ACTION-TRIGGERED PUBLIC-KEY SYSTEM FOR GSM USING RSA WITH PHONE-DEPENDENT ENCRYPTION

Rehab K. El-Nemr
Computer Science department, Faculty of Media Engineering, German University in Cairo, Egypt
rehab.elnemr@guc.edu.eg

A. Prof. Imane Aly Saroit Ismail, Prof. S. H. Ahmed
Information Technology Department, Faculty of Computers and information, Cairo University, Egypt
iasi63@yahoo.com , **s.hanafy@fci-cu.edu.eg**

Keywords— GSM, Authentication, Ciphering, A3/5/8, RSA, Public key and Digital Certificate

Abstract— Security is a burning issue with intelligent security pausing as the most relevant as it is important in all types of applications which suffer from security related concerns. Accordingly, Security has become a need rather than a luxury. GSM Security flaws have been identified several years ago. Some of these flaws have been mended by the 3GPP but others are left to discussion. In this paper we will integrate a well known technique in the system; Public-key technique. Yet, we will introduce the solutions in a different point of view; they are Action-Triggered, meaning; it will work only if the flaw occurs. The original system will work in normal cases. We will also discuss End-to-End security and propose a mechanism of Key management to provide the subscribers with private calls' option. Phone-Dependent technique is conducted to consider Service provider attacks.

1 INTRODUCTION

Mobile phones are used on a daily basis by hundreds of millions of users, over radio links. Fixed phones offer some level of physical security (i.e. physical access is needed to the phone line for listening in). Unlike a fixed phone, with a radio link, anyone with a receiver is able to passively monitor the airwaves. Therefore it is highly important that reasonable technological security measures are taken to ensure the privacy of user's phone calls and text messages (data) as well to prevent unauthorized use of the service (J. Quirke, 2004).

Global System for Mobile Communication (GSM) specification 02.09 (GSM 02.09) identifies three areas of security that are addressed by GSM as follows:

Authentication of a user: it is the ability for a mobile phone to prove that it has access to a particular account with the operator.

Data and signaling confidentiality: this requires that all signaling and user data are protected against interception by means of ciphering.

Confidentiality of a user: when the network needs to address a particular subscriber, or during the authentication process, the unique IMSI (International Mobile Subscriber Identity) should not be disclosed in plaintext. Thus, someone intercepting communications should not be able to learn if a particular mobile user is in the area.

A more detailed Security features were specified by Motorola Corporation (R. Campbell and D. Mckunas, 2003) in their annual report as follows:

Mutual Authentication: The mobile user and the serving network authenticate each other

Data Integrity: Signaling messages is protected by integrity code

Network to Network Security: Secure communication between serving networks.

User – Mobile Station Authentication: The user and the mobile station share a secret key, PIN (Personal Identification Number)

Visibility and Configurability: Users are notified whether security is on and what level of security is available

Multiple Cipher and Integrity Algorithms: The user and the network negotiate and agree on cipher and integrity algorithms. At least one encryption algorithm exported on world-wide basis

Lawful Interception: Mechanisms to provide authorized agencies with certain information about subscribers

GSM Compatibility: GSM subscribers roaming are supported by GSM security context

2 EXISTING SECURITY SYSTEM

When a subscriber is added to a home network for the first time, a Subscriber Authentication Key (Ki) is assigned in addition to the IMSI to enable the authentication. Ki must be stored in the user's SIM (Subscriber Identity Module). At the network side, the key Ki is stored in the AuC (Authentication Center) (Chengyuan Peng, 2003). SIM is the small smartcard which is inserted into a GSM phone. It contains all of the details necessary to obtain access to a particular account. The SIM card contains the following values: (J. Quirke, 2004)(ETSI TS100 929, November 1999)

- **IMSI**: International Mobile Subscriber Identity – a unique number for every subscriber in the world. It is saved in the SIM.

- **Ki**: the root encryption 128-bit key. This key seeds the generation of all keys and challenges used in the GSM system. The Ki is highly protected, and is only known in the SIM and the network's AuC.

The SIM itself is protected by an optional PIN; The PIN is entered on the phone's keypad, and passed to the SIM for verification. Algorithms used in GSM security architecture are: **A3** (Used in the Authentication procedure), **A8** (Used to generate the Private Key Kc), **A5** (Used in Ciphering).

The two main security features offered by GSM and the role of the above algorithms are discussed in the following subsections.

a. Authentication

Authentication is needed in a cellular system to prevent an unauthorized user from logging into the network claiming to be an authorized mobile subscriber. If this were possible, it would be easily possible to "hijack" someone's account and impersonate that person (or simply making that person pay for the services) (J. Quirke, 2004).

Authentication is a function which is triggered by the network when a subscriber applies for a change of subscriber-related information (location updating) element in the VLR (Visiting Location Register) or HLR (Home Location Register). These work together as a database of user information for all people in the network and the immediate location area. While the HLR stores the user records permanently, the VLR dynamically stores the user records of people in their location area to save time connecting to the HLR. Also it is triggered when a subscriber accesses to a service (call setup, terminating calls, activation or deactivation of a supplementary service) or when a subscriber accesses to the network for the first time after restarting of MSC (Mobile Service Switching Center) or a VLR. Finally it is triggered when the cipher key sequence number mismatch (Chengyuan Peng, 2003). In order to authenticate a user to the network, the SIM card should prove knowledge of the correct K_i but it will be highly insecure to send the K_i as a plaintext to the network for authentication. The K_i in this case can be intercepted. Instead the procedure works as following (O. Benoit1& N. Dabbous, 2004):

1. A connection is attempted between the phone and the network. The phone submits its identity. Where possible, it avoids sending its IMSI in plaintext (to prevent eavesdroppers knowing the particular subscriber is attempting a connection). Instead, it uses its TMSI (Temporary Mobile Subscriber Identity).
2. The network generates a 128-bit random number, known as the RAND and uses the A3 algorithm to mathematically generate an authentication token known as the SRES.
3. The network sends the RAND to the phone to do the same.
4. At the SIM side, a 32-bit SRES is generated which is returned to the network for comparison. If the received SRES matches the network's generated SRES, then the K_i's must be the same (to a high mathematical probability), and the phone has proved knowledge of the K_i and is thus authenticated.

The RAND must obviously be different every time. Otherwise, an attacker could impersonate the user by sending the same SRES. If authentication fails the first time, and the TMSI was used, the network may choose to repeat the authentication with the IMSI. If this fails, the network releases the radio connection and the mobile should consider that SIM to be invalid (O. Benoit1& N. Dabbous, 2004).

b. Ciphering

Ciphering is highly important to protect user confidentiality. It is done to protect both data and signaling information. The purpose of this function is to avoid an intruder to identify a subscriber on the radio path by listening to the signaling exchanges. This function can be achieved by protecting the subscriber's IMSI and any signaling information

elements. Therefore, a protected identifying method should be used to identify a mobile subscriber instead of the IMSI on the radio path. The signaling information elements that convey information about the mobile subscriber identity must be transmitted in ciphered form (Chengyuan Peng, 2003).

The GSM system uses symmetric cryptography - the data is encrypted and decrypted using the same ciphering key – the Kc. The idea is that the Kc should only be known by the phone and the network. If this is the case, the data is meaningless to anyone intercepting it. The Kc should also frequently change, in case it is eventually compromised (J. Quirke, 2004). Whenever the A3 algorithm is run (to generate SRES), the A8 algorithm is run as well. The A8 algorithm uses the RAND and K_i as input to generate a 64-bit ciphering key, the Kc, which is then stored in the SIM and is readable by the phone. The network also generates the Kc and distributes it to the Base Station handling the connection.

At any time, the network can then order the phone to start ciphering the data (once authenticated) using the Kc generated. The network can pick from a number of algorithms to use, as long as the phone supports the one chosen. It can choose from up to 7 different ciphering algorithms (or no ciphering), however it must choose an algorithm the phone indicates it supports. Currently there are 3 algorithms defined – A5/1, A5/2 and A5/3. It should be noted that A5/0 (no encryption) is available for use in countries where there may be political obstacles in supplying cryptographic hardware, such as Middle Eastern or certain former Soviet countries. This allows roaming to continue to work, and also offers these countries the ability to use modern GSM handsets (Bruce Potter, May 2004).

3 EVALUATION OF THE EXISISTING SECURITY MEASURES

There are still some potential threats posed in the GSM system although of these security measures (GSM 02.09)(R. Campbell & D. Mckunas, 2003)(Yong LI, Yin CHEN& T. MA, 2002)(L. Ertaul and B. Kasim, June 2005) summarized as follows:

- Limited encryption scope (Encryption terminated at the base station)
- Insecure key transmission (Cipher keys and authentication parameters are transmitted in clear between and within networks).
- Security through Obscurity- Authentication and encryption *algorithms* were never made public. The whole security model developed in secret which rises suspicion that cryptographic algorithms are weak. Although never published, ciphering algorithm A5 has been reverse engineered by authors in (A. Biryukov and A. Shamir, 2000). Authentication algorithms are also reversed engineered (J. Rao, P. Rohatgi, H. Scherzer and S. Tinguely, 2002).
- End to end security is not provided.
- If track of TMSI is lost then the mobile needs to transmit the IMSI, this can be done by the false base station.
- Using the knowledge of IMSI and using repeated authentication requests, the Ki can be broken.
- Network does not authenticate itself to the phone, making it possible for an attacker to set up false base station.
- Ciphering is optional and is turned on by the base station.
- It is believed that GSM is secure for average users. However it is not secure for high security transmission.

4 ACTION-TRIGGERED PUBLIC-KEY SECURITY SYSTEM (ATPKSS)

In our proposed integration system, public key technique is the main factor. Public-key algorithms are based on number theory. It is asymmetric, involving the use of two separate keys, in contrast to the symmetric conventional encryption, which uses only one key (RSA Labs). Each one of the communicating parties has a pair of keys, "*Public Key*" and "*Private Key*". Those keys are used in both Encryption and Authentication (digital signature) (William Stallings)(Limor Elbaz, 2002).

In this section we will emphasize on some of the above problems and highlight the solutions in our proposed system. Of course, using Public-key technique in mobile communication is not un-explored before but it was not used due to its high computations that cause a delay. But our solutions based on an *Action Triggered* mode, meaning, if a flow occurs, like losing the IMSI for example, the use of public key system is triggered.

System to be proposed is based on the idea of obtaining a digital certificate from a third trusted party i.e: a CA. A digital certificate is an electronic identity, constructed of a public key and an identification of the owner of the corresponding public key. Digital certificates are issued, managed

and revoked by a CA (Limor Elbaz, 2002). Problems attached to the existence or the extinction of a CA is mostly political. Issues like selecting the Certificate Authority (CA) or selecting a certain public-key algorithm that is most suitable for GSM are out of our scope. Proposed system requirements are:

- The SIM/HLR/AuC/VLRs should have Digital certificates along with their public keys.
- The Digital Certificate of the home network should be distributed when a new SIM card is issued to a customer.
- A public key Algorithm should be mounted on the Mobile Station.
- The files in AuC and HLR should be protected against attacks using highly secure procedure of "Password-locking" mechanism in order to protect the users' data (Keys and IMSI).

Problem 1: IMSI sent in a plain text

The GSM specifications have gone to great length to avoid phone's being addressed (i.e. paged) or identifying themselves in plaintext by their IMSI. This is supposed to prevent an eavesdropper listening in, on the initial plaintext stage of the radio communication, learning that a particular subscriber is in the area (and what they are doing). Thus where possible the network pages users by their TMSI and maintains a database mapping TMSIs to IMSIs. If the network somehow loses track of a particular TMSI, and therefore cannot determine who the user is, it must then ask the subscriber for his IMSI over the radio link. Obviously, the connection cannot be ciphered if the network does not know the identity of the user, and thus the IMSI is sent in plaintext (J. Quirke, May 2004).

Triggered Action 1

When this flaw is identified, SIM extracts the HLR public key from its certificate. In SIM-VLR communication, the public key of the VLR is distributed in the initiation process. SIM then encrypts the IMSI using the public-key and sends it to the HLR/VLR. The VLR decrypts the ciphered data using the correspondent private key. This process is illustrated in figure 1.

Problem 2: Network does not authenticate itself to a phone

This is the most serious fault with the GSM authentication system. The network does not have to prove its knowledge of the K_i, or any other authentication context to the phone. Thus it is possible for an attacker to setup a false Network node. Since the authentication procedure initiation is up to the network's discretion, the false network may choose not to authenticate at all, or simply send the RAND and ignore the response. It does not have to activate ciphering either (J. Quirke, May 2004).

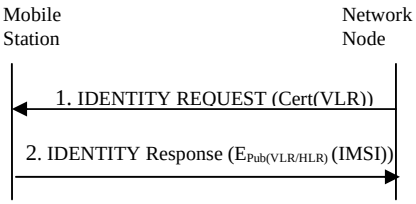

Figure 1: IMSI retreival mechanism

Triggered Action 2

The SIM should have the option to initiate the authentication process, for both Home Network and a Visiting Network as follows:

1. ***Authenticating the Home Network*:** two scenarios can be presented (illustrated in figure 2):
   Scenario A: SIM generates a new RAND and sends it to the Network. The Network encrypts it using its *Private Key* and then sends the ciphered data to the SIM. The SIM then decrypts the ciphered data using the extracted Network *Public key* and compares the two codes. If the two codes do not match then the SIM sends a REJECT_REGISTERATION message and the connection fails.
   Scenario B: authenticity can be proven also by proving the knowledge of K_i, in this case the procedure is the following: SIM sends a RAND to the Network and the network produces the correspondent SRES and sends it back to the SIM. But this procedure is not safe because an attacker can obtain both SRES and RAND and perform a "Known-plaintext attack" to retrieve the K_i. Therefore RAND should be sent encrypted by the Network public key; in this case the attacker can not obtain both RAND and SRES together.

2. ***Authenticating a foreign network***: two scenarios can be presented
   Scenario A: As we mentioned before, authenticity can be proven by proving the knowledge of the K_i. But If the Mobile Station is authenticating a foreign VLR, the Home Network will not send the K_i of the specified SIM in plain. A proposed scenario is to do the following:
   - SIM sends a new RAND along with the TMSI encrypted using the VLR public key.

- VLR decrypts the message and extracts the RAND then encrypts it using the home Network public key and sends it to the HLR/AuC.
- The HLR checks the "Chain of trust" of the VLR and checks its validity. If it is valid, the HLR computes the SRES using RAND and K_i. The Kc is computed as well.
- The Kc and SRES are sent to the VLR encrypted using the VLR public key.
- The VLR decrypts the message and obtains SRES and Kc, encrypts SRES using Kc and sends it to the phone.
- At this stage the SIM has calculated the Kc and uses it to decrypt the message and compares the two SRESs then sends either Accept or Reject RESPONSE.

Since the SIM can not keep all the public keys of the VLRs dealt with, SIM and the VLR should exchange public Keys for future use in the initiation phase.

Scenario B: another scenario to reduce the computation overhead in the SIM is to change the first step in scenario A to the following:

- SIM sends the RAND in plain form to the VLR.

The rest of the steps are repeated.

These processes are illustrated in figures 3, 4 and 5.

Advantages of these two approaches are:

- The VLR authentication relies on the HLR validation procedure now. Note that there is a list of Forbidden Network operators in the HLR. Also the HLR checks the validity of the VLR by sending its information to the CA.
- K_i will never be sent in plain or even encrypted form.
- RAND and SRES are not sent in plain form. So attacks of getting both SRES and RAND to calculate the K_i is not possible now.

Problem 3: Kc is sent in plain form in Roaming

Roaming is defined as the ability for a cellular customer to automatically send & receive data when traveling outside the geographical coverage area of the home network, by means of using a visited network. When a VLR connects to a user, it requests the Kc from the HLR. HLR sends the Kc of a user in plain form to the VLR.

Triggered Action 3

HLR identifies the last Kc being used by the user and encrypts it using VLR public key and sends it to the VLR. The VLR then decrypts it using the correspondent private key. This procedure can be

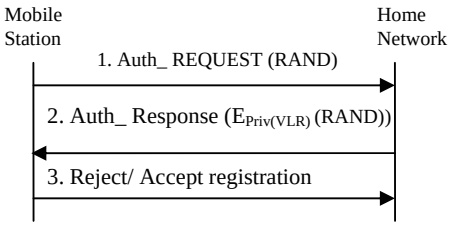

Figure 2: Mobile Station – Home Network Authentication Procedure

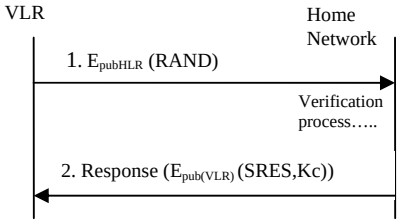

Figure 3 VLR/ HLR connection to get SRES and Kc

applied also if Kc is lost from the VLR. If the last Kc used is not updated in the HLR, then a new RAND should be sent to the SIM to calculate a new Kc taking into consideration that RAND in this case should not be transmitted in plain form. The HLR, however, sends the Kc to the VLR encrypted using VLR public key.

Problem 4: End-to-End security is not available

Although GSM focuses on some of the security aspects addressed by the 3GPP standards but still there is no defined procedure to initiate *end-to-end secure communication* between two users. This is acceptable for average users where speed is the most important factor, but some subscribers will sacrifice this in favor of getting higher security level.

SPC and Phone-Dependent Key

- "*SPC: Special Private Calls*" where a certain subscriber has the ability to transfer data or make calls in a private mode. The data is transferred in an encrypted form between the two users. This option will delay the transfer of data but still will give subscribers, who prefer security over speed, the ability to increase the security level. It should be optional to the customer to subscribe in this option.
- *Use a built-in key in the phone*:

If MS-A would like to communicate with MS-B in a secure manner then the procedure will be partitioned into 2 phases:

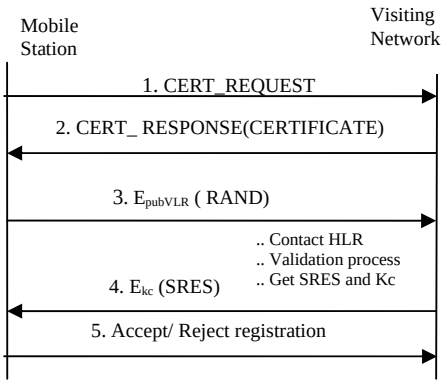

Figure 4 Mobile Station – Visiting Network authentication procedure (Scenario A)

Phase 1 Key Management phase

- MS-A asks the network to send a "secret session key" in order to start a secure session between A and B
- The network generates a secret key, encrypts it using the A-Kc then sends it to A. Also it encrypts the secret key using B-Kc and sends it to B.
- At this point A and B can communicate securely using the secret key sent by the network
- *Key- deletion* procedure should be triggered immediately in the AuC, where *Secret Session Key* is deleted.

Phase 2 Exchanging of Phone-dependent sub-key

For further security (considering the case that there is an attacker exists inside the Service provider Network or attack the service provider Data base), MS-A sends MS-B a phone-dependent Key that is encrypted using the secret session key obtained from the network. Some will argue that an attacker can clone a user and initiate a session with MS-A in order to have the Key *P* to intercept any future communication for MS-A. This can be solved by changing the key *P* for each session. A sub-key P_i is created each time the session is initiated – creating sub-keys from the original P-key:

$$P_i = SUB(P)$$

, where SUB is the function performed over the root *P*-Key to get a new P_i each time. Now, A and B can encrypt their data using both the Session Key *S* and the P_i key or by using P_i key only. It is up to the network operator to use either A5 or another symmetric key algorithm as the encryption algorithm.

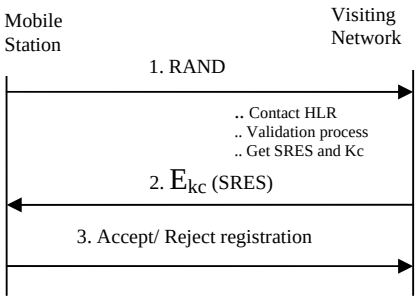

Figure 5 Mobile Station – Visiting Network authentication procedure (Scenario B)

5 PROPOSED SYSTEM ADVANTAGES

Our Proposed system has the following advantages:

- Our main advantage that our system is action triggered due to flaws occurrences.
- A new key parameter is presented that is independent of the SIM and the Network operator; Built-in Key. The Built-in key is the root of other sub-keys.
- IMSI and Kc are not sent in plain form anymore.
- Secure communication between HLR and VLR can be implemented.
- End-to-End secure communication, for non-average users, can be implemented.
- Mutual Authentication is possible.
- Known Security algorithms can be used such as RSA or Elliptic Curves.

In order to apply our system, the SIM components must change to include user certificate, home network public key and a public key algorithm. New SIMs can be provided for the new users of any network or this system can be applied in *future Mobile Communication* systems.

6 IMPLEMENTATION RESULTS

The simulation is implemented in JAVA. Server side and Client side modules are implemented by J2SE v1.5. The codes run on Intel Centrino 1.7 Ghz machine with 512MB RAM. We have implemented the RSA as our public key system for its popularity. Time taken for Encrypting/Decrypting: *IMSI, RAND, Kc and a 64bit session key* is measured to evaluate the delay that will be caused by applying the RSA algorithm.

System parameters like RANDs and K_is are real test data taken from 3GPP technical specification (3GPP TS 55.205 V6.1.0) to test our system. We run the simulation for 100 times and computation times are recorded for 512, 1024 and 2048 bit RSA keys. We recorded the standard Authentication time (Creating both SRES and Kc). We also recorded the time taken to Encrypt/Decrypt data (84 and 160 bytes) using A5. Algorithms are seeded using 20 different RANDs and 20 different K_is.

For an efficient security system to work in a mobile environment, the time taken to generate a new public key pair, key generation process, should be minimized as much as possible. The process of selecting the primes and generating the corresponding encryption and decryption keys is large, but it is worth mentioning that *Key Generation* in our system is done for each run. This is conducted for the sake of testing our system versus several public key values. Table 1 illustrates the average time in milliseconds taken to select p, q, e, d and n.

Table 1

Key size	512 bit	1024 bit	2048
Time	164.4334	1120.894	11333.304

As JAVA calls the garbage collector in undefined periods, which will affect the time records, we eliminated the best and the worst results. In the following, the results are summarized.

Table 2: describes the time taken in m-seconds to encrypt/ decrypt an IMSI (10 and 15 digits) using RSA algorithm.

Table 2

	RSA (average processing time in msec)					
	512 bit key		1024 bit key		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
10	3.19	6.65	28.7	46.48	264.2	383.12
15	4.46	6.7	29.9	46.92	266.12	383.24

Table 3 describes the time taken in m-seconds to encrypt/decrypt a 64 bit Kc using RSA algorithm.

Table 3

Kc	RSA (average processing time in msec)					
	512 bit key		1024 bit key		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
	4.55	6.69	28.7	46.5	265.31	367.643

Table 4 describes the time taken in m-seconds to encrypt/ decrypt a 64 bit Session Key using RSA algorithm.

Table 4

	RSA (average processing time in msec)					
	512 bit key		1024 bit key		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
	2.93	6.56	21.2	46.59	306.77	352.623

Table 5 describes the time taken in m-seconds to encrypt/ decrypt a 64 bit Session Key using A5.

Table 5

SESSION KEY	A5 (average processing time in msec)	
	Encryption	Decryption
64 bit	0.298	0.224

Table 6: describes the time taken in m-seconds for authentication by signing a generated RAND, where Network encrypts the RAND using its Private Key/ SIM decrypts RAND using Network Public Key.

Table 6

	RSA (average processing time in msec)					
	512		1024		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
	6.67	4.46	47.15	28.7	387.91	294.54

Table 7: describes *Authentication Scenario A* with additional step*;* where row 1 denotes that SIM encrypts a 128 bit RAND using network Public key/ Network decrypts RAND using network Private Key. Row 2 denotes that Network encrypts RAND using network private key /SIM decrypts RAND using network public key.

Table 7

	RSA (average processing time in msec)					
	512 bit key		1024 bit key		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
1	4.48	6.66	28.6	46.62	264.88	363.23
2	6.71	4.46	46.7	28.87	350.761	297.24

Table 8.1: describes the time taken in m-seconds for Authentication by proving knowledge *of Ki*; where SIM encrypts RAND using Network Public Key/ Network decrypts RAND using Network Private Key. Table 8.2 Row 1 denotes the time taken to encrypt/decrypt SRES using A5. Row 2 denotes the time taken to create SRES using RAND and Ki.

Table 8.1

	RSA (average processing time in msec)					
	512 bit key		1024 bit key		2048 bit key	
	Enc	Dec	Enc	Dec	Enc	Dec
	4.52	6.75	28.56	46.6	265.50	360.392

Table 8.2

	Average Time in Milliseconds	
	Encryption	Decryption
A5	0.2888	0.2537
SRES	0.20229381	

8 CONCLUSION AND FUTURE WORK

In this paper we discussed some of the flaws occur in the existing GSM security system. We also presented an application for Public Key techniques. Action-Triggered Public Key Security System (ATPKSS). It is a way to solve some of the flaws occur in GSM security system without overloading the system with a whole public key technique. Our approach presents a hybrid system; where the original system works in normal conditions and only when a flaw occurs, the ATPKSS is triggered. RSA is implemented as our public key technique. Time (in milliseconds) is recorded for using RSA with three key lengths; 512 bit, 1024 bit and 2048 bit. By analyzing our results for 512 bit key; the highest delay that will be caused by using ATPKSS is 6.75 milliseconds in average which is a very few price to pay in terms of ensuring security. For 1024 bit key the highest delay will be 47.15 milliseconds and for 2048 the delay is 387.91 milliseconds.

Also we presented a new end-to-end approach where a key agreement phase takes place between the network and the two users first, then in the second phase, the initiating user sends a built-in phone sub-key. The original built in phone key is the root of the sessions' sub-keys. Each time a new session is opened, a function is applied to the root key to obtain a sub-key. The data is transferred between the two users afterwards encrypted by this key only or a combination key between the phone key and the network session key. This will address the problem of attacking the Service provider itself.

Since in reference (Julio Lo`pez and Ricardo Dahab) the authors states that ECC is preferable in mobile systems due to the use of smaller key, we suggest as a further research that an ECC implementation is tested instead of RSA and see whether the time measured is decreased or not.

REFERENCES

J. Quirke, May 2004. Security in the GSM system, http://www.ausmobile.com

GSM 02.09 - Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 version 8.0.1 Release 1999).

R. Campbell and D. Mckunas, 2003. Analysis of Third Generation Mobile Security, Annual Motorola Project Review, Computer Science Dept., University of Illinois.

Chengyuan Peng, 2003. GSM and GPRS Security, Telecommunications Software and Multimedia Laboratory, Helsinki University.

ETSI TS 100 929.Digital Cellular Telecommunication System (Phase 2); Security related network functions. *European Telecommunications Standards Institute.*, November 1999.

O. Benoit1, N. Dabbous, 2004. Mobile Terminal Security, Report in the International Association for Cryptologic Research (IACR) Vol. 21, No. 3.

Bruce Potter, May 2004. GSM Security, Network Security, vol. 2004, no.5, pp.4-5.

Yong LI, Yin CHEN, Tie-Jun MA, Feb 2002. Security in GSM,WWW.GSM-SECURITY.NET/PAPERS/SECURITYINGSM.PDF.

L. Ertaul and B. Kasim, June 2005. GSM Security, Proceedings of the 2005 International Conference on Wireless Networks, ICWN'05.

A. Biryukov and A. Shamir, , April 2000. Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption Workshop 2000, NY.

J. Rao, P. Rohatgi, H. Scherzer and S. Tinguely, May 2002. Partitioning Attacks: Or how to rapidly clone some GSM cards, IEEE Symposium on Security and privacy, Okaland, p. 31.

RSA Labs. RSA PKCS documents, http://www.rsasecurity.com/rsalabs/node.asp?id=2124

William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, ISBN: 0130914290.

Limor Elbaz, October 2002. Using Public Key Cryptography in Mobile Phones, Discretix Technologies Ltd,VP. Research.

3GPP TS 55.205 V6.1.0 (2003-12): Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8.

Julio Lo`pez and Ricardo Dahab. An overview of Elliptic Curve Cryptography, Institute of Computing, State University of Campians, Brazil.