American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 16, May, 2023

SECURITY OF CELLULAR COMMUNICATION SYSTEMS!

Abdugafur Hotamov
Associate Professor of the Samarkand
Branch of TUIT named after Muhammad al-Khwarizmi.
abdugafur.xotamov@gmail.com

Shahlo Rasulova
Student of the Samarkand Branch of TUIT named after
Muhammad al-Khwarizmi

Annotation
First generation cellular communication systems such as NMT, TACS and AMPS had little security capability and this resulted in significant levels of fraudulent activity that harms both subscribers and network operators. A number of incidents of great significance have highlighted the sensitivity of analog telephones to eavesdropping on radio lines. The GSM system has many security features that are designed to provide the subscriber and network operator with a greater level of protection against fraudulent activity.

Keywords: protection level, access network, identifier, security aspects, Internet banking.

Introduction

Authentication mechanisms ensure that only conscientious subscribers with honest equipment, that is, not stolen or non-standard, will be granted access to the network. Once a connection has been established, the information on the link is transmitted in an encrypted form to avoid eavesdropping. The privacy of each subscriber is protected, guaranteed that their identity and location are protected. This is achieved by assigning a Temporary Mobile Subscriber Identity (TMSI) to each user, which changes from call to call. Thus, there is no need to transmit the International Mobile Subscriber Identity (IMSI) over the air interface, which makes it difficult for an eavesdropper to identify and locate the user.

The first and simplest level of protection against mobile phone fraud is a Personal Identification Number (PIN) designed to protect against fraudulent use of stolen SIM cards. In a SIM card, the PIN code has the form of a four to eight digit number. The user may have the option to disable this level of protection. The SIM card can also store a second four to eight digit decimal code, known as PIN2, to protect certain features that are available to the subscriber. Once the PIN, and if required PIN2, is entered correctly, the maintenance entity will have access to the data stored in the SIM card. The technical requirements also define the procedures to be followed when a PIN is entered incorrectly. After three consecutive

incorrect PIN attempts, the SIM card is blocked and further attempts to enter the PIN code are ignored, even if the SIM card is removed from the maintenance entity. The SIM card can be unlocked by entering an eight-digit decimal code known as PUK (Personal Unlock Key), which is also stored in the SIM card. After 10 incorrect attempts to enter the PUK code, the SIM card is permanently blocked.

The procedure for establishing an authentication or authentication (authentication) is carried out under the control and at the initiative of the VLR. To carry it out, a request-response scenario is used, in which the VLR sends to the MS a special random number RAND, which is one of the input parameters of the A3 algorithm used in the SIM card to calculate the SRES response value. Another input parameter of the A3 algorithm is the secret key Ki contained in the SIM card. The Ki key is not readable from the SIM and this is one of the main aspects of GSM security.

The VLR, in which the subscriber registers, sends a request to the AuC of the subscriber's home network, in response to which the AuC sends a set of triplets, each of which contains RAND, SRES and the encryption key Kc. RAND is a random number, SRES is calculated in AuC by the A3 algorithm based on the secret key Ki and RAND, and Kc is the radio interface encryption key and is calculated by the A8 algorithm based on Ki and RAND. These triplets will later be used by the VLR for authentication and encryption. Thus, all calculations using the Ki key occur inside AuC, on the network side, and inside SIM, on the subscriber side, which eliminates Ki leakage and interception by an attacker.

In modern communication equipment, the Ki keys are loaded into the AuC in encrypted form, and this excludes access to the keys even from the operator's technical staff. The authentication procedure can be performed on outgoing calls, incoming calls, network registration, packet data transfer, SMS sending or receiving, and location update. Each telecom operator independently determines in which cases the VLR will perform authentication.

The authentication procedure begins after a transparent channel is organized between MS and MSC for the exchange of service information. The VLR selects the first triplet and sends its RAND to the mobile station along with the triplet number, which will be referred to as CKSN - Ciphering Key Sequence Number, also known as the encryption key number Kc. On the MS side, algorithm A3 calculates the SRES, which is returned to the VLR, where it is compared with the SRES value from the composition of the triplet obtained from the AUC. The identity of the two SRES is a sign of the authenticity of the subscriber. The triplet in the VLR is marked as used, and another triplet will be used next time. After all the triplets are used up, the VLR requests a new portion of triplets from the AuC. The secret algorithm A3 makes it relatively easy to generate SRES from RAND and Ki, but makes it difficult to determine Ki from SRES and RAND or pairs of SRES and RAND, which provides high resistance to compromise.

Once the identity of the subscriber has been verified, thus protecting both the subscriber and the network operator from the influence of fraudulent access, the user must be protected from eavesdropping. This is achieved by encrypting the data transmitted over the air

interface using the second key Kc and the initially secret algorithm A5. Kc is generated during authentication using Ki, RAND and the A8 secret algorithm, which is also stored in the SIM card. Like Algorithm A3, A8 is not unique and can also be chosen by the operator. The Kc keys for each user are calculated in the AuC of the home network and transmitted to the VLR as part of a set of triplets, where each triplet and, accordingly, the Kc key is assigned a key number - CKSN. In some implementations, algorithms A3 and A8 are combined into a single algorithm, A38, which uses RAND and Ki to generate Kc and SRES. Unlike A3 and A8, which may be different for each individual operator, A5 is selected from a list of 7 possible options.

Before encryption, there is a negotiation phase that determines which version of A5 will be used. If the network and the mobile station do not share A5 versions, the communication must continue in open mode or the connection must be dropped. Algorithm A5 uses the 64-bit key Kc and the 22-bit TDMA frame number to calculate two 114-bit encryption words, BLOCK1 and BLOCK2, used in transmission and reception, respectively. Encryption words - EXORed with 114 bits of data in each package. Because the encrypted data is computed using the TDMA frame number, the words change from burst to burst and do not repeat over the course of a hyperframe (approximately 3.5 hours).

Before starting encryption, the mobile station (MS) sends to the VLR the encryption key number CKSN, which has been stored in its memory since the last authentication procedure. The CKSN does not contain secret data, but only serves to let the MS tell the network which key Kc it "remembers". After that, the VLR sends a command to the MS to enable encryption and transmits to the base station (BTS) the Kc key from the triplet that corresponds to the CKSN number received from the MS. Thus, an agreement is reached between the MS and the VLR on the choice of an encryption key without transmitting the key itself over the air interface.

Some transmissions on the radio link cannot be encrypted. For example, after an initial assignment, the mobile station must transmit its network ID before encryption can be activated. This would obviously allow the eavesdropper to determine the subscriber's location by intercepting this message. This problem is solved in GSM by the introduction of a temporary mobile subscriber identity (TMSI), which is an "alias" assigned at each mobile station by the VLR. The TMSI is transmitted to the mobile station during the previous encrypted communication session, and it is used by the mobile station and the network for any subsequent paging and access procedures. The TMSI is only valid within the area served by a specific VLR.

Although GSM was developed as a standard with a high level of protection against fraudulent activity, there are various types of attacks on GSM.

Initially, the security of GSM networks was based on the principle of "security through obscurity", but by 1994 the main details of the A5 algorithm were known.

When encrypted traffic is transmitted via GSM, it contains system information that is known to the cryptanalyst in advance. With this information, a plaintext attack can be applied. In December 2010, at the World Congress of Hackers, Sylvain Munaut and Karsten Nohl

demonstrated the cracking of the Kc key and the subsequent decryption of voice traffic[1][. To speed up the attack by brute-forcing the key from the known plaintext, they used a precomputed method with the creation of rainbow tables.

For authentication in GSM networks, it is necessary for the subscriber to work in the GSM network to be authenticated in it. In general, a multi-factor authentication scheme is used, in which a SIM card is used. The process begins when the user enters the PIN code and continues with identification on the network. Authentication is performed using the A3 algorithm. In order to exclude the identification of the subscriber by intercepting messages transmitted over the radio channel, each subscriber of the communication system is assigned a "temporary identity card" _ temporary international identification number of the TMSI user, which is valid only within the LA location zone.

This TMSI will be used for all subsequent accesses to the system. If a mobile station moves to a new location area, its TMSI must be transmitted along with the identification number of the LAI zone in which the TMSI was assigned to the subscriber. This scheme is shown in Figure 1.

In turn, the necessary information about subscribers is stored in the databases of the subscriber's network operator. Information that relates a subscriber to his network (authentication parameters, subscription levels, additional services, current or last used network and location) is stored in the location register of HLR's own subscribers. The VLR guest subscriber register, in turn, contains data on all subscribers who are currently using the network of this operator. IMSI is transmitted to HLR, HLR, in turn, checks whether it has such a subscriber, and, if so, whether it is blocked. If everything is in order, then this subscriber is registered in the VLR and from that moment can make calls. Large operators may have not one, but several HLRs and VLRs running in parallel. These registers are part of the authentication center (authentication) AiS (Authentication Centre) of the subscriber operator and provides sets of security parameters (RAND, SRES, Ki),

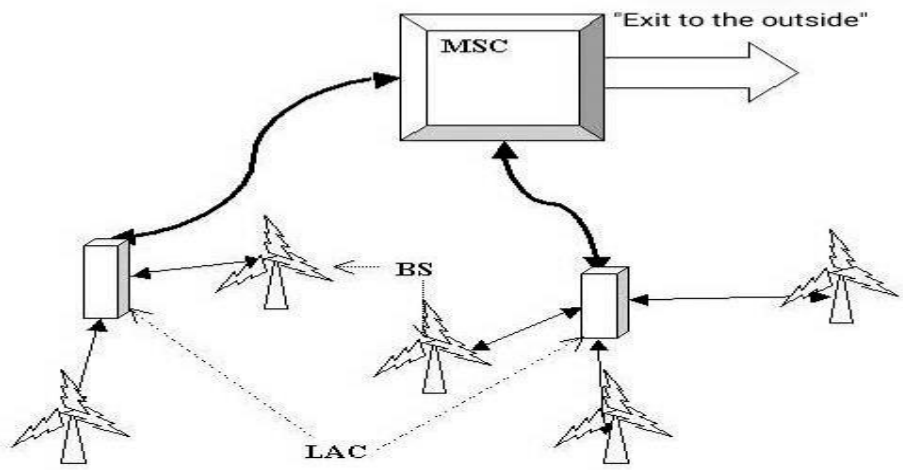

Fig.1 _ Data transmission scheme in GSM network

American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 16, May, 2023

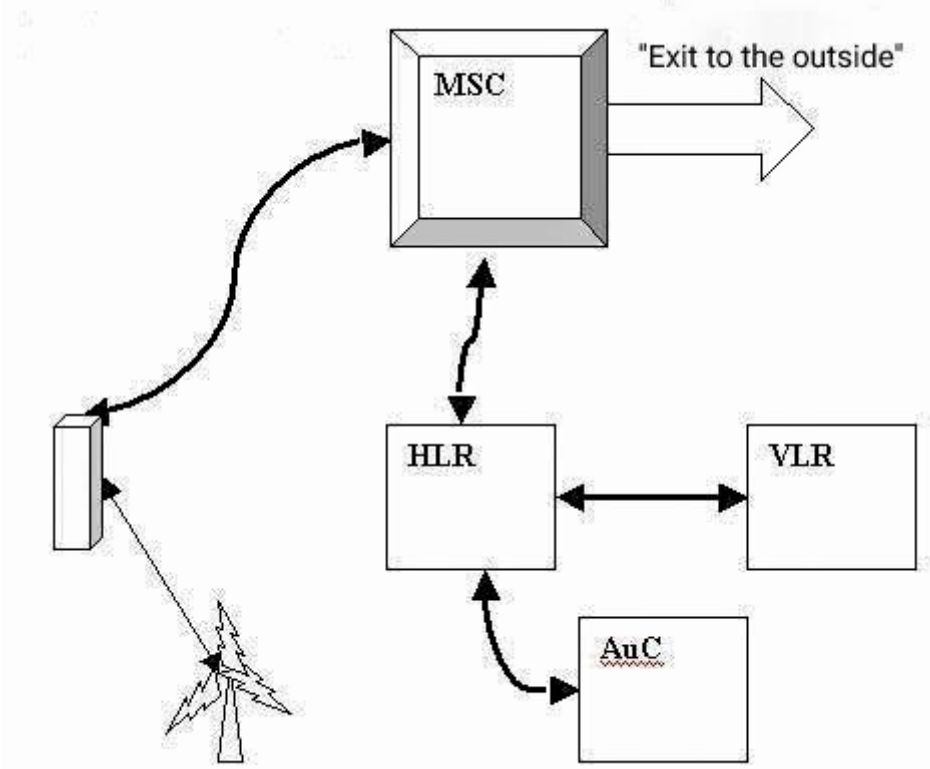

Fig.2 _ Scheme of transmission of key information in the GSM network

Usually, the main subscriber operator provides other operators with five sets of RAND/SRES/Kc. The location register of its own subscribers knows the location of all mobile stations of this operator at any time. Moreover, the values of RAND/SRES/Kc are never used twice. The AiS authentication center works in close contact with HLR, which provides the information necessary to verify the authenticity of a subscriber using the network, namely, it receives the RAND value and generates a pair of SRES (response) and Cs (encryption key) values using the A3, A8 algorithms and the Ki secret key of this subscriber. The scheme for implementing the authentication process is shown in Figure 3. If the subscriber is outside the range of the subscriber's main operator, the authentication center transmits sets of corresponding RAND, SRES and Cs values to other operators during roaming.

The subscriber's primary operator is defined as the operator who provided the subscriber with a SIM card. At the same time, the subscriber's main operator transmits to other operators five sets of RAND/SRES/Kc values, and not the Ki key, which protects the subscriber and his main operator from an unscrupulous telecom operator. Thus, the authentication center provides authentication of the mobile station. This allows you to protect the network from the possibility of unauthorized access to it and listening to the transmitted information.

It is worth noting that virtually all the security of the GSM standard is based on the knowledge of the unique secret key Ki, which is used to calculate the SRES response values (for authentication in the network) and the Kc key for stream encryption of the subscriber's

conversation with the A5 algorithm (specifications A5/1 and A5/2). Thus, the calculation of this key completely compromises the subscriber. It is after the attacker gets access to this key that he will be able not only to listen to the conversations of this user, but also to make calls at the expense of this subscriber, since now he will be identified by the system as the real owner of the SIM card.

Conclusion

Although cellular operators categorically deny the technical possibility of remote initiation of an outgoing call and sending SMS from the subscriber's phone, the phenomenon is widespread, and the problem is described on a significant number of Internet resources. The fact that this is not related to the equipment or software of the subscriber indicates that it is possible to disable the service via the USSD command. Violation of the principle of non-repudiation in cellular communications has far-reaching social consequences, both in proving committed offenses using cellular data, and in using it for authorization on websites and Internet banking.

Used Literature

1. Gatchin Yu.A., Sukhostat V.V. Information security theory and information security methodology. - St. Petersburg: SPbGU ITMO, 2010. - 98 p.
2. Malicious program [Electronic resource]. - Access mode: http://en.wikipedia.org/wiki/Malware_program
3. Traffic analyzer [Electronic resource]. - Access mode: Shr://gy. wikipedia.org/wiki/Traffic_Analyzer
4. Spam [Electronic resource]. - Access mode: http://ru.wikipedia.org/wiki/Spam.
5. Phishing [Electronic resource]. - Access mode: ht:tp://ru.wikipedia. org/wiki/Phishing.
6.Worldwide Smartphone Shipments Top One Billion Units for the First Time [Electronic resource]. - Access mode: http://www.idc.com/getdoc.
7. Review of Android threats for 2013 by Doctor Web [Electronic resource]. - Access mode: http://www.freedrweb.com/show.