www.icgst.com

Action-Triggered Public-Key cryptography for GSM systems with Phone-Dependent end-to-end encryption

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

Imane Aly Saroit Ismail
Information Technology department,
Faculty of Computers and
information, Cairo University
iasi63@yahoo.com

S. H. Ahmed
Vice dean,
Faculty of Computers and
information, Cairo University
s.hanafy@fci-cu.edu.eg

Abstract

Security is a burning issue and intelligent security will remain relevant, as it is important in all types of applications. GSM Security flaws have been identified several years ago. Some of these flaws have been fixed by the 3GPP but others are left to discussion. In this paper we will integrate a very well known technique in the system, namely Public-key technique. Yet, we will introduce the solutions in a different point of view. These solutions are Action-Triggered, meaning; it will work only if the flaw occurs. That will leave the original system working in normal cases. End-to-End security will be discussed also and a mechanism of Key management is proposed if this service is requested by the customer. Phone-Dependent technique is conducted to consider Service provider attacks.

Key-Words: *Authentication, Ciphering, SIM, Ki, VLR, A3/5/8, Public key and Digital Certificate*

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 [1].

Global System for Mobile Communication (GSM) specification 02.09 [2] 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 (such as text messages and speech) 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 (unciphered). 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 [3] as follows:

- **Mutual Authentication:** The mobile user and the serving network authenticate each other
- **Data Integrity:** Signaling messages between the mobile station and RNC (Radio Network Controller) 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 (KASUMI)
- **Lawful Interception:** Mechanisms to provide authorized agencies with certain information about subscribers
- **GSM Compatibility:** GSM subscribers roaming in 3G network are supported by GSM security context (vulnerable to false base station)

The rest of the paper is organized as follows: Section 2 details the existing GSM security system. Section 3 evaluates the existing security measures, illustrating its flaws. Section 4 explains the concept of public key techniques. Section 5 proposes the new system named; Action-triggered public-key security system (ATPKSS). Section 6 and 7 evaluates the proposed system logically and using simulation results respectively. Finally conclusion and future work are illustrated in section 8.

2. Existing GSM 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) [4].

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 phone on its own has no connection with the network.

The SIM card contains the following values [1,5]:

- **IMSI:** International Mobile Subscriber Identity – a unique number for every subscriber in the world. It includes information about the home network of the subscriber and the country of issue. This information can be read from the SIM provided there is local access to the SIM (normally protected by a simple PIN code).
- $\mathbf{K_i}$: the root encryption key. This is a randomly generated 128-bit number allocated to a particular subscriber that 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.

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). In fact, this was possible in some earlier cellular systems [1].

Authentication is a function which is triggered by the network when a subscriber applies for a change of subscriber-related information 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. The subscriber-related information element includes location updating. It is also triggered when the cipher key sequence number mismatch [4].

In order to authenticate a user to the network, the SIM card should prove knowledge of the correct $\mathbf{K_i}$ but it will be highly insecure to send the $\mathbf{K_i}$ as a plaintext to the network for authentication. The $\mathbf{K_i}$ in this case can be intercepted. Instead the procedure works as follows [6]:

1. The phone submits its identity. All potential messages used at the start of a connection contain an identity field. 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**.
3. Then the network uses the **A3** algorithm to mathematically generate an authentication token known as the **SRES**.
4. The network sends the **RAND** to the phone to do the same.
5. At the SIM side, a 32-bit **SRES** is generated which is returned to the network for comparison.
6. If the received SRES matches the network's generated SRES, then the $\mathbf{K_i}$**'s** must be the same (to a high mathematical probability), and the phone has proved knowledge of the $\mathbf{K_i}$ and is thus authenticated.

The **RAND** must obviously be different every time. Otherwise, if it were the same, 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 that fails, the network releases the radio connection; and the mobile should consider that SIM to be invalid (until switch-off or the SIM is re-inserted) [6].

B. Ciphering

Ciphering is highly important to protect user confidentiality. It is done to protect both data and signalling information. The purpose of this function is to avoid an intruder to identify a subscriber on the radio path by listening to the signalling exchanges. This function can be achieved by protecting the subscriber's IMSI and any signalling information elements. The signalling information elements that convey information about the mobile subscriber identity must be transmitted in ciphered form [4].

The GSM system uses symmetric cryptography - the data is encrypted using an algorithm which is 'seeded' by the ciphering key – the **Kc**. This same **Kc** is needed by the decryption algorithm to decrypt the data. 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. The method of distributing the **Kc** to the phone is closely tied in with the authentication procedure previously discussed [1]. Whenever the **A3** algorithm is run (to generate SRES), the **A8** algorithm is run as well (in fact the SIM runs both at the same time). The **A8** algorithm uses the RAND and $\mathbf{K_i}$ as input to generate a 64-bit ciphering key, the **Kc**, which is then stored in the SIM and is readable by the phone.

At any time, the network can then order the phone to start ciphering the data using the **Kc** generated. The network can pick from a number of algorithms to use, as

long as the phone supports the one chosen.

The network 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**. **A5/1** and **A5/2** were the original algorithms defined by the GSM standard and are based on simple three clock-controlled LFSRs (Linear Feedback Shift Registers). **A5/2** was a deliberate weakening of the algorithm for certain export regions, where **A5/1** is used in countries like the US, UK and Australia. **A5/3** was added in 2002 and is based on the open Kasumi algorithm defined by 3GPP. It should be noted that **A5/0** (another way of describing 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 [7].

3. Evaluation of the existing security measures

There are still some potential threats posed in the GSM system although of these security measures [2, 3, 8, 9].

- Limited encryption scope (Encryption terminated at the base station, in clear on microwave links).
- 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 Alex Biryukov, Adi Shamir and David Wagner [10]. Also Wagner, Goldberg and Briceno released a paper describing a weakness in COMP128 that allowed them to clone GSM phones [7].
- End to end security is not provided.
- 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 (although it is not easy or cheap to build false base station).
- If track of TMSI is lost then the mobile needs to transmit the IMSI, this can be done by the 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. Public key Techniques

In the proposed integration system, public key technique is the main factor. Public-key algorithms are based on mathematical functions rather than on substitution and permutation (based on number theory). But more important, public key cryptography is asymmetric, involving the use of two separate keys, in contrast to the symmetric conventional encryption, which uses only one key [11].

Each one of the communicating parties has a pair of keys, namely "*Public Key*" and "*Private Key*". The relation between the keys is used as follows:

- **Public key encryption** - to send encrypted data to someone, the sender encrypts the data with the receiver's **public key**, which may be known by anybody, and the receiver decrypts it with his/her (corresponding) **private key**, known only to the recipient. Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data.
- **The reverse scheme**, sometimes called **private key encryption**, is also useful, being used for **digital signatures**. A person can digitally sign data by encrypting it with his/her private key. The receiver can use the signer's **public key** to verify the digital signature. Given that data verified with a public key could have been signed only with the corresponding private key, which is possessed only by its owner [12, 13].

In the proposed system a public key algorithm should be mounted on the Mobile Station with A5, A8 and A3. This can be provided either in the next generation in mobile communication operators or can be provided to the new users in the existing system. The issue of selecting a certain public-key algorithm that is most suitable for GSM is out of our scope.

Reduction in key size brings the advantage of less storage area and less required bandwidth, which are important requirements of wireless network architectures [14]. 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 Certificate Authority (CA) [13]. Problems attached to the existence or the extinction of a CA is mostly political.

Before describing our proposed system, we have to mention its requirements as the following:

- 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.

5. Action-triggered public-key security system (ATPKSS)

In this section we introduce our proposed system; called ATPKSS. 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 will 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 should be triggered. And according to [16], elliptic curves cryptosystem is suitable for mobile communications. Issues like selecting the CA (Certificate Authority) or initiating the CA is out of our scope.

5.1.1 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 – i.e. the nature of communication can be known prior to ciphering – SMS, voice call, location update, etc). Thus where possible the network pages users by their TMSI (Temporary Mobile Subscriber Identity) and maintains a database in the VLR 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 [1].

Triggered Action 1 SIM will extract the HLR public key from its certificate. In SIM-VLR communication, the public key of the VLR is distributed in the initiation process. The SIM then encrypts the IMSI using the public-key and send it to the HLR/VLR. The VLR in this case will decrypt the ciphered data using the correspondent private key. Authentication of VLR will be discussed later in problem 2.

5.1.2 Problem 2: Network does not authenticate itself to a phone.

This is the most serious fault with the GSM authentication system. The authentication procedure described before does not require the network 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 with the same Mobile Network Code as the subscriber's network.

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. The attacker can set the cell reselection parameters of his false base station to values that will highly encourage his 'victims' to camp on it. [1]

Triggered Action 2 The SIM should have the option to initiate the authentication process, for both Home Network and a Visiting Network. Two solutions are proposed:

1. **Authenticating the Home Network**: two scenarios can be presented:

Scenario A: SIM will extract the public key of the Home Network. Then SIM will send a RAND code (that is changed every time the authentication process is initiated) to the Network. The Network will encrypt the RAND code using its private key and then send the ciphered data to the SIM. The SIM then decrypt the ciphered data using the Network *Public key* and compares the two codes. If the two codes do not match then the SIM will send a REJECT_REGISTERATION message and the connection will fail. This process should be optional for the user to initiate. This procedure is illustrated in figure 1.

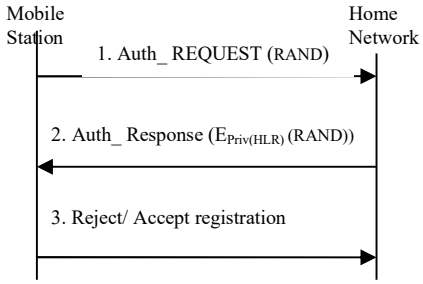

Figure 1 Mobile Station – Home Network Authentication Procedure

Scenario B: authenticity can be proven also by proving the knowledge of K_i, in this case the procedure will be the following: SIM will send a RAND to the Network and the network will produce the correspondent SRES and send 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 HLR 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 (Known only by the SIM and the Home AuC). But If the Mobile Station is authenticating a foreign VLR, the Home Network will not send and reveal the K_i of the specified SIM. A proposed scenario is to do the following:

- Since the SIM will not keep all the public keys for the VLRs dealt with, SIM and the VLR should exchange public Keys for future use in the initiation phase.
- SIM will send a RAND along with the TMSI encrypted using the VLR public key.
- VLR will decrypt the message and extract the RAND.
- VLR will encrypt the RAND using the Home Network public key and send it to the HLR/AuC.
- The HLR will check the "Chain of trust" of the VLR and check its validity, if valid, compute the SRES using RAND and K_i. The HLR will compute also the Kc using RAND and K_i.
- The Kc and SRES is sent to the VLR encrypted using

the VLR public key. VLR/HLR connection is illustrated in figure 2.

- The VLR will decrypt the message and obtain SRES and Kc.
- The VLR will encrypt SRES using Kc and send it to the phone.
- At this stage the SIM has calculated the Kc and will use it to decrypt the message and compare the two SRESs then send either Accept or Reject RESPONSE.

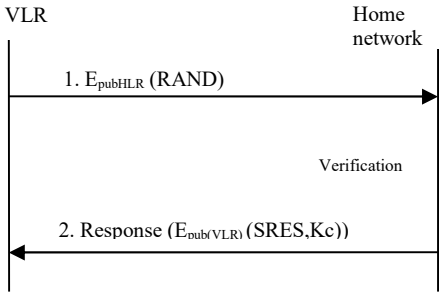

Figure 2 VLR/ HLR connection to get SRES and Kc

Scenario B: another scenario to reduce the computation overhead in the SIM is to do the following:

- SIM will send the RAND in plain form to the VLR.
- The VLR will encrypt it using HLR public key and send the encrypted RAND to the HLR.
- The HLR will check the "Chain of trust" of the VLR and check its validity, if valid, Compute the SRES using RAND and K_i. The HLR will compute also the Kc using RAND and K_i.
- The Kc and SRES is sent to the VLR encrypted using the VLR public key.
- The VLR will decrypt the message and obtain SRES and Kc.
- The VLR will encrypt SRES using Kc and send it to the phone.
- The SIM will decrypt the message and compare the two SRESs and send either Accept or Reject RESPONSE.

Messages between the Mobile Station and the Visiting Network for both Scenario A and B are illustrated in figure 3 and figure 4 respectively.

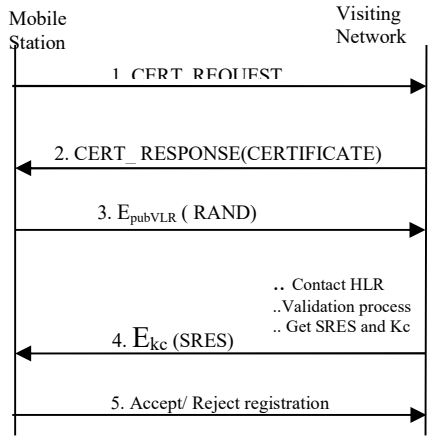

Figure 3 Mobile Station – Visiting Network authentication procedure (Scenario A)

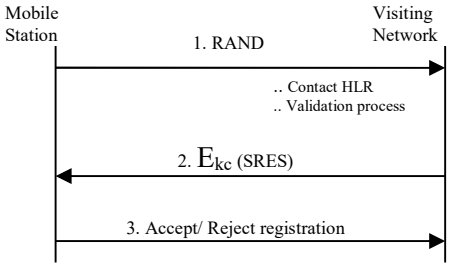

Figure 4 Mobile Station – Visiting Network authentication procedure (Scenario B)

Advantages of these two approaches are:

- The VLR authentication will rely on the HLR validation procedure now. Note that there is a list of Forbidden Network operators in the HLR. Also if CA is available then the HLR will check 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.

5.1.3 Problem 3 *Kc is sent in plain form in Roaming*

Roaming is defined as the ability for a cellular customer to automatically make & receive voice calls, send & receive data, or access other services when travelling outside the geographical coverage area of the home network, by means of using a visited network. When a VLR connect 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 will identify the last Kc being used by the user and encrypt it using VLR public key. The VLR then will decrypt it using the correspondent private key. This procedure can be applied also if Kc is lost from the VLR that according to this send the HLR a request for Kc. 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.

5.1.4 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 favour of getting higher security level.

Facilities: SPC and Phone-Dependent Key

- Add a new option that is sold to the customer, we will call it "**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 along the way 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.

- **Use a built-in key in the phone**: If SIM-A would like to communicate with SIM-B in a secure manner then the procedure will be partitioned into 2 phases:

Phase 1 Key Management phase

- SIM-A asks the network to send a "secret session key" in order to start a secure session between A and B.
- The network will generate a secret key and encrypt it using the Kc of A and send it to A then encrypt the secret key using the Kc of B and send 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 at once in the AuC, where Session Secret Key is deleted.

This phase is illustrated in figure 5.

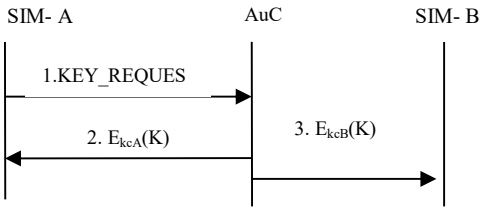

Figure 5 Key distribution of end-to-end Session Key

Phase 2 Exchanging of Phone-dependent sub-key

For further security (if there is an attacker exists inside the Service provider Network or attack the service provider information Data base), SIM-A will send SIM-B a phone-dependent Key that is encrypted using the secret session key obtained from the network. A and B can encrypt their data using both the "Secret Key S" and the "Phone dependent P" key or by using "Phone dependent" key only: $C = E_{S+P}(Plain)$

Where C is the result of encrypting the Plain data using both the Session key (S) and the Phone dependent key (P).

Some will argue that an attacker can clone a user and initiate a session with SIM-A in order to have the Key P. Then the attacker can reveal any future communication for SIM-A. This can be solved by changing the key P for each session. A sub-key is created each time the session is initiated – creating sub-keys from the original P-key. We can view the phone dependent key P as the K_i where it is the root of all session keys. It is up to the network operator to use either A5 or another symmetric key algorithm as the encryption algorithm.

6. Proposed system versus previous public-key solutions

Public-key based authentication and key exchange protocols described in [15] has the following enhancements and flaws:

- Known and accepted security algorithms such as DES and MD5 are used in these protocols.
- Classical public key cryptography techniques such as the Diffie-Hellman (DH) protocol are used in the proposed system. These techniques are characterized by higher key sizes and lower speed performance, which are not acceptable in mobile network environment where the mobile equipment has smaller storage area and limited computing power.
- No protocol for performing secure communication between the foreign and the home network authentication centers is defined.

Public-key based authentication and key exchange protocols described in [13] are mainly for WAP users.

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 will be the root of other sub-keys.
- IMSI is 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.
- Network can authenticate itself to the user. And the user will have the choice to authenticate the network.
- Known Security algorithms can be used such as RSA or Elliptic Curves.

Due to the potential delay of using public key algorithms, it can be limited to certain actions only, such as sending the IMSI or authenticating a VLR. In order to apply our system, the SIM components must change to include user certificate, home network public key and a public key algorithm. For commercial reasons, new SIMs can be provided for the new users of any network or this system can be applied in *future Mobile Communication* systems.

7. Implementation results

The simulation is implemented in JAVA language. 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. Time taken for the following operations is measured to evaluate the delay that will be caused by applying the RSA algorithm:

1. Encrypting/decrypting the IMSI.
2. Encrypting/decrypting the RAND.
3. Encrypting/ decrypting the Kc.
4. Encrypting and decrypting a 64 bit session key.

RSA is selected as our Public Key system because it is a well known algorithm that has proven its efficiency.

System parameters like RANDs and K_is are real test data taken from 3GPP technical specification [17] to test our system. We run the simulation for 100 times and computation times are recorded for 512 and 1024 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 Kis.

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 tables, the results are summarized.

Table 1: The time taken in m-seconds to encrypt/ decrypt an IMSI using RSA algorithm.

IMSI	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512 BIT KEY		1024 BIT KEY	
	ENC	DEC	ENC	DEC
10	3.195	6.657	28.726	46.487
15	4.461	6.705	29.897	46.923

Table 2: The time taken in m-seconds to encrypt/decrypt a 64 bit Kc using RSA algorithm.

KC	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512 BIT KEY		1024 BIT KEY	
	ENC	DEC	ENC	DEC
64 BIT	4.559	6.699	28.746	46.561

Table 3: The time taken in m-seconds to encrypt/ decrypt a 64 bit Session Key using RSA algorithm.

KEY	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512 BIT KEY		1024 BIT KEY	
	ENC	DEC	ENC	DEC
64 BIT	2.937	6.563	21.249	46.593

Table 4: The time taken in m-seconds to encrypt/ decrypt a 64 bit Session Key using A5.

Session Key	A5 (AVERAGE PROCESSING TIME IN MSEC)	
	ENC	DEC
64 BIT	0.29870002	0.22414863

Table 5: The time taken in m-seconds for *Authentication Scenario A*, where Network encrypts a 128 bit RAND using its Private Key/ SIM decrypts RAND using Network Public Key.

	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512		1024	
	ENC	DEC	ENC	DEC
128 BIT	6.676	4.465	47.158	28.704

Table 6: *Authentication Scenario A* with additional step*;* where row 1 denotes that SIM encrypts a 64 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.

	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512 BIT KEY		1024 BIT KEY	
	ENC	DEC	ENC	DEC
1	4.488	6.667	28.606	46.629
2	6.711	4.461	46.752	28.877

Table 7.a: The time taken in m-seconds for *Authentication Scenario B*; where SIM encrypts RAND using Network Public Key/ Network decrypts RAND using Network Private Key. Table 7.b 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.

RAND	RSA (AVERAGE PROCESSING TIME IN MSEC)			
	512 BIT KEY		1024 BIT KEY	
	ENC	DEC	ENC	DEC
128 BIT	4.529	6.758	28.564	46.658

(a)

	AVERAGE TIME IN MSEC	
	ENC	DEC
A5	0.2888551	0.2537865
SRES	0.20229381	

(b)

We can conclude from these results that the time taken to apply the ATPKSS is very small:

- Using 512 and 1024 bit key, the highest delay that will be caused by using ATPKSS to authenticate a network to a user using RSA algorithm is 6.75 and 47.15 milliseconds in average respectively, which is a very few price to pay in terms of ensuring security.
- Encrypting a 64 bit session key with the RSA algorithm will take an average of 6.5630045 milliseconds for 512 bit key and 46.5936592 milliseconds for 1024 bit key. This time is taken only in the initial session setup when the session key is distributed. If the operator decided to use A5 as the *Symmetric Algorithm* in the SPC option, the average time taken to encrypt/ decrypt a stream of 84 bytes of data is 9 milliseconds which is a very reasonable delay due to the service offered.

8. Conclusion and future work

Public-key based protocols, with a mature public key infrastructure (PKI), will enable all the involved entities such as users, network operators and service providers to have full range of state-of the-art security features including non-repudiation services, mutual authentication and anonymity [18].

In this paper a new system is proposed to solve some of the flaws occurring in GSM security system. This system is called; Action-Triggered Public Key Security System (ATPKSS). This system uses public key technique without overloading the network. It is a hybrid system; where in normal condition the original algorithms and protocols work, only when a flaw occurs, the solution is triggered.

To prove the effectiveness of the proposed system, we have implemented simulations for it using RSA as our public key algorithm and also simulation for the original algorithms; then measured the time taken for each operation. It is found that the time taken to apply the ATPKSS is very small (with maximum of 47 msec using 1024-bit key length for authentication or

encryption); which is a very few price to pay in terms of ensuring security. In order to apply our system both Mobile Stations and Network entities must change to include digital certificates and a public key algorithm. The software implementation the RSA algorithm can be mounted in both MS and Network HLR/VLR. The computations will be faster if the algorithm is implemented as a H/W chip. In this case, it will require changing the Mobile Equipment (ME) to include it. And due to the evolution in ME industry, it is possible to do that.

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.

For further research; we suggest testing the Elliptic Curve Public Key instead of RSA and see whether the time measured is decreased or not.

REFERENCES

[1] Jeremy Quirke, "Security in the GSM system", May 2004, http://www.ausmobile.com

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

[3] Roy Campbell and Dennis Mckunas, "Analysis of Third Generation Mobile Security", Annual Motorola Project Review, Computer Science Dept., University of Illinois at Urbana-Champaign, 2003.

[4] Chengyuan Peng, "GSM and GPRS Security", Telecommunications Software and Multimedia Lab, Helsinki University of Technology, 2003.

[5] 3GPP TS 43.020 V6.2.0 (2005-09): "Security related network functions", Technical Specification Group Services and system Aspects, Release 6.

[6] Olivier Benoit1, Nora Dabbous, "Mobile Terminal Security", Report in the International Association for Cryptologic Research (IACR) Vol. 21, No. 3, Fall 2004.

[7] Bruce Potter, "GSM Security", Network Security, vol. 2004, no.5, pp.4-5, May 2004.

[8] Yong LI, Yin CHEN and Tie-Jun MA, "Security in GSM", February 2002 www.gsm-security.net/papers/securityingsm.pdf.

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

[10] A. Biryukov and A. Shamir, "Real Time Cryptanalysis of A5/1 on a PC", proceedings of the 7th International Workshop Fast Software Encryption (FSE 2000), Springer, vol.1978.

[11] RSA Data Security Inc., "Public Key Cryptography standard ", Technical standards, 2004, http://www.rsasecurity.com/rsalabs/node.asp?id=2125

[12] William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 2003, ISBN: 0130914290.

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

[14] Jurgen Fell, Ing. Klaus Peter Graf, "Application of Public key Procedure for the Aeronautical Telecommunication Network.", Munchin University, Germany, Diploma Thesis, March 2000.

[15] C. Park, "On Certificate Based Security Protocols for Wireless Mobile Communication Systems", IEEE Network Sept/Oct 1997. pp.:50-55

[16] Kristin Lauter, "The advantages of elliptic curve cryptography for wireless security", IEEE Wireless Communications magazine, vol.11, no.1, pp.62-67, February 2004.

[17] 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 (3GPP TS 55.205 version 6.1.0 Release 6).

[18] Kyungah Shim and Young-Ran Lee, "Security flaws in authentication and key establishment protocols for mobile communications", Applied Mathematics and Computation, vol.169, no.1, pp.62-74, October 2005.

Rehab Khaled EL-Nemr. She is graduated from Faculty of Computers and Information, Cairo University, 2001. She will soon finish her Master thesis in the field of Mobile Network Security. She is currently a teaching assistant in Computer Science department, Faculty of Media Engineering, German University in Cairo.

Imane Aly Saroit Ismail. She obtained her B.Sc in 1985, M.Sc in 1990 and Ph.D in 1994, all from Faculty of Engineering, Communication department, Cairo University. She worked in Cairo University since 1989, She is currently an associate professor in Information Technology department, Faculty of Computers and Information, Cairo University.

S.H. Ahmed. She obtained her Ph.D in 1980 from university of Toulouse, France, M.SC in 1977 and B.SC in 1971 both from Faculty of Engineering, Communication department, Cairo University. She is a professor and currently a vice dean, in Faculty of Computers and Information, Cairo University.