UDC 621.391
DOI https://doi.org/10.17721/ISTS.2021.1.25-34

R. S. Odarchenko, orcid.org/0000-0002-7130-1375, **odarchenko@ukr.net**
National Aviation University, Kyiv, Ukraine,
S. Y. Dakov, orcid.org/0000-0001-9413-3709, **dacov@ukr.net**
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
L. V. Dakova, orcid.org/0000-0001-6104-8217, **dacova@ukr.net**
State University of Telecommunications, Kyiv, Ukraine

RESEARCH OF CYBER SECURITY MECHANISMS IN MODERN 5G CELLULAR NETWORKS

The main feature of the 5G network is Network slicing. This concept enables network resource efficiency, deployment flexibility, and support for rapid growth in over the top (OTT) applications and services. Network Slicing involves splitting the 5G physical architecture into multiple virtual networks or layers. Each network layer (slice) includes control layer functions, user traffic level functions, and a radio access network.

Slice isolation is an important requirement that allows the basic concept of Network slicing to be applied to the simultaneous coexistence of multiple fragments in a single infrastructure. This property is achieved by the fact that the performance of each slice should not affect the performance of the other. The architecture of network fragments expands in two main aspects: slice protection (cyber attacks or malfunctions affect only the target slice and have a limited impact on the life cycle of other existing ones) and slice privacy (private information about each slice, such as user statistics) does not exchange between other slices).

In 5G, the interaction of the user's equipment with the data networks is established using PDU sessions. Multiple PDU sessions can be active at the same time to connect to different networks. In this case, different sessions can be created using different network functions following the concept of Network Slicing.

The concept of "network architecture", which is developed on hardware solutions, is losing its relevance. It will be more appropriate to call 5G a system, or a platform because it is implemented using software solutions.

5G functions are implemented in VNF virtual software functions running in the network virtualization infrastructure, which, in turn, is implemented in the physical infrastructure of data centers, based on standard commercial COTS equipment, which includes only three types of standard devices - server, switch and a storage system.

For the correct operation of a network, it is necessary to provide constant monitoring of parameters which are described above. Monitoring is a specially organized, periodic observation of the state of objects, phenomena, processes for their assessment, control, or forecasting. The monitoring system collects and processes information that can be used to improve the work process, as well as to inform about the presence of deviations.

There is a lot of network monitoring software available today, but given that 5G is implemented on virtual elements, it is advisable to use the System Center Operations Manager component to monitor network settings and performance and to resolve deviations on time.

The Operations Manager reports which objects are out of order sends alerts when problems are detected and provides information to help determine the cause of the problem and possible solutions.

So, for the 5G network, it is extremely important to constantly monitor its parameters for the timely elimination of deviations, as it can impair the performance and interaction of smart devices, as well as the quality of communication and services provided. System Center Operations Manager provides many opportunities for this.

The purpose and objectives of the work. The work aims to analyze the main mechanisms of cybersecurity in 5G cellular networks.

Keywords: *5G; network; monitoring; virtual software.*

1. INTRODUCTION

The modern world is impossible to imagine without the Internet, smartphones, and other gadgets that have become an integral part of our lives. With the development of information technology, the needs of users are growing rapidly, which cannot always meet the 4th generation mobile networks. That is why it is necessary to develop and implement a 5G network.

5G will allow the active development of IoT technologies, which will ensure the emergence of smart cities, smart vehicles, and other IoT technologies. Base stations will be able to communicate with objects that move at high speeds, up to 500 km / h.

5G is a qualitative development of technologies, not just an increase in network bandwidth. Enhanced security, increased connection stability, increased number of devices connected to the network at the same time, the ability to work with IoT in real-time - these are the opportunities that can provide 5G.

In general, the 5G network absorbs not only mobile but also fixed communication services, high-speed low-speed Internet access, and specialized corporate networks for industries.

The 5G network platform provides operators with significant benefits, primarily in terms of functionality, increased network bandwidth, and increased user satisfaction.

5G network security features

The security concept of mobile communication networks of the fifth generation is based on the reuse of the corresponding technologies adopted in the 4G-LTE standard [26]. Figure 1 shows the general architecture for building the core of a 5G network. Functional objects that implement security mechanisms are highlighted in dark color [27]:

Security Anchor Function (SEAF) - security anchor function.

Authentication Server Function (AUSF) is an authentication server function.

Authentication Credential Repository and Processing Function (ARPF) is a function of storing and processing authentication credentials.

Security Context Management Function (SCMF) is a security context management function.

Security Policy Control Function (SPCF) is a security policy management function.

Subscription Identifier De-concealing Function (SIDF) - a function to retrieve user ID Fig. 1.

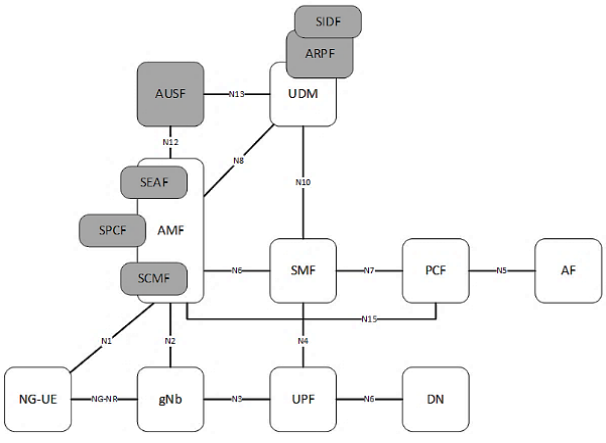

Fig. 1. 5G backbone architecture

During the first phase, the SEAF, SCMF, and SPCF are expected to be combined with the Access and Mobility Management (AMF) module of the ARPF and SIDF with the Unified Database (UDM).

Safety anchor function (SEAF). In cooperation with the AUSF, it provides authentication of the user of the terminal (UE) upon registration in the network (attach) for any access technology.

Authentication function (AUSF.). Acts as an authentication server, terminating requests from SEAF and translating them into ARPF. Can be combined with the Authentication Credentials Repository (ARPF).

Authentication Credential Repository (ARPF). Provides storage of personal secret keys (KI) and parameters of cryptographic algorithms, as well as generation of authentication vectors following 5G-AKA or EAP-AKA algorithms. It is in a home network protected from external physical influences of the data center and, as a rule, is integrated with a unified database (UDM).

Security Context Management Function (SCMF). Provides 5G security context lifecycle management.

Security Policy Management Module (SPCF). Ensures the negotiation and enforcement of security policies for specific user terminals (UE). This considers network capabilities, UE capabilities, and specific service requirements. Application of security policies includes a selection of AUSF, selection of authentication algorithm, selection of data encryption and integrity control algorithms, determination of the length and life cycle of keys.

User ID Delete Function (SIDF). Provides extraction of the permanent subscriber subscription identifier (5G SUPI) from the hidden identifier (SUCI) obtained as part of the "Auth Info Req" authentication procedure request.

Overall, the 5G network security concept includes:

User authentication from the network.

User side authentication of the network.

Negotiation of cryptographic keys between the network and the user terminal.

RRC signaling traffic encryption and integrity control (between UE and gNb).

Encryption and integrity control of signaling traffic at the NAS layer (between UE and AMF).

Encryption and integrity control of user traffic (between UE and gNb).

User ID protection.

Protection of interfaces between different network elements following the concept of a network security domain described in the recommendation 3GPP TS 33.310, incl. protection of interfaces N2, N3, and Xn.

Isolating the different layers of the Network slicing architecture and defining its security levels for each layer.

Protection of signaling and user traffic between 4G-LTE eNb and 5G gNb in the "Option 3" 4G to 5G migration scenario, including cryptographic key negotiation, encryption, and integrity control.

User authentication and traffic protection at the end service level (IMS, V2X – Vehicle to Everything, IoT).

Authentication and Key Agreement Procedure

The purpose of the Authentication and Key Agreement (AKA) procedure is to perform mutual authentication between the user terminal and the network, as well as generate the security function key KSEAF (see Fig. 2). Once generated, the KSEAF key can be used to form several security contexts, incl. for 3GPP and non-3GPP access.

Release 15 3GPP defines two mandatory methods for authentication and key agreement - EPS-AKA "and 5G-AKA, which will be discussed below.

Within both methods, a derivation function (KDF) is called, which, based on the control character string, converts the cryptographic key. The control character string may include the name of the serving subscriber of the guest network (Serving Network Name - SN-name). In particular, SN-name is used when calculating:

- security function key KSEAF;
- Authentication revocation (RES * XRES *)
- intermediate keys CK "and IK".

The SN-name is constructed by combining a service code (service code = "5G") and a guest network identifier, user authentication (network identifier or SN Id). SN Id is calculated based on Mobile Country Code (MCC) and Mobile Network Code (MNC) – see Fig. 2.

	7	6	5	4	3	2	1	0
1	MCC digit 2				MCC digit 1			
2	MNC digit 3				MCC digit 3			
3	MNC digit 2				MNC digit 1			

Fig. 2. Network identifier or SN Id

Using the name of the serving network (SN-name) allows you to unambiguously bind the results of cryptographic algorithms in a specific guest network.

Initiation and selection of authentication method

In accordance with the operator's security policy, SEAF can initiate user authentication of the terminal (UE) in any procedure involving the establishment of a signaling connection with the UE, for example, when registering with the network (attach) or updating the tracking area (tracking area update). To "go on the air", the UE must use either the hidden SUCI code (when first registering with the network) or 5G-GUTI (otherwise).

To authenticate the terminal user, SEAF uses a previously created and not yet used authentication vector, or sends an "Authentication Initiation Request" (5G-AIR) to the AUSF, setting the user ID to SUCI (upon initial registration in the network) or SUPI (upon receipt from the UE valid 5G-GUTI). The authentication request (5G-AIR), in addition to the user ID, must also include the access type (3GPP or non-3GPP), as well as the serving network name (SN-name).

Next, the AUSF verifies the legality of using the serving network name (SN-name) and, upon successful verification, translates the received request to the unified database (UDM) block, where (if necessary) the user identifier retrieval functional module (SIDF) decrypts the hidden user identifier (SUCI), after which the Authentication Credential Repository (ARPF) selects the appropriate authentication algorithm - 5G-AKA, or EAP-AKA. "

EAP-AKA Authentication Method '

The EAP-AKA authentication method is a further development of the EAP-AKA and introduces a new derivation function that binds cryptographic keys to the access network name. The "EAP-AKA" method described in RFC 5448 is triggered by UDM / ARPF when it receives a user authentication request from AUSF (Authentication Information Request - Auth Info-Req message) Fig. 3 shows a diagram including the following steps.

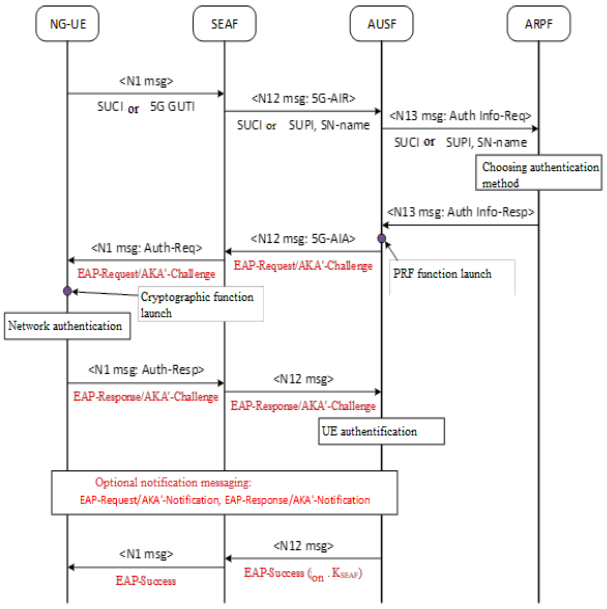

Fig. 3. EPS-AKA Authentication Method

The user credential storage and processing module (UDM / ARPF) generates an authentication vector including RAND, AUTN, XRES, CK, IK. To calculate the authentication vector, five one-way functions f1-f5 are used, implemented based on the MILEAGE block cipher (following 3GPP TS 33.102 – see Fig. 4) with the AMF bit set to "1". When calculating f1-f5, a 128-bit operator-variant algorithm configuration field (OP) is used. OP allows you to make a unique (secret) implementation of the algorithm for each operator. The OP value (or OPC, calculated from OP and KI via the block cipher function) must be stored in the ARPF and on the user's USIM.

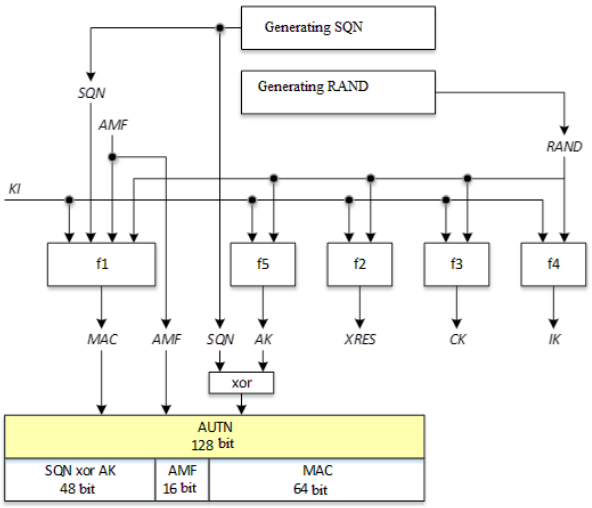

Fig. 4. Authentication vector

2. UDM / ARPF using the derivation function and using the service network name (SN-name) calculates the "bound" value CK ", IK 'and transmits the vector (RAND, AUTN, XRES, CK", IK') of the authentication server (AUSF) from which the request was received.

3. AUSF launches the cryptographic function PRF of the EAP-AKA method "described in RFC5448. The input parameters of the function are the keys CK" and IK ", as well as the name of the serving network (SN-name). The following fields are obtained at the output of the function:

- K_encr – key (128 bit) used to encrypt individual attributes of EAP-AKA messages "(in accordance with the operator's security policy);
- K_aut – key (256 bit) used to calculate the message integrity control codes EAP-AKA "(MAC - Message Authentication Code)
- K_re – key (256 bits) used for re-authentication;
- MSK (Master Session Key) – master key (512 bit)
- EMSK (Extended Master Session Key) – extended master key (512 bits).

4. The AUSF sends an EAP-Request / AKA'-Challenge to the Security Anchor Function (SEAF), which is then transparently broadcast to the terminal user in the NAS message. EAP-Request / AKA'-Challenge contains the following attributes:

- AT_RAND (random number)
- AT_AUTN (authentication token)
- AT_KDF (identifier of the used derivation function, where 1 corresponds to using the default derivation function)
- AT_KDF_INPUT (serving network name – SN-name)
- AT_MAC (Message Authentication Code).

5. User terminal:

- calculates the value of XMAC, RES, CK "and IK
- starts the cryptographic function PRF of the EAP-AKA algorithm "(similar to the function performed by the authentication server)
- checks the correctness of the message integrity control code (AT_MAC attribute)
- checks if the AMF bit of the AT_AUTN attribute is set to "1";
- performs network authentication by comparing the calculated and received AUTN values;
- sends an EAP-Response / AKA'-Challenge with the attributes AT_RES and AT_MAC to the security anchor function (SEAF), which is then transparently broadcast by the authentication server (AUSF).

6. AUSF validates the message integrity check code (AT_MAC attribute) and authenticates the terminal user by comparing the RES and XRES values received from the UE and ARPF / UDM, respectively.

7. If successful, the AUSF sends an EAP-Success Feedback to the UE via the Security Anchor Function (SEAF). If the operator's security policy provides for the transmission of an encrypted EAP-Success – "protected successful result indications", notification messages are first exchanged. Also (if necessary), through the SIDF function call, the hidden identifier (SUCI) decryption and 5G SUPI extraction are performed.

8. At the final stage, ARPF / UDM generates an authentication function key KAUSF, which is used as the first 256 bits of the extended master key (EMSK). Further, based on KAUSF, encryption and integrity control keys are calculated according to the hierarchy of cryptographic keys shown in Fig. 7.

2. 5G-AKA AUTHENTICATION METHOD

The 5G-AKA authentication method is a further development of the EPS-AKA described in 3GPP TS 33.401 and is applied on 4G-LTE networks. The 5G-AKA method is triggered by UDM / ARPF when it

receives a user authentication request from AUSF (Authentication Information Request message – Auth Info-Req). In fig. 6 is a diagram that includes such steps.

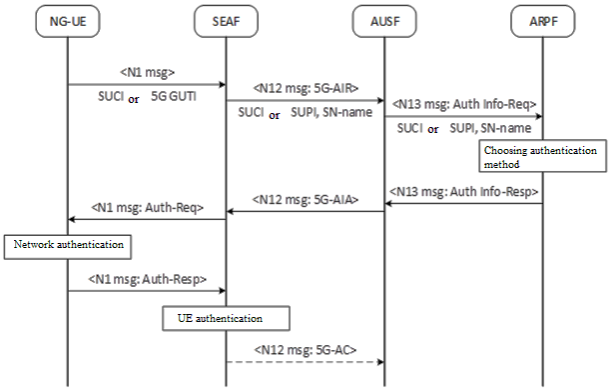

Fig. 5. 5G-AKA Authentication Method

1. By analogy with the EAP-AKA algorithm "the user credentials repository and processing module (UDM / ARPF), based on the MILENAGE block cipher, generates an authentication vector that includes RAND, AUTN, XRES, CK, IK (the AMF bit must be set to unit).

2. UDM / ARPF using the derivation function and using the serving network name (SN-name) calculates:

- the value of the expected response XRES * is bound
- the key value of the authentication function KAUSF,
- generates the vector "5G not the AV" (Home Environment Authentication Vector), including RAND, AUTN, XRES * KAUSF and sends it to the authentication server (AUSF).

3. AUSF calculates:

- the HXRES * value, which is a hash truncated to 128 bits from the concatenation of the expected XRES * authentication response and a random number RAND: HXRES * num lower 128 bits from SHA-256 [RAND || XRES *];
- the value of the key of the security function KSEAF.

The AUSF then generates 5G AV (5G Authentication Vector) including RAND, AUTN, HXRES * KSEAF and sends it to the Security Anchor Function (SEAF) using a 5G-AIA (Authentication Initiation Answer) message. If the authentication request (5G-AIR) contained a hidden user code (SUCI), the AUSF receives the 5G SUPI through the SIDF function call and adds it to the 5G-AIA.

4. SEAF monitors the received vector lifetime timer and sends an Auth-Req message to the NAS terminal user with the RAND and AUTN parameters enabled.

5. User terminal:

- calculates the value of RES, AUTN, CK, IK by calling the corresponding functions of the USIM module;
- performs network authentication by comparing the calculated and received AUTN values;
- calculates the values of the keys KAUSF and KSEAF;
- computes the bound values of the RES * authentication response;
- sends an Auth-Resp message containing RES * to the safety anchor function (SEAF).

6. SEAF calculates the hash HRES * (similar to AUSF) and authenticates the terminal user by comparing HRES * and HXRES *.

7. Upon successful authentication, SEAF sends a 5G-AC (Authentication Confirmation) message to the AUSF, including the RES * response values received from the UE. This step is optional and may not be used when registering a user on a home network.

8. AUSF checks the lifetime timer of the authentication vector, compares the value of the calculated (XRES *) and received (RES *) feedback, and then completes the authentication procedure.

3GPP recommends that only one vector be generated and used per authentication procedure. This will allow a confirmation message to complete each authentication procedure.

Hierarchy of cryptographic keys

The following are the keys, variables, and cryptographic functions that are used in 5G security procedures:

1. The user's secret key KI – 128 (or 256) bits. Stored in read-protected ARPF and USIM memory of the module.

2. Random number RAND (RANDom challenge) – 128 bits;

3. Rejection of authentication RES (authentication RESponse) – 128 bits. Generated by a user terminal (UE) and used in the UE's network authentication procedure.

4. The expected revocation of XRES authentication (eXpected RESponse) is 128 bits. An ARPF is generated and used in a terminal (UE) user authentication procedure by the network.

5. Pegged Authentication Revocation (pending authentication revocation) (X) RES * – 128 bits. Represents (X) RES modified by the derivation function.

6. Shortened hash of the bound (expected bound) authentication response and the random number H (X) RES * – 128 bits.

7. Sequence number SQN (SeQuence Numbers) – 48 bits.

8. Anonymous key AK (Anonymity Key) – 48 bits. Used to protect the sequence number (SQN).

9. AMF (Authentication Management Field) – 16 bits. Specifies the type of authentication vector generated by ARPF (UMTS or EPS / 5G).

10. Message Authentication Code (MAC) – 64 bits. An ARPF is generated and used in the UE's network authentication procedure.

11. The expected eXpected Message Authentication Code (XMAC) is 64 bits. Generated by a user terminal (UE) and used in the UE's network authentication procedure.

12. Authentication token AUTN (authentication token) – 128 bits. Includes an Authentication Message Code (expected Authentication Message Code) – (X) MAC and an Authentication Control Field (AMF).

13. Keys CK (Cipher Key) and IK (Key Integrity) – 128 bits each. They are located at the top of the tree of the hierarchy of cryptographic keys and underlie the calculation of encryption keys and control the integrity of signaling and user traffic.

14. Is the second ancestor of the KAUSF authentication function key.

15. Key for authentication function KAUSF.

16. Security function key KSEAF.

17. KAMF access and mobility management function key. When performing a handover with changing the access and mobility control module to the target Fig. 6.

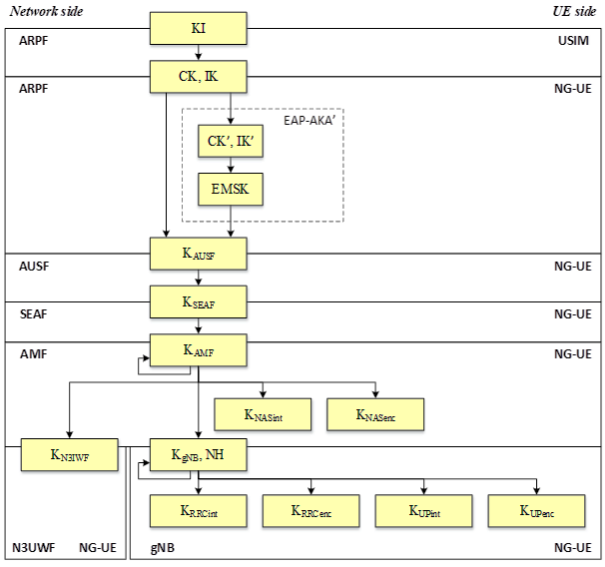

Fig. 6. Key hierarchy

Security contexts

One of the fundamental concepts of traffic protection in 5G networks is the concept of a security context (5G security context) – a block of information that includes keys, parameters, variables that ensure the functioning of encryption and data integrity control mechanisms. Symmetric copies of the "5G security context" are stored in the user terminal and on the network elements. 3GPP defines three types of "5G security context":

- "full native" – a context created within the 5G authentication and key agreement (EAP-AKA "or 5G-AKA) for which NAS traffic security mechanisms (NAS-SMC) were successfully activated
- "partial native" – a security context created within the 5G authentication and key agreement (EAP-AKA "or 5G-AKA) for which the NAS traffic security mechanisms (NAS-SMC) have not yet been activated.
- "mapped" – a security context created when a user transitions from a network of one communication standard to a network of another, by converting UMTS (or EPS) keys into a 5G key.

The security context can be in one of two possible states – "current" – the current (last activated security context) and "non-current". The "current" state can be a context of the "full native" or "mapped" type, the "non-current" state – "fully native" or "partial native". At the same time, in the "non-current" state, the context has no 5G AS data.

The 5G security context includes the following sections:

1) 5G NAS security context – parameters and variables to ensure the security of NAS alarm, including:

- the key of the KAMF access and mobility management function,
- a list of NAS security algorithms supported by the user terminal (UE),
- identifiers of selected algorithms for NAS encryption and integrity control,
- the value of NAS COUNT counters for downstream and upstream traffic,
- keys for NAS encryption and KNASint and KNASenc integrity control.

2) 5G AS security context – parameters and variables to ensure the security of RRC signaling and user traffic, including:

- base station key KgNB,
- a list of security AS algorithms supported by the user terminal (UE),
- identifiers of selected algorithms for RRC / UP encryption and integrity control,
- the value of the RRC / COUNT UP counters for downstream and upstream traffic,
- key for RRC / UP encryption and integrity control KRRCint, KRRCenc, KUPint, KUPenc,
- NH (Next Hop parameter) and NCC (Next Hop Chaining Counter parameter) parameters are used for key derivation.

3) 5G AS security context for non-3GPP access - parameters and variables to ensure user security and signaling traffic for non-3GPP access (Wi-Fi, etc.).

The mechanisms for using this context are not defined at the time of this writing.

When the user turns off the terminal, the AMF and UE store copies of the current NAS security context (current 5G NAS security context) and all unused authentication vectors, which allows the next time the terminal is turned on, on the one hand, to minimize its registration time, on the other hand, to ensure the required level of security. On the UE side, a copy of the current security context can be stored either by the USIM (if the module contains the appropriate files for storing the network connection parameters) or in the non-volatile memory of the UE.

Securing NAS Traffic

Securing NAS traffic includes encryption parameters and integrity control of NAS signaling messages transmitted between the user terminal (UE) and the access and mobility control module (AMF) via the N1 interface (see Fig. 1).

Security mechanisms for NAS traffic are activated as part of the NAS Security Mode Command - NAS-SMC procedure (see Fig. 10). The choice of encryption and integrity control algorithms is performed by AMF based on the priorities set by the operator, as well as following the priorities received from the UE security capabilities. If the user terminal (UE) does not have an up-to-date security context, then the primary NAS message should be sent in an open (unencrypted form and contain only the user ID and "security capabilities". In this case, the integrity of the NAS messages signaling is provided starting with "NAS Security Mode Command encryption – with" NAS Security Mode Complete. "If the UE has an up-to-date security context, then the attributes of the primary NAS message MUST be encrypted except for the already mentioned user ID and" security capabilities ".

Using a man-in-the-middle attack, an attacker can change the value of the "security capabilities" field of the primary unsecured NAS message and thereby reduce the security level of the NAS conversation as a whole. To detect this, the AMF sends a copy of "security capabilities" to the UE and has integrity protection to the "NAS Security Mode Command", allowing the UE to detect an attack. For the same purpose, the AMF, by setting the Request Initial Message Flag, may invite the UE to send a copy of the primary NAS message as part of the NAS Security Mode Complete secure revocation.

Securing AS Traffic

Securing AS traffic includes parameter encryption and integrity control of RRC signaling messages, as well as user data packets transmitted between the UE and the base station (gNb) via the NG-NR interface (Fig. 7).

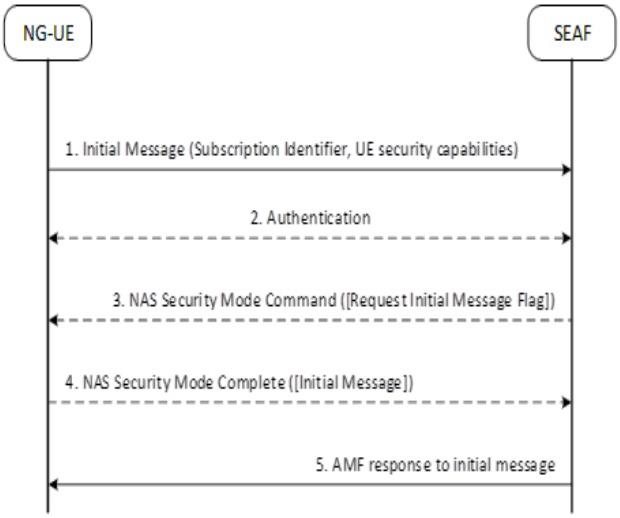

Fig. 7. NAS Security Mode Command Procedure

The activation of security mechanisms for AS traffic is carried out as part of the AS Security Mode Command (AS-CMS) procedure, which includes the exchange of AS Security Mode Command and AS Security Mode Complete messages (the integrity of these messages must be protected). The choice of encryption and integrity control algorithms is performed by gNb based on the priorities set by the operator, as well as following the security capabilities received from the UE.

Integrity control is provided starting from the RRC message "AS Security Mode Command", encryption – from the "AS Security Mode Complete".

When the handover is performed, the source base station transmits encryption and integrity control algorithms and capabilities for the terminal user in the handover request message to the target base station. Based on the received data, the target gNb, on the one hand, can read the "RRCReestablishmentComplete" message from the UE, and on the other hand, can select and broadcast new algorithms to the UE.

As part of the handover procedure, a new KgNB * key is generated at the target base station. The key is generated either on the basis of the pre-key KgNB (horizontal derivation) or on the basis of NH (vertical derivation). This mechanism is called "AS key refresh" in 3GPP terminology.

3. USER IDs

Many identifiers have been defined for 5G users, detailed in 3GPP TS 23.003. Below is a brief description of them:

1. International permanent subscriber subscription identifier – 5G SUPI (Subscription Permanent Identifier). Assigned to each subscriber of the 5G network and stored in the unified UDM and USIM database of

user modules. The SUPI identifier can be an international mobile subscriber identifier - IMSI (International Mobile Subscriber Identity), or a network access identifier – NAI (Network Access Identifier), the format of which is defined by RFC 4282.

2. Hidden user identifier – SUCI (Subscription Concealed Identifier). It is an encrypted copy of the international permanent subscriber subscription identifier (5G SUPI) and avoids the transmission of 5G SUPI over the network in the clear, even when the terminal user is initially registered in the network (Initial attach).

SUPI is protected using an Elliptic Curve Integrated Encryption Scheme (ECIES). The public key used for SUPI encryption must be stored in the secure memory of the USIM card; the private key is in the User ID Withdrawal Functional (SIDF). In this case, the SUPI part containing the mobile country code (MCC) and mobile network code (MNC) and is used for routing signaling traffic is not encrypted. 3GPP allows SUPI encryption in the user terminal (default option) and USIM modules. The operator's network and user terminal must also support the so-called null-scheme, in which the public user ID is not protected.

The 5G Globally Unique Temporary Identifier (5G Globally Unique Temporary Identifier) is assigned by the Access and Mobility Management (AMF) module regardless of the type of access network (3GPP, non-3GPP). When "going on the air", the user terminal must use exactly 5G-GUTI (except for initial registration in the network – initial attach, as well as in other cases when there is no valid 5G-GUTI) The 5G-GUTI format is shown in Fig. 8.

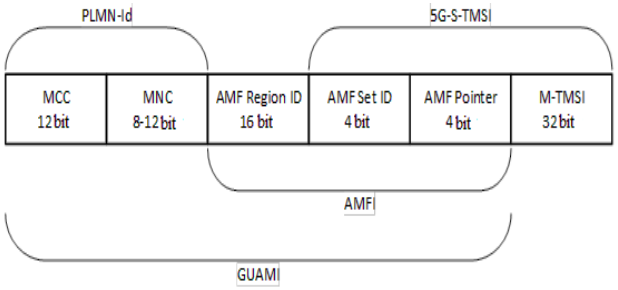

Fig. 8. 5G-GUTI structure

here:

- GUAMI (Globally Unique AMF Identifier) - global (international) identifier of the AMF access and mobility control module;
- MCC - mobile country code;
- MNC - mobile network code;
- AMF Region ID – identifier of the region served by the AMF module;
- AMF Set ID – unique identifier of the group of AMF modules within the region;
- AMF Pointer – unique identifier of the AMF module within the AMF Set ID group;
- AMFI – unique (within the network) AMF identifier;
- 5G-TMSI (5G Temporary Mobile Subscription Identifier) – a temporary identifier of a 5G mobile subscriber (unique within AMF)
- 5G-S-TMSI – unique (within the region) temporary identifier of a 5G mobile subscriber.

4. CONCLUSION

Explained to the public understanding of the "monitoring of the fancy". It is centrally organized, systematically changing over the camp of objects, appearances, processes with the mark of evaluating, monitoring or forecasting. Monitoring is a systematic collection and processing of information, as it can be used for polishing the process of taking decisions, as well as for informing loudness and or as a design tool for a star star link tool for measuring. In the Danish hour, the monitoring of the measurement will be added to the number of additional subsystems, for example:

- intrusion detection system – follow the emergence of threats (Intrusion detection system). The whole system, which displays fancy traffic on the subject of suspicion of activity and type of improvement, if such activity is detected. Other quality of service is provided by the administrator or selected centrally for additional systems and security and management of pods. The SIEM system integrates vyhodi with decilkoh dzherel and vikorista methods of filtering trivia, allowing you to identify the malicious activity of pompous trivia.

The intrusion memorization system is an excellent degree to enable the use of the Intrusion Prevention System. Bagato IPS can also react to the threat of a threat, if you do not allow it to be damaged. Smell the vicious methods of reacting, teach the IPS the attack itself, reduce the middle of the bezpeka or change the attack. The system for monitoring the productivity of the net (Network Performance Monitoring, NPM) is a rewiring of the attachment / channel. With the monitoring of the hedgehog, the vison is watching over the hedge in the jokes of the problems that are caused in the robots of the server systems, their attachments or the hedgehogs.

At the connection with the active, growing nature of the development of information technologies, the growth of the foldability of the scale of the systems and the net, in its turn, a special acceleration of the monitoring and forecasting of For such universities, it is not necessary to throw viruses of increased and

security, as well as toxicity.

Boolean view System Center Operations Manager (SCOM). The product of the building consoles information about the function of the new IT-infrastructure components, which is secured in the second consoles.

Vikoristannya Operational manager will lie behind a great number of computers, annexes, services and supplements. Console for dose management to reconsider the rate, productivity, availability of all advanced facilities in the middle, and

Agents view the dzherela on computers pick up the views according to the configuration that controls the server. When I change the status of the object or the visibility of other minds, the agent can change. Tse with the permission of the operator to know, if vimagим їхної respect. I will transfer the data about the status of the post-hosted object to the control server, the agent will send the picture of the pre-delivery status of the annex and all the data

Bulo is proponent of the option of the system and monitoring of parameters in the 5G grid. Merezhi of the fifth generation are implemented on virtual elements, also on the secondary SCOM component for controlling the parameters and correctness of the hedge and the time-consuming operation.

5G functions are implemented in virtual programmable VNF functions, which are implemented in the NFV infrastructure. In its own place, NFV is implemented in the physical infrastructure of the data center on the basis of the standard commercial property of COTS.

The 5G skin element is used for monitoring agents. A data modifier generates various data with preceding variable icons that trigger the actions that result from the action. Server for management of configuration and extended agencies on state-of-the-art computers. All agents send calls to the management server in the group. The cei server is used as the main control server of the agent.

A circuit has been installed in the maybutny can of the vikoristan for the control of parameters in the 5G mesh.cellular networks.

REFERENCES

[1] Tomas Hegr, Leos Bohac, Impact of Nodal Centrality Measures to Robustness in, Software-Defined Networking // Advances in Electrical and Electronic Engineering. 2014;12(4):252-259 DOI 10.15598/aeee.v12i4.1208

[2] R. S. Odarchenko, S. Yu. Dakov, V. V. Polischuk, A. M. Tyrsenko, Modeling of SDN Overlay Networks and Their Main Characteristics Research // Knowledge-based technologies № 3 (31), 2016 с. 284

[3] Odarchenko, R., Abakumova, A., Polihenko, O., Gnatyuk, S., Traffic offload improved method for 4G/5G mobile network operator // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 – Proceedings 2018-April, pp. 1051-1054

[4] Hung LeHong, Jackie Fenn. Key Trends to Watch in Gartner. Emerging Technologies Hype Cycle / Hung LeHong, Jackie Fenn, 2012.

[5] Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

[6] Intrusion Prevention System (IPS) URL: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/.

[7] Reporting Server URL: https://scom.fandom.com/wiki/Reporting_Server.

[8] Data Warehouse URL: https://scom.fandom.com/wiki/Data_WarehouseACS Database URL https://scom.fandom.com/wiki/ACS_Database.

[9] Operational Database URL: https://scom.fandom.com/wiki/Operational_Database.

[10] Operations Console URL https://scom.fandom.com/wiki/Operations_Console.

[11] Web Console URL https://scom.fandom.com/wiki/Web_Console.

Стаття надійшла до редколегії 11.05.2021

Дослідження механізмів кібербезпеки стільникової мережі 5G

Основною особливістю мережі 5G є розділення мережі. Ця концепція забезпечує ефективність використання мережних ресурсів, гнучкість розгортання та підтримку швидкого зростання топових (OTT) програм і служб. Зрізування мережі передбачає поділ фізичної архітектури 5G на кілька віртуальних мереж або шарів. Кожен мережний рівень (зріз) включає функції рівня керування, функції рівня трафіка користувача та мережу радіодоступу. Ізоляція фрагментів є важливою вимогою, яка дозволяє застосувати основну концепцію зрізу мережі до одночасного співіснування кількох фрагментів в одній інфраструктурі. Ця властивість досягається тим, що продуктивність кожного зрізу не повинна впливати на продуктивність іншого. Архітектура мережних фрагментів розширюється за такими основними аспектами: захист фрагментів (кібератаки або збої в роботі зачіпають лише цільовий фрагмент і мають обмежений вплив на життєвий цикл інших існуючих) і конфіденційність фрагмента (приватна інформація про кожен фрагмент, наприклад, користувача), статистика (не обмінюється з іншими фрагментами). У 5G взаємодія обладнання користувача з мережами передачі даних встановлюється за допомогою сеансів PDU. Декілька сеансів PDU можуть бути активними одночасно для підключення до різних мереж. У цьому випадку можна створити різні сеанси за допомогою різних мережних функцій відповідно до концепції Network Slicing. Поняття "архітектура мережі", яке розроблено на апаратних рішеннях, втрачає свою актуальність. 5G доцільніше буде називати системою, або платформою, оскільки вона реалізована за допомогою програмних рішень.Функції 5G реалізовані у віртуальних програмних функціях VNF, що працюють в інфраструктурі віртуалізації мережі, яка, у свою чергу, реалізована у фізичній інфраструктурі центрів обробки даних, на основі стандартного комерційного обладнання COTS, яке включає лише три типи стандартних пристроїв – сервер, комутатор і система зберігання.

Для правильної роботи мережі необхідно забезпечити постійний моніторинг параметрів, які описані вище. Моніторинг – це спеціально організоване періодичне спостереження за станом об'єктів, явищ, процесів для їх оцінювання, контролю чи прогнозування. Система моніторингу збирає та обробляє інформацію, яка може бути використана для покращення робочого процесу, а також для інформування про наявність відхилень. Сьогодні існує велика кількість програмного забезпечення для моніторингу мережі, але враховуючи те, що 5G реалізовано на віртуальних елементах, доцільно використовувати компонент System Center Operations Manager для моніторингу налаштувань і продуктивності мережі, а також для вчасного усунення відхилень. Менеджер операцій повідомляє, які об'єкти вийшли з ладу, надсилає сповіщення при виявленні проблем і надає інформацію, яка допоможе визначити причину проблеми та можливі рішення. Отже, для мережі 5G надзвичайно важливо постійно контролювати її параметри для своєчасного усунення відхилень, які можуть погіршити продуктивність і взаємодію розумних пристроїв, а також якість зв'язку та наданих послуг. System Center Operations Manager надає багато можливостей для цього. Мета цієї роботи – аналіз основних механізмів кібербезпеки в стільникових мережах 5G.

***Ключові слова**: 5G; мережа; моніторинг; віртуальне програмне забезпечення.*

Roman Odarchenko,
Doctor of Technical Sciences, Associate Professor. Head of the Department of Telecommunication and Radio Electronic Systems of the National Aviation University.

Роман Одарченко,
доктор технічних наук, доцент, завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.

Serhii Dakov,
Candidate of Technical Sciences, Assistant Department Cybersecurity And Protection Information.
Taras Shevchenko National University of Kyiv.

Сергій Даков,
кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Larisa Dakova,
Candidate of Technical Sciences, Associate Professor of the Department of International Relations of the State University of Telecommunications.

Лариса Дакова,
кандидат технічних наук, доцент кафедри МВТ Державного університету телекомунікацій.