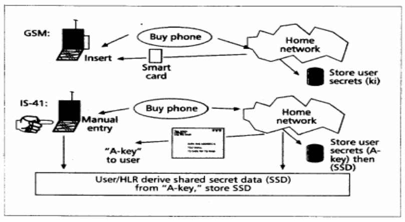


Fig. 3 AKA process: a general method

This subtopic is very important because a well designed Privacy and Authentication (P&I) technique is necessary to protect assets. So, Privacy and Authentication are generally linked together because the derivation of a "session key" for an encryption algorithm is often an integral part of the authentication process. Authentication and Key Agreement (AKA) is the access control and derivation of a session key form a single activity. To summarize, the AKA method of preference for some proposed Personal Communication Systems (PCS) air interfaces that are currently under development by standard bodies. Fig. 3 depicts the general AKA process. The figure shows the user's handset on the upper left and the service provider's network in the upper-right corner. The three part security model that connects this endpoint provides the logical steps necessary to accomplish this process. The first part of the general security model is provisioning. This is means by which the user's handset acquires the bona fide that will enable the network to subsequently recognize him as a legitimate user. Part two of the model is the means by which a handset establishes credibility when the user registers with a local service provider such as Maxis and Celcom.

The third part of the model is the protocol that is executed to permit network access and establish a key for protection of channel traffic. In secret key systems, this is generally simple challenge/response mechanism. By referring the Fig. 5, the SIM contains information about the services that have been purchase. It contains a 128-bit number called "Ki". The Ki enables the SIM to authenticate itself to the network.

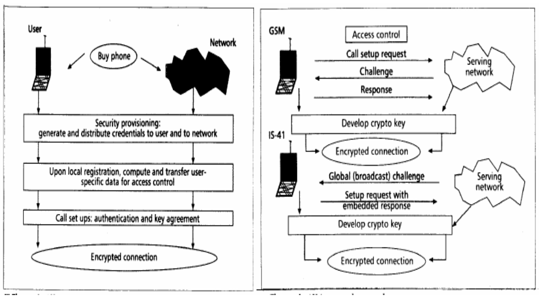
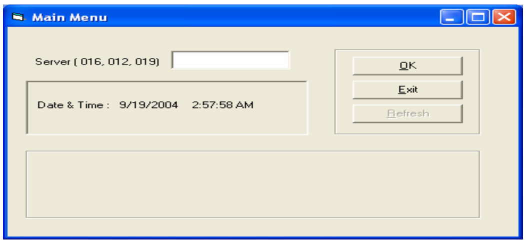

User
Buy phone
Network
Security provisioning: generate and distribute credentials to user and to network
Upon local registration, compute and transfer user-specific data for access control
Call set ups: authentication and key agreement
Encrypted connection
GSM
Access control
Call setup request
Challenge
Response
Serving network
Develop crypto key
IS-41
Encrypted connection
Global (broadcast) challenge
Setup request with embedded response
Serving network
Develop crypto key
Encrypted connection

Fig. 4 P&A provisioning of secret key systems



Server (016, 012, 019)

Date & Time : 9/19/2004 2:57:58 AM

Fig. 5 AKA Protocol: Secret key system

Fig. 5 shows the authentication and key agreement protocol in secret key systems. Both cases GSM and IS-41 systems show the goals to assure the serving network that the handset is entitled to service and to develop a set of chipper bits for protection of user traffic over the RF link.

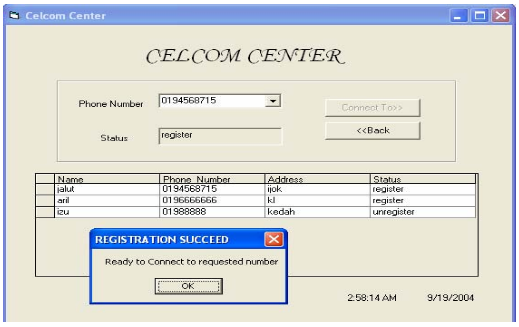
GSM based AKA utilizes a challenge/response protocol to perform authentication and to generate chipper bits. Firstly, the network begins RAND/SRES. The combination of 128-bit RAND with the user Ki will produce SRES and Kc. The match between SRES network and calculate internally, will be considered authentic. Besides, for Kc cases, it functions to protect traffic. IN a roaming situation, the above scenario is unchanged, except that the RAND/SRES/Kc triplets are recomputed by the home network. Triplets are transferred to the visited network to support a roaming user as a result of handset registration and/or a request for additional security information. The VLR performs the SRES comparison and provides Kc to the encipherment function, based on inputs from the home network.

VI. Simulation

In this section, we are trying to simulate the real security system of cellular communication is functioning by using Visual Basic application. As theoretically, we know that in security system of the GSM there are 4 parts to be take care. The four parts are anonymity, authentication, signaling protection and user data protection. By using this application first of all the box will display as below.

Input:

From the box we can choose our server and there are three servers provide; Maxis (012), Digi (016) and Celcom (019). After that, the new text box will display. This box will display all the data about our phone number, name, address and status. From the chosen scroll box we can select our phone number and this message box will appear. The important of this message box is to make sure that we can use the server or not. There are two conditions. Connection available or registration fails. If registration is fail we cannot connect to the server and transmission will stop and vice versa. If connection is available, then the user can continue the transmission with dialing the number of the person that he wants to speak. As the result, the box will appear with the registration number and the dial number.



Phone Number 0194568715

Status register

	Name	Phone Number	Address	Status
	jalut	0194568715	ijok	register
	aril	0196666666	kl	register
	izu	01988888	kedah	unregister

REGISTRATION SUCCEED

Ready to Connect to requested number

2:58:14 AM 9/19/2004

VII. Limitation of GSM Security

Each system in this world has a limit. It happens in GSM security system or requirements, where there are a number of potential weaknesses. In this section, we would like to explain in 4 categories.

The security for GSM has to be appropriate for the system operator and customer: The countermeasures. The limitation of security in cellular communication is a result of the fact that all cellular communication is sent over the air, which then gives rise to threats from eavesdroppers with suitable receivers. Keeping this in account, security controls were integrated into GSM to make the system as secure as public switched telephone.

A. The security for GSM has to be Appropriate for the System Operator and Customer

The system operator and customer system should be appropriate because of two reasons.

- The operators of the system wish to ensure that they could issue bills to the right people, and that the services cannot be compromised.
- The customer requires some privacy against traffic being overheard.

B. The Countermeasures

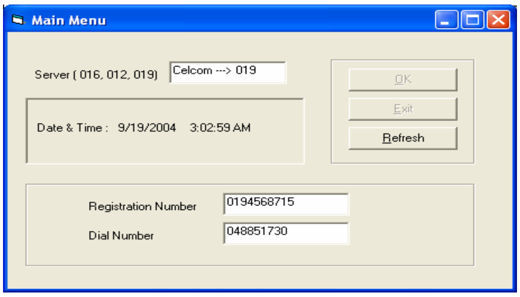
There are three aspects that countermeasures are designed:

1. Anonymity implies to make the radio path as secure as the fixed network and the confidentiality is to protect against eavesdropping or an intruder being able to interact with the communication channel so that information can be extracted from the channel, possibly without the knowledge of any of the communicating parties.
2. To have strong authentication, to protect the operator against billing fraud. In Malaysia, the communication companies that have been used this systems are Maxis, Celcom, Digi and TimeCell.
3. Due to competitive pressures and inadvertently, the countermeasure has to prevent the operator from compromising each other's security.

C. The Security Process Prohibition

Those below are the precaution in the security processes:

1. The security processes must not significantly add to the delay of the initial call set up or subsequent communication.
2. In security processes, we must not increase the bandwidth of the channel.
3. Besides, we must not allow for increased error rates, or error propagation.
4. Adding excessive complexity to the rest of the system should be avoided.
5. Lastly, to save budget of the processes implementation, there must be cost effectiveness to take care.



Server (016, 012, 019) Celcom ---> 019

Date & Time : 9/19/2004 3:02:59 AM

Registration Number 0194568715

Dial Number 048851730

D. The Design of Operator's GSM System

In this section, we are focusing on the designs of an operator's GSM system must take into account the environment and have secure procedures such as:

1. The generation and distribution of keys.
2. Exchange of information between operators.
3. The confidentiality of the algorithms.

The explanations that had been explained in 4.1 to 4.3 are made by the GSM MoU Group. The GSM MoU Group had produced guidance on these areas of operator interaction for members. The technical features for security are only a small part of the security requirements; the greatest threat is from simpler attacks such as disclosure of the encryption keys, insecure billing systems or corruption. Also, a balance is required to ensure that these security processes meet these requirements. At the same time a judgment must be made of the cost and effectiveness of the security measures.

VIII. Discussion and Conclusion

Security system is extremely important nowadays because most of the components that we use today are basically deal with electronics component e.g. cellular, computer, car, door, weapons, machines, and many others. In brief, we had study about the GSM technology of security system implement in cellular communication. We had explained about The GSM technology in term of networking. The reason why we had chosen GSM because more than one in ten of the world's population and over 179 countries including Malaysia are using this system. As we had explained, the General Packet

Radio Service is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks, e.g., to the Internet. Also, it applies a packet radio principle to transfer user data packets in an efficient way between mobile stations and external packet data networks. The GSM network in term of security had 4 important aspects: Anonymity, Authentication, Signaling protection and User Data Protection. The security system of GSM starting from the user's handset to the service of GSM network was implemented. The whole security has started from Subscriber Interface Module or SIM and goes through the network. Also, 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 make sure complete security. The security provided by GSM is well in advance of similar mobile or cellular radio systems. In this simulation, we had used Visual Basic application. Most of the criteria of the system especially in Fig. 3 (AKA process: a general method) had been clarify through the simulation that we had made. The limitations of GSM security system were discussed. In this paper, the topics had been divided into 4 main factors. The factors are the security for GSM has to be appropriate for the system operator and customer, the countermeasures, the security process prohibition and the design of operator's GSM system. The important of this topic is to prevent from the hackers. Usually, the greatest threat is simply the attacker from inside where the attacker can manipulate the encryption keys. As a result, corruption and insecure billing cannot be stop.

References

[1] Definition of GSM, Retrieved January 2007, http://www.about-wireless.com/terms/gsm.htm

[2] Imai, H., et. al., Wireless communications security, Boston: Artech House, 2006.

[3] EIA/TIA, Cellular Radio-Telecommunications Intersystem Operations," Tech. Rep. IS-41 Revision C, 1995.

[4] M. Mouly and M. B. Pautet, *The GSM System for Mobile Communications*, M. Mouly, 49 rue Louise Bruneau, Palaiseau, France, 1992.

[5] GSM Association 2007, retrived January 2007, http://www.gsmworld.com/index.shtml

[6] H. Granbohm and J. Wiklund, GPRS: General Packet Radio Service, *Ericsson Review*, vol. 76, no. 2, pp. 82-88, 1999.

[7] J. Eberspächer and H.-J. Vögel, GSM: Switching, Services and Protocols, John Wiley & Sons, 1998.

[8] Yang, H., et. al., Securing a Wireless World, *Proceedings of the IEEE* v. 94 no. 2 Feb. 2006.

[9] Fernandez, E., et. al., Some security issues of wireless systems, Advanced Distributed Systems: 5th International School and Symposium, ISSADS 2005, Guadalajara, Mexico, January 24-28, 2005

[10] Zhu, J., A new authentication scheme with anonymity for wireless environments, Consumer Electronics, *IEEE Transactions on Publication* Feb 2004 Volume: 50, Issue: 1 p.p.: 231- 235.

[11] Carneiro, G., Cross-Layer Design In 4G Wireless Terminals, *IEEE Wireless Communications*, 2004.

[12] Lauter, K., The Advantages Of Elliptic Curve Cryptography For Wireless Security, *Wireless Communications, IEEE* Feb 2004 Volume: 11, Issue:1, pp. 62-67.

[13] Akyildiz, McNair, et al. Mobility management in next-generation wireless systems. *Proceedings of the IEEE,* August 1999.

[14] Brookson, C., GSM security: a description of the reasons for security and the techniques, *IEE Colloquium on Security and Cryptography Applications to Radio Systems.* June '94.

Othman O. Khalifa received his Bachelor's degree in Electronic Engineering from the Garyounis University, Libya in 1986. He obtained his Master degree in Electronics Science Engineering and PhD in Digital Image Processing from Newcastle University, UK in 1996 and 2000 respectively. He obtained his Master degree in Electronics Science Engineering and PhD in Digital Image Processing from Newcastle University, UK in 1996 and 2000 respectively. He worked in industrial for eight years and he is currently an Associate Professor and Head of the department of Electrical and Computer Engineering, International Islamic University Malaysia. His area of research interest is Communications, Information theory and Coding, Digital image / video and speech processing, coding and Compression, Wavelets, Fractal and Pattern Recognition. Dr Khalifa published more than 100 papers in international journals and Conferences. He is SIEEE member, IEEE computer, Image processing and Communication Society member.