http://doi.org/10.35784/iapgos.2877 *received: 02.02.2022 | revised: 16.03.2022 | accepted: 28.03.2022 | available online: 31.03.2022*

METHODS FOR ENSURING DATA SECURITY IN MOBILE STANDARDS

Serhii Moroz, Anatolii Tkachuk, Mykola Khvyshchun, Stanislav Prystupa, Mykola Yevsiuk
Lutsk National Technical University, Faculty of Computer and Information Technologies, Department of Electronics and Telecommunications, Lutsk, Ukraine

Abstract. *The analysis of mobile communication standards is carried out, the functional structure and interfaces of interaction between the structural elements of the cellular network are considered. To understand the principle of communication according to the GSM standard, a block diagram of a mobile switching center (MSC), base station equipment (BSS), control and service center (MCC), mobile stations (MS) is presented. The main algorithms for ensuring the confidentiality and security of mobile subscribers' data, in different types of standards, as well as the vulnerabilities of information flows are considered. In particular, the following dangerous types of attacks have been identified, to which mobile network subscribers are sensitive: sniffing; leakage of personal data; leakage of geolocation data; spoofing; remote capture of SIM-card, execution of arbitrary code (RCE); denial of service (DoS). It is established that the necessary function of the mobile network is the identification of subscribers, which is performed by IMSI, which is recorded in the SIM card of the subscriber and the HLR of the operator. To protect against spoofing, the network authenticates the subscriber before starting its service. In the case of subscriber identification, the subscriber and the network operator are protected from the effects of fraudulent access. In addition, the user must be protected from eavesdropping. This is achieved by encrypting the data transmitted over the radio interface. Thus, user authentication in UMTS, as well as in the GSM network, is carried out using encryption with a common key using the "hack-response" protocol (the authenticating party sends a random number to the authenticated party, which encrypts it according to a certain algorithm using a common key and returns the result back).*

Keywords: mobile communication, radio communication equipment, encryption, authentication

METODY ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH W STANDARDACH MOBILNYCH

Streszczenie. *Przeprowadzana jest analiza standardów komunikacji mobilnej, rozważana jest struktura funkcjonalna i interfejsy interakcji między elementami strukturalnymi sieci komórkowej. Aby zrozumieć zasadę komunikacji w standardzie GSM, przedstawiono schemat blokowy centrali ruchomej (MSC), wyposażenia stacji bazowej (BSS), centrum sterowania i obsługi (MCC), stacji ruchomych (MS). Rozważane są główne algorytmy zapewniające poufność i bezpieczeństwo danych abonentów telefonii komórkowej w różnych typach standardów, a także podatności na przepływ informacji. W szczególności zidentyfikowano następujące niebezpieczne rodzaje ataków, na które podatni są abonenci sieci komórkowych: sniffing; wyciek danych osobowych; wyciek danych geolokalizacyjnych; podszywanie się; zdalne przechwytywanie karty SIM, wykonanie dowolnego kodu (RCE); odmowa usługi (DoS). Ustalono, że niezbędną funkcją sieci komórkowej jest identyfikacja abonentów, która jest realizowana przez IMSI, która jest zapisywana na karcie SIM abonenta i HLR operatora. Aby zabezpieczyć się przed podszywaniem się, sieć uwierzytelnia subskrybenta przed uruchomieniem usługi. W przypadku identyfikacji abonenta, abonent i operator sieci są chronieni przed skutkami nieuprawnionego dostępu. Ponadto użytkownik musi być chroniony przed podsłuchem. Osiąga się to poprzez szyfrowanie danych przesyłanych przez interfejs radiowy. Tak więc uwierzytelnianie użytkownika w UMTS, jak również w sieci GSM, odbywa się z wykorzystaniem szyfrowania wspólnym kluczem z wykorzystaniem protokołu „hack-response" (strona uwierzytelniająca wysyła do strony uwierzytelnianej losową liczbę, która ją szyfruje zgodnie z określnym algorytmem używając wspólnego klucza i zwraca wynik).*

Słowa kluczowe: komunikacja mobilna, sprzęt radiokomunikacyjny, szyfrowanie, uwierzytelnianie

Introduction

Mobile communications are currently viewed as a necessity, and mobile communications technologies are the most in-demand and rapidly growing. Mobile communication systems are developing at a very fast pace. Considering the evolution of mobile communication systems, we come to the concept of "generations" [2]. The first to be fully digital were second-generation (2G) mobile communication systems. They have brought significant benefits in terms of offering improved services, capacity, and quality to subscribers. GSM (Global System for Mobile communication) refers to 2G technology and is the fundamental technology on which the technologies of existing mobile communication systems have grown.

The increase in the number of users and the expansion of the volume of services has led to the creation of the concept of third-generation (3G) systems that will allow communication, exchange of information, and the provision of various entertainment services focused on a wireless terminal. The development of such services has already begun for 2G systems, but to support these services, the system must have a high capacity and bandwidth of radio channels, as well as interoperability between systems. An example of a 3G system is the Universal Mobile Telecommunications System (UMTS) [17].

4G is the fourth generation of cellular communications. Unlike previous generations, namely the third, 4G does not support traditional circuit-switched telephony services. 4G uses IP telephony, that is, packet switching. For telephony services, calls and messages can be switched over existing 2G and 3G networks. The 4G standard allows information to be transmitted at a speed five to seven times higher than that of 3G [18]. The main difference between 4G networks and earlier ones is that 4G technology is based entirely on packet data transfer protocols, while 3G combines both packet switching and circuit switching. For transmission in 4G, VoLTE technologies are provided [15]. The fifth generation of 5G mobile communications, operates on the basis of telecommunications standards, more modern than the existing 4G / IMT-Advanced standards. 5G will provide higher bandwidth than 4G technologies, which will enable greater availability of mobile broadband and the Internet of Things [3].

Let's consider how the user is authenticated and the encryption key is generated in GSM networks (Fig. 1).

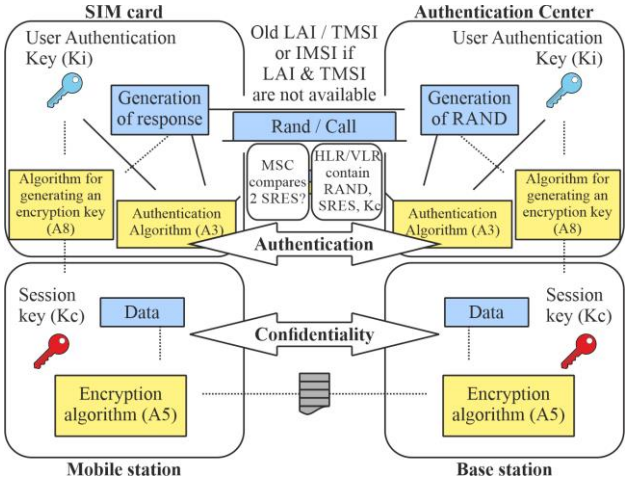

Fig. 1. User authentication and encryption key generation in GSM networks

Figure 1 shows schematically the following steps:

1. The phone connects to the network.
2. To confirm its identity, the phone sends a special identification code TMSI (Temporary Mobile Subscriber Identity).
3. The Authentication Center (CA) generates a 128-bit random number RAND and sends it to the Mobile Station (MS).
4. MS encrypts the received RAND using its private key Ki and the A3 authentication algorithm.

5. MC takes the first 32 bits from the sequence obtained in the previous step (SRES (signed response)) and sends them back to the DA.
6. The CA performs the same operation and receives a 32-bit XRES (expected response) sequence.
7. CA compares SRES and XRES. If both values are equal, the phone is considered authenticated.
8. MS and CA calculate the session encryption key using the private key Ki and the key generation algorithm A8 Kc = A8ki (RAND).

1. Literature review

Consider the process of encryption and authentication in the GSM network. In addition to IMSI, the SIM card stores a randomly generated sequence "Ki", which it returns only in a hashed form. Ki is stored in the HLR of the operator and is not transmitted in the open [10]. The authentication process is based on the principle of "four-way handshake":

1. The subscriber performs Location Update Request, then provides IMSI.
2. The network sends a pseudo-random RAND value.
3. The phone's SIM card hashes Ki and RAND according to the A3 algorithm. A3 (RAND, Ki) = SRAND.
4. The network hashes Ki and RAND by algorithm A3.
5. If the value of SRAND on the part of the subscriber coincided with the calculated on the network side, then the subscriber has been authenticated (Fig. 2).

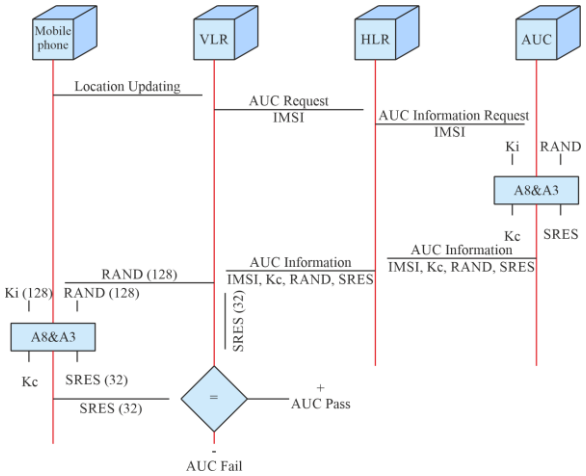

Fig. 2. Authentication procedure scheme

In order to achieve the required level of security, algorithm A3 must be a unidirectional function [7]. This means that the calculation of SRES for known Ki and RAND should be simple, and the reverse – the calculation of Ki for known RAND and SRES – should be as complex as possible. This determines the level of security of the system. The value calculated by the A3 algorithm must be 32 bits long [4]. Cryptographic methods make it possible to achieve a high level of security by simple means. GSM uses common methods to protect all data: user information, signal transmission, message transmission, and system signal transmission [1]. When the authenticity 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 data transmitted over the radio using the key Kc and secret algorithm A5 (Fig. 3) [19].

Kc is generated during authentication using Ki, RAND, and the secret algorithm A8, which is stored on the SIM card. Like the A3 algorithm, the A8 is not unique and can also be generated by an operator [21]. The Kc keys for each user are calculated by the AuC of the home network and transmitted to the VLR as part of a set of triplets, where each triplet and, accordingly, the key Kc, 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 [9]. Unlike A3 and A8, which may be different for each individual operator, A5 is selected from a list of 7 possible options. The encryption is preceded by an information exchange phase, during which it is determined which version of the A5 will be used. If the network and the mobile station do not have common versions of A5, the connection must continue in open mode or the connection will be lost. Algorithm A5 uses a 64-bit key Kc and a 22-bit TDMA frame number to compute the two 114-bit encryption words BLOCK1 and BLOCK2, which are used in transmission and reception, respectively [8]. Encryption words – EXORed with 114 bits of data in each frame. Because the encrypted data is computed using the TDMA frame number, the words change from frame to frame and are not repeated during the hyper frame (~ 3.5 hours). Before starting the encryption, the mobile station (MS) sends to the VLR the number of the CKSN encryption key, which is stored in its memory since the last authentication procedure. CKSN does not contain secret data, but serves to allow the MS to tell the network which key Kc it "remembers" [5]. The VLR then sends a command to the MS to enable encryption and transmits to the base station (BTS) the key Kc from the triplet that corresponds to the CKSN number received from the MS. Thus, the choice of the encryption key is agreed upon between the MS and the VLR without transmitting the key itself over the radio interface [20].

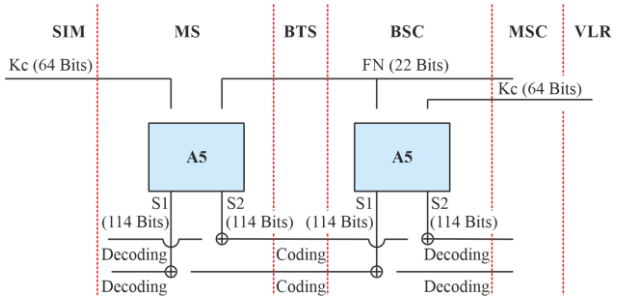

Fig. 3. Encryption and decryption procedure in the GSM standard

The GSM network is characterized by the following restrictions in ensuring information security:

- one-way authentication (provides for user authentication only). This is the reason for the lack of protection, for example, against attack by a false base station BTS;
- there is no mechanism for ensuring message authentication, protecting data integrity;
- fixed security mechanisms without the possibility of flexible shifts in order to enhance protection;
- The data is encrypted only between the mobile station (MS) and the base station (BTS). In the section between the BTS and the base station controller BSC, this data is transmitted in cleartext.

In UMTS, as well as in GSM, the temporary TMSI is used to protect the privacy of the location and to ensure the confidentiality of the IMSI in the area of the CC core network. Similar temporary identifiers are used in the area of the KP core network. To distinguish them from TMSI, the term Packet Temporary Mobile Subscriber Identity (P-TMSI) is used here.

When the connection is established, the temporary TMSI / P-TMSI is periodically changed. Since the temporary identifier is local in nature, then, as in GSM, it must be accompanied by the identifier of the location area. Therefore, the Local Area Identity (LAI) location area identifier is added to the TMSI, and the Routing Area Identity (RAI) routing area identifier is added to the P-TMSI.

Each location area LA (Local Area) is uniquely identified by the identifier LAI, consisting of:

LAI = MCC + MNC + LA code, where MCC is the mobile country code (three digits),

MNC – mobile network code (2–3 digits),

LA is a number that identifies this area.

The KP core network area has its own location registration procedure, which is based on the concept of the RA (Routing Area) routing area. The RA is defined similarly to the LA (as the area within which the UE can move without the routing area update procedure). At the same time, the RA region is a "subset".

2. Researches methodology

Consider mutual authentication of users and networks. UMTS provides mutual user and network authentication. The 3G network structure can be integrated into a system with many different terrestrial radio access technologies, which in turn requires network authentication [11]. The authentication mechanism is based on a master key (master key) K, which is shared between the USIM and the home network database. This 128-bit key never becomes visible between two points on the network. Along with mutual authentication, encryption and integrity keys are generated [12]. At the same time, the principle of cryptography (Kirchhoff's principle) is fulfilled in limiting the duration of using a permanent key to a minimum and using temporary keys [13]. The authentication procedure starts after the user is identified in the serving network by the procedure for ensuring the privacy of the location of the mobile station [16]. User identification is carried out as a result of signaling messages containing TMSI or P-TMSI (in exceptional cases IMSI) to the VLR or SGSN [6, 14]. In Fig. 4 shows a diagram of mutual authentication.

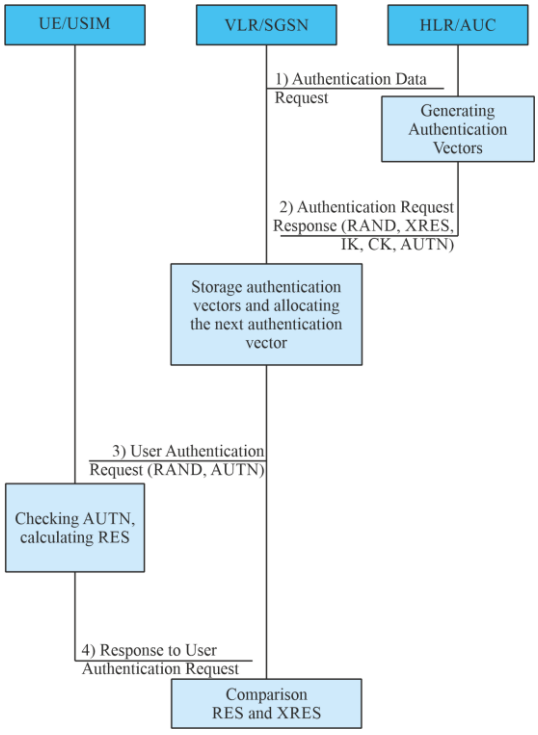

Fig. 4. Mutual authentication framework

In message 1, the VLR or SGSN sends a request for user authentication data to the AUC. This message includes the user ID IMSI. Based on the key K, the AUC authentication center generates and transmits to the HLR authentication vectors for the user with the IMSI.

Each authentication vector contains:

1. Random number RAND (hail);
2. Expected response to the hail, XRES;
3. Encryption key, CK (Cipher Key);
4. Integrity key, IK (Integrity Key);
5. Parameter (label) of network authentication AUTN (An Authentication Token).

In message 2 (response to a request for authentication data), the HLR sends the authentication vector back to the VLR or SGSN. Messaging 1 and 2 are exchanged using the SS7 MAP mobile application protocol. Message 3 (User Authentication Request) contains two parameters from the Authentication Vector, RAND and AUTN.

This message 3 is transmitted to the subscriber identification module USIM, which is located in a protected environment from unauthorized access (to a UMTS smart card – UICC, UMTS Integrated Circuit Card). The USIM user uses the AUTN parameter value to verify the authenticity of the connected network. The USIM user uses RAND to compute the RES response to the user's authentication request.

Message 4 (response to user authentication request) contains the parameter RES. This message is sent back from the UE to the VLR / SGSN where RES is compared to the expected XRES value. If RES and XRES match, the network verifies the identity of the user.

3. Results

In Fig. 5 shows a scheme for generating an authentication vector in HLR / AUC for generation 3G networks. The Authentication Center contains the user's master keys and, based on the international mobile station identifier IMSI, generates authentication vectors for the user. Note that in a GSM network, such a key generates an authentication vector from two parameters – a revocation and an encryption key. Here the number of authentication vector parameters is greater.

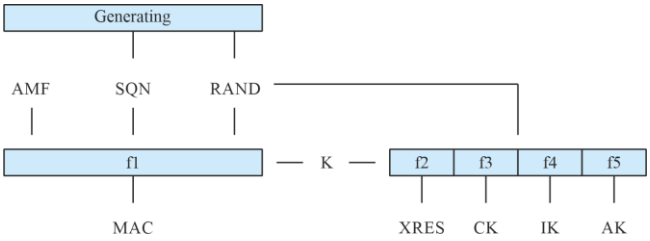

Fig. 5. Generation of the authentication vector: SQN (Sequence Number) – the sequence number of the authentication is used to protect against the "retry" threat; AK (Anonymity Key) – the key used to encrypt SQN; AMF (Authentication Management Field) – administrative control field of authentication, can be used to specify multiple encryptions; MAC (Message Authentication Code) – message authentication code, MAC = f (K, AMF, SQN, RAND)

Five one-way functions are used to compute the authentication vector – f1, f2, f3, f4, f5. The f1 and f5 functions are used to authenticate the network, and the f2 function to authenticate the user. The AV authentication vector, in addition to the AUTN authentication parameter, the XRES response (function f2), also includes the encryption key CK (function f3) and the integrity key IK (function f4): {\ displaystyle AV = RAND \ | XRES \ | CK \ | IK \ | AUTN}. Network Authentication Option {\ displaystyle AUTN = SQN \ oplus AK \ | AMF \ | MAC}.

The protection of a subscriber in the 4G generation of cellular communication is that in the process of servicing it is hidden with temporary identifiers. To close data in LTE networks, streaming encryption is used by superimposing a pseudo-random sequence on open information using the XOR operator. These networks use the principle of tunneling connections to ensure security within the network. S1 and X2 packets can be encrypted using IPsec ESP, and signaling messages on these interfaces are encrypted. At the moment of connection or activation of the user equipment (UE) in the network, the network starts the authentication procedure and AKA (Authentication and Key Agreement). The purpose of this procedure is to mutually authenticate the subscriber and the network and generate an intermediate KASME key. The algorithm for authentication and key generation is shown in Fig. 6.

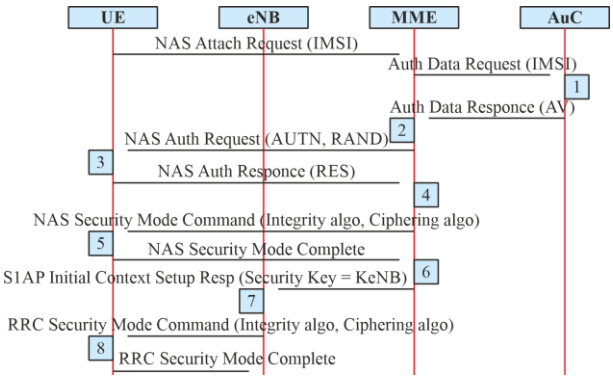

Fig. 6. Authentication and key generation diagram

Step 1. Request for a network connection from a mobile station (UE). The MME requests authentication data related to a specific IMSI by sending an Authentication Data Request. The AuC / HSS selects the PSK associated with a specific IMSI and computes the PSK authentication data. AuC / HSS sends back AV with Authentication Data Response.

Step 2. MME gets IK, CK, XRES, RAND, and AUTH from AV. MME sends AUTH and RAND with Authentication Request to UE.

Step 3. The UE authenticates the NW by checking the received AUTH. Then it calculates IK, CK, RES, XMAC from its security key, AMF, (OP), AUTH and RAND. She sends RES with an Authentication response.

Step 4. After receiving the RES, the MME compares it with XRES and if they match, then the authentication was successful, otherwise the MME sends an Authentication failure to the UE. MME resets DL NAS counter. Calculates KASME, KeNB, Knas-int, Knas-enc. Sends the NAS security mode command (integrity algorithm, encryption algorithm, NAS keyset ID, UE security function) with the integrity protected but not encrypted using Knas-inc.

Step 5. After the NAS receives the security mode command, the UE calculates KASME, KeNB, Knas-int, Knas-enc.

Step 6. After the NAS receives the security mode command from the UE, the MME sends the KeNB to the eNB with the S1AP initial setting of the initial context (security key).

Step 7. After receiving KeNB, eNB calculates Krrc-int, Krrc-enc, Kup-enc. It then sends the RRC security key command with the AS integrity of the algorithm and the AS encryption algorithm.

Step 8. After receiving the RRC command of the security key, the UE calculates Krrc-int, Krrc-enc, Kup-enc. The UE sends the RRC the executed encryption key to the eNB.

After all the described actions, all NAS and AS messages will be reliably protected and encrypted, in contrast to user data, which will only be encrypted. The LTE security architecture defines a security mechanism for both the NAS and AS layers (figure 7).

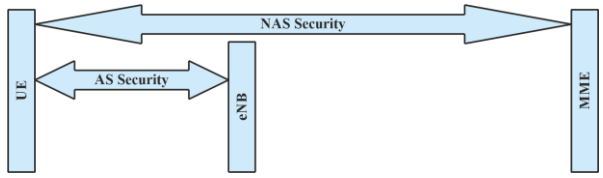

Fig. 7. Security layers

NAS (Non-Access Stratum) security. Made for NAS messages and belongs to the UE and MME. In this case, integrity is required when transmitting NAS messages between the UE and the MME, protected and encrypted with an optional NAS security header.

AS security (Access Stratum). Implemented for RRC and user data plane belonging to the UE and eNB. The PDCP layer on the UE and eNB sides is responsible for encryption and integrity protection. RRC messages are integrity protected and encrypted, however, U-Plane data is only encrypted.

In 5th generation networks, the trust in the elements of the network decreases as the elements move away from the core of the network. This concept influences the solutions implemented in the 5G security architecture. Thus, we can talk about a 5G network trust model that determines the behavior of network security mechanisms. From the user's side, the trust domain is formed by the UICC and USIM. On the network side, the trust domain has a more complex structure. The radio access network is subdivided into two components – DU (Distributed Units) and CU (Central Units) (Fig. 8).

Together they form the gNB – the radio interface of the 5G network base station. DUs do not have direct access to user data, since they can be deployed in segments of unprotected infrastructure. CUs, on the other hand, should be deployed in protected network segments, since they are responsible for terminating the traffic of AS security mechanisms. At the core of the network is the AMF, which terminates the traffic of the NAS's security mechanisms. In 5th generation networks, the authentication procedure has two components: primary and secondary authentication. Primary authentication is required for all user devices connecting to the network. Secondary authentication can be performed upon request from external networks if the subscriber connects to those. After the successful completion of the primary authentication and the generation of a shared key K between the user and the network, KSEAF is extracted from the key K – special anchor (root) key of the serving network. Subsequently, keys are generated from this key to ensure the confidentiality and data integrity of the RRC and NAS signaling traffic.

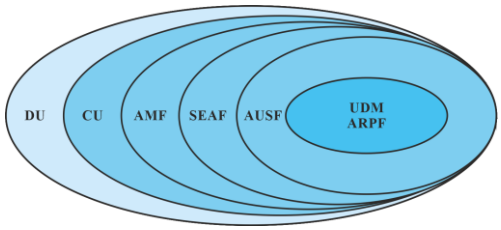

Fig. 8. Components of a 5G radio access network

Initial authentication procedure. On 5G networks, EAP-AKA and 5G AKA are the standard primary authentication mechanisms. Let's split the primary authentication mechanism into two phases: the first is responsible for initiating authentication and choosing an authentication method, the second is for mutual authentication between the user and the network (Fig. 9).

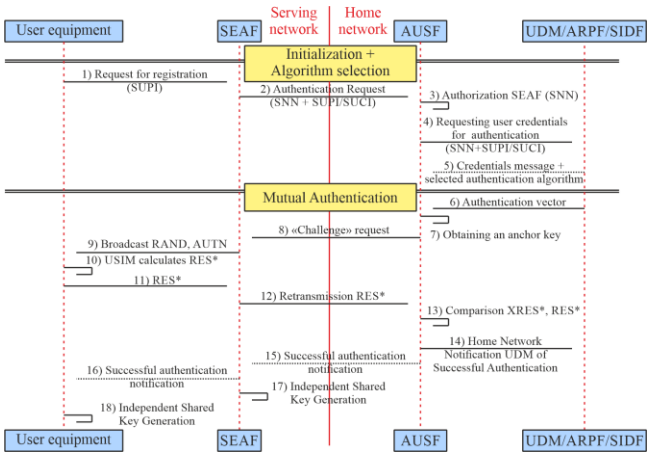

Fig. 9. Initial authentication procedure 5G

Initiation. The user submits a SEAF registration request that contains the user's hidden subscription identifier SUCI.

SEAF sends to AUSF an authentication request message (Nausf_UEAuthentication_Authenticate Request) containing SNN (Serving Network Name) and SUPI or SUCI.

The AUSF checks if the SEAF requestor is allowed to use the given SNN. If the serving network is not authorized to use this SNN, then the AUSF responds with an authorization error "Serving network not authorized" (Nausf_UEAuthentication_Authenticate Response).

Authentication credentials are requested from AUSF in UDM, ARPF, or SIDF over SUPI or SUCI and SNN. Based on SUPI or SUCI and user information, UDM / ARPF chooses an authentication method that will be used further and issues user credentials.

Mutual authentication. When using any authentication method, the UDM / ARPF network functions MUST generate an Authentication Vector (AV). EAP-AKA: UDM / ARPF first generates an authentication vector with AMF splitting bit = 1, then generates CK 'and IK' from CK, IK, and SNN and composes a new AV authentication vector (RAND, AUTN, XRES *, CK ', IK '), which is sent to AUSF with the instruction to use it only for EAP-AKA. 5G AKA: UDM / ARPF obtains the KAUSF key from CK, IK, and SNN, and then generates 5G HE AVangl. 5G Home Environment Authentication Vector). The 5G HE AV authentication vector (RAND, AUTN, XRES, KAUSF) is sent to AUSF with the instruction to use it for 5G AKA only.

The AUSF then obtains the anchor key KSEAF from the KAUSF key and sends a request to SEAF "Challenge" in a "Nausf_UEAuthentication_Authenticate Response" message containing also RAND, AUTN, and RES *. Next, RAND and AUTN are transmitted to the user equipment using a secure NAS signaling message. The user's USIM calculates RES * from the received RAND and AUTN and sends it to SEAF. SEAF will relay this value to AUSF for verification.

AUSF compares the XRES * stored in it and the RES * received from the user. In case of a match, AUSF and UDM in the operator's home network are notified of successful authentication, and the user and SEAF independently generate a KAMF key from KSEAF and SUPI for further communication.

Secondary authentication. The 5G standard supports optional secondary authentication based on EAP-AKA between the user equipment and external data network. In this case, the SMF acts as an EAP authenticator and relies on the external network AAA server to authenticate and authorize the user (Figure 10).

- Mandatory primary user authentication occurs on the home network and develops a common NAS security context with AMF.
- The user sends a session request to the AMF.
- AMF sends a request to establish a session in the SMF with the user's SUPI.
- SMF verifies user credentials in UDM using the provided SUPI.
- SMF sends a response to a request from AMF.
- SMF starts the EAP authentication procedure to obtain permission to establish a session from the AAA server of the external network. To do this, the SMF and the user exchange messages to initiate the procedure.
- The user and the AAA server of the external network then exchange messages to authenticate and authorize the user. The user sends messages to the SMF, which in turn exchanges messages with the external network via the UPF.

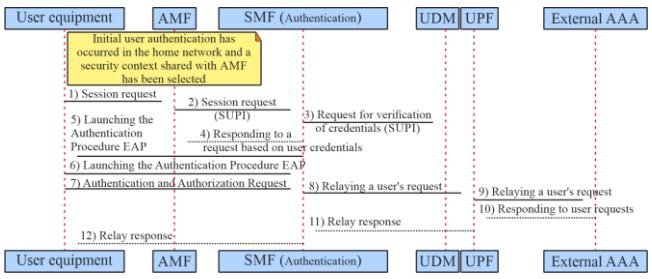

Fig. 10. Secondary authentication procedure 5G

The presented researches allow us to carry out the comparative analysis of different generations of mobile communication from the point of view of safety. In particular, studies of data encryption and authentication procedures for various mobile networks have been conducted. The conducted research will make it possible to identify the main vulnerabilities in the process of establishing a mobile connection and propose measures to eliminate the identified vulnerabilities.

4. Conclusions

As a result of the study, the following types of threats to mobile networks were identified and classified.

A. Unauthorized access to sensitive data (breach of confidentiality).

A1. Eavesdropping: An intruder intercepts messages without being detected.

A2. Masquerading: an intruder tricks an authorized user by posing as a legitimate system in order to obtain confidential information from the user, or an intruder tricks a legitimate system by posing as an authorized user in order to obtain system services or confidential information.

A3. Traffic analysis: the intruder monitors such data as time, the volume of messages, source, and recipient of messages in order to determine the location of the user or find out important information.

A4. Browsing: An intruder browses the stored data in search of sensitive information.

A5. Leakage: An intruder obtains sensitive information through legitimate access to data.

A6. Interference: An intruder observes the system's response by sending requests to it. For example, an intruder can initiate a connection and then monitor the radio interface for data such as the source and recipient of messages, the volume of messages.

B. Unauthorized manipulation of important data (violation of integrity). Manipulation of messages: A message can be deliberately altered, inserted, duplicated, or destroyed by an intruder. Network disruption (resulting in a denial of service or reduced availability).

B1. Intervention: An intruder can prevent an authorized user from serving by deliberately interfering with traffic, signaling, or control data.

B2. Resource exhaustion: An intruder can prevent an authorized user from being served by creating an overload.

B3. Misuse of privileges: A user or service network uses its priorities to obtain unauthorized service or information.

B4. Abuse of services: An offender may abuse certain special services or facilities in order to gain an advantage or cause disruption to the network.

C. Repudiation: A user or network is giving up the actions that took place. Unauthorized access to services.

C1. An intruder can gain access to the service masquerading as a user or network object.

C2. A user or a network object can gain unauthorized access to the service without using their access rights.

Most of the threats to mobile generations have been addressed. However, attackers are looking for new and new vulnerabilities in communication standards. That is why the analysis of the security architecture of various communication technologies is important for counteracting illegal access to mobile network data. The following studies, it is planned to highlight ways to protect the information flows of mobile networks with virtual technical functions (VTF) and their evolution to generations 6G and above.

References

[1] Al-Tawil K., Akrami A.: A new authentication protocol for roaming users in GSM networks. Proceedings IEEE International Symposium on Computers and Communications (Cat. No. PR00250) 1999, 93–99, [http://doi.org/10.1109/ISCC.1999.780775].

[2] Bakhovskyy P. et al.: Stages of the Virtual Technical Functions Concept Networks Development. D. Cagáˇnová et al. (eds.), Advances in Industrial Internet of Things, Engineering and Management. EAI, Springer Innovations in Communication and Computing, 2021, 119–135 [http://doi.org/10.1007/978-3-030-69705-1_7].

[3] Cai Y. et al.: Modulation and Multiple Access for 5G Networks. IEEE Communications Surveys & Tutorials 20(1), 2018, 629–646, [http://doi.org/10.1109/COMST.2017.2766698].

[4] Chen W. et al.: NFC Mobile Transactions and Authentication Based on GSM Network. Second International Workshop on Near Field Communication, 2010, 83–89, [http://doi.org/10.1109/NFC.2010.15].

[5] Deng L. et al.: Mobile network intrusion detection for IoT system based on transfer learning algorithm. Cluster Comput 22, 2019, 9889–9904 [http://doi.org/10.1007/s10586-018-1847-2].

[6] Gupta A., Jha R. K.: A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access 3, 2015, 1206–1232, [http://doi.org/10.1109/ACCESS.2015.2461602].

[7] Hongfeng Z. et al.: A Novel and Provable Authenticated Key Agreement Protocol with Privacy Protection Based on Chaotic Maps towards Mobile Network. International Journal of Network Security 18(1), 2016, 116–123.

[8] Melnyk V. et al.: Design and implementation of interdomain communication mechanism for high performance data processing. Eastern-European Journal of Enterprise Technologies 1(9), 2016, 10–15, [http://doi.org/10.15587/1729-4061.2016.60629].

[9] Melnyk V. et al.: Implementation of the simplified communication mechanism in the cloud of high performance computations. Eastern-European Journal of Enterprise Technologies 2(86), 2017, 24–32, [http://doi.org/10.15587/1729-4061.2017.98896].

[10] Pekh P. et al.: Generators of Some Kinds Random Erlang Numbers and Estimation of Their Complexity. 10th International Conference on Advanced Computer Information Technologies, ACIT 2020, 306–310, [http://doi.org/10.1109/ACIT49673.2020.9208831].

[11] Pham Q. et al.: A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art. IEEE Access 8, 2020, 116974–117017, [http://doi.org/10.1109/ACCESS.2020.3001277].

[12] Ren Y. et al.: Dynamic Auto Scaling Algorithm (DASA) for 5G Mobile Networks. 2016 IEEE Global Communications Conference (GLOBECOM), 2016, 1–6, [http://doi.org/10.1109/GLOCOM.2016.7841759].

[13] Růzičková M. et al.: The estimation of the dynamics of indirect control switching systems. Tatra Mountains Mathematical Publications 48(1), 2011, 197–213, [http://doi.org/10.2478/v10127-011-0018-0].

[14] Saad W. et al.: A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Network 34(3), 2020, 134–142, [http://doi.org/10.1109/MNET.001.1900287].

[15] Satsyk, V. et al.: Reduction of Server Load by Means of CMS Drupal. 10th International Conference on Advanced Computer Information Technologies ACIT 2020, 523–528, [http://doi.org/10.1109/ACIT49673.2020.9208874].

[16] Shafi M. et al.: 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. IEEE Journal on Selected Areas in Communications 35(6), 2017, 1201–1221, [http://doi.org/10.1109/JSAC.2017.2692307].

[17] Tkachuk A. et al.: Basic Stations Work Optimization in Cellular Communication Network. D. Cagánová et al. (eds.), Advances in Industrial Internet of Things, Engineering and Management. EAI, Springer Innovations in Communication and Computing 2021, 1–19 [http://doi.org/10.1007/978-3-030-69705-1_1].

[18] Toroshanko Y. et al.: Control of Traffic Streams with the Multi-Rate Token Bucket. International Conference on Advanced Information and Communications Technologies – AICT 2019, 352–355, [http://doi.org/10.1109/AIACT.2019.8847860].

[19] Wu L., Lin Y.: Authentication Vector Management for UMTS. IEEE Transactions on Wireless Communications 6(11), 2007, 4101–4107, [http://doi.org/10.1109/TWC.2007.060245].

[20] Xu L. et al.: A Comprehensive Operation and Revenue Analysis Algorithm for LTE/5G Wireless System Based on Telecom Operator Data. IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2019, 1521–1524, [http://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00274].

[21] Zhang Y., Fujise M.: An improvement for authentication protocol in third-generation wireless networks. IEEE Transactions on Wireless Communications 5(9), 2006, 2348–2352, [http://doi.org/10.1109/TWC.2006.1687756].

Ph.D. Serhii Moroz
e-mail: s.moroz@lntu.edu.ua

Author of more than 100 scientific papers, 7 patents for utility models. Research interests: Methodological bases of construction of sensors of physical quantities and measuring modules, Research of info-communication systems in the context of the development of the concept of the Internet of Things.

http://orcid.org/0000-0003-4677-5170

Ph.D. Anatolii Tkachuk
e-mail: a.tkachuk@lntu.edu.ua

Vice-dean for R&D Faculty of Computer and Information Technologies, Lutsk National Technical University.
Member of European Alliance for Innovation (EAI), International Association for Technological Development & Innovations (IATDI).
http://www.researchgate.net/profile/Anatolii-Tkachuk

http://orcid.org/0000-0001-9085-7777

Ph.D. Mykola Khvyshchun
e-mail: m.khvyshchun@lntu.edu.ua

Author of more than 100 scientific papers, 2 patents for utility models. Research interests: Investigation of semiconductor materials, Research of radiation-protective epoxy composite coating for n-Ge and n-Si single crystals.

http://orcid.org/0000-0002-3918-4527

Ph.D. Stanislav Prystupa
e-mail: s.prystupa@lntu.edu.ua

Author of more than 60 scientific papers, 5 patents for utility models. Research interests: design of microelectronic intelligent sensors of physical quantities.

http://orcid.org/0000-0003-3705-1541

Ph.D. Mykola Yevsiuk
e-mail: m.yevsiuk@lutsk-ntu.com.ua

Research interests: telecommunication networks, radio engineering devices, power supply systems of radio engineering devices and systems. Author and co-author of about 40 scientific articles, two textbooks, two monographs

http://orcid.org/0000-0002-3768-8959