[1.]Petar ČISAR, [2.]Sanja MARAVIĆ ČISAR

SECURITY ASPECTS OF 5G MOBILE NETWORKS

[1.] University of Criminal Investigation and Police Studies, Cara Dušana 196, 11080 Zemun–Belgrade, SERBIA
[2.] Subotica Tech, Deparment of Informatics, Marka Oreškovića 16, 24000 Subotica, SERBIA

Abstract: 5G (or fifth generation) represents the latest generation of mobile network technology, whose implementation is underway in some countries. This mobile system has undeniable advantages over its predecessors. This paper gives an overview of security aspects of 5G networks, based on data derived from available literature. Authentication and key management are fundamental processes to the security of cellular networks. That is why the emphasis in the paper is put on elaborating these security methods and comparing features with the previous 4G system. Authentication components in 5G are different in regard to 4G because of the new service–based architecture. Further, 3GPP and non–3GPP access networks are treated more equally. Also, in case of 5G, the user equipment uses the public key of the home network to encrypt permanent identifier before it is sent to a network. In 4G, this identifier is sent as clear text (unencrypted). Key structure is longer in 5G than in 4G because of the implementation of two additional keys. Despite the evident advantages, consideration must be given to the security challenges brought to 5G networks by new services, architectures and technologies. For example, authentication in 5G is not without deficiencies. Namely, user tracking ability in 5G may still be possible.

Keywords: 5G, network security, architecture, authentication, key management

1. INTRODUCTION

Fifth generation mobile network (5G) is a wireless networking architecture (cellular technology) built on the 802.11ac IEEE wireless networking standard, which aims to significantly increase data communication speeds compared to its predecessor 4G LTE (Long–term Evolution – IEEE 802.11n).[1]

Mobile networks transmit data over the air using 700 MHz spectrum band. Low frequencies transfer data slower, but have a larger range. To achieve the declared speeds used by 5G, it is necessary to use a wide frequency range between 24 GHz and 86 GHz – belongs to the area of millimeter waves (6 – 100 GHz). 5G use spectrum in the existing LTE frequency range (600 MHz to 6 GHz) and also in millimeter wave bands (24 – 86 GHz). The problem is that the signals at these high frequencies are extremely sensitive, so even the smallest obstacle causes serious problems in transmission.

The 5G network is in a phase of gradual implementation. The fifth generation of mobile internet has 10 to 100 times higher download (theoretical) speeds than the current 4G network (4G – 100 Mbps, 5G – 10 Gbps). The downside of 5G is that the upload speeds are about the same as on 4G. While the average download speed is about 200 Mbps, the average upload speed is about 100 Mbps.

— Mobile systems overview

As different generations of mobile telecommunications developed, each of them brought its own improvements.

» 1st generation (1G): These technologies were analog and used the first mobile phones. Although progressive at the time, they offered extremely low degree of bandwidth efficiency and security. The maximum speed range (data rate) was 2.4 kbps.

» 2nd generation (2G): These devices were based on digital technology and offered a much better bandwidth efficiency, higher security and new features such as text messaging and communication with low data transmission rates. Maximum flow rate was about 40 kbps.

» 3rd generation (3G): The goal of this technology was to enable faster data transmission. The previous technology has been upgraded to provide data rates of up to 384 kbps.

» 4th generation (4G): This is a fully IP–enabled technology capable of delivering data rates of up to 100 Mbps (theoretical).

— Benefits of 5G

Each new generation of mobile network has made great advances for end users. The 3G network made it possible to send photos and, although with restrictions, to stream calls and videos. 4G has made these capabilities faster, reliable and easy. The 5G network operates seamlessly wherever the user is without the need for a good Wi–Fi signal. Virtual reality (VR) and augmented reality (AR) and artificial intelligence (AI) moved boundaries forward, while also allowing users to stream high quality video (4K/8K) and engage in real–time multiplayer gaming. New mobile technology has also advanced the self–driving car industry.

[1] [1] https://www.techopedia.com

— 5G specifications

Although standardization organizations have not completed the definition of parameters required to meet 5G performance, other organizations have formulated their own goals, which could ultimately affect the final version of specifications.

Typical parameters and proposed wireless performances for a 5G standard include:

Parameter	Proposed performances
Network capacity	10,000 times the current network
Peak data rate	10 Gbps
Cell edge data rate	100 Mbps
Latency	< 1 ms

Fifth generation mobile technology enables a significant increase in quality over previous systems in order to provide mobile operators with an adequate business impulse to invest in new systems. The capabilities that come with 5G technology are a far better level of connectivity and coverage. In order for 5G technology to be able to achieve this, new connectivity methods were introduced since the major disadvantages of previous generations were lack of coverage, call interruption and poor cell edge performance.

Standardization of 5G architecture does not include a way how functions are implemented and realized. The main aim of the specifications is to provide interoperability between the functions required for realization of network connectivity. Because of that, there is little detail of virtualization and cloud utilization in the specifications. These details will be specified at the implementation and deployment phases.

— Basic concepts of 5G technology

Research organizations consider several key areas and concepts in 5G domain:[2]

- Millimeter wave technologies: The use of much higher frequencies requires a wider frequency spectrum and also provides much wider channel bandwidth 1 – 2 GHz. However, this poses new aims for headphone development, where maximum frequencies are about 2 GHz and currently bandwidths 10 – 20 MHz. For 5G, frequencies above 50 GHz are considered, which presents a challenge to the design of circuits, technologies, and also how the system is used, since the signals of these frequencies do not travel as far and the obstacles almost completely absorb them.
- Waveforms: There are many possibilities in this area, from the use of new modulation modes such as GFDM (Generalized Frequency Division Multiplexing), FBMC (Filter Bank Multi–Carrier), UFMC (Universal Filtered Multi–Carrier) and other multi–schema access. A higher signal processing level means that multicarrier systems do not have to be orthogonal such as OFDM (Orthogonal Frequency Division Multiplexing). This allows better flexibility.
- Massive MIMO (Multiple Input Multiple Output): Although MIMO is used in many applications (from LTE to Wi–Fi), the number of antennas is quite limited. Microwave frequencies create opportunity of using large number of antennas on the same equipment due to the size of the antennas and spacing in terms of wavelength. 4G base stations might typically have 12 antennas, while 5G base stations might support 100 antennas.
- Network density (using thousands of low power small base stations – femtocells): Reducing cell sizes enables more efficient use of the available bandwidth. Techniques are needed to ensure that small cells in large networks can function satisfactorily.
- Beam forming is employed to determine the optimum route to each connected user, which helps to reduce interference and increases the chances of easily blocked signals reaching their planned recipient.[3]
- Full duplex signal transmission: Signals travel on different frequencies in both directions – 1 GHz and 800 MHz with use of high speed switches.

— Advanced 5G concepts

There are new concepts being researched and developed for the fifth generation mobile system. Some of them are:

- Ubiquitous networks: In this technology, a user can be simultaneously connected to several wireless access technologies and move between them without interruption.
- Cooperative forwarding: This is a technique that is being considered to ensure high data rates across a wider area of a cell. Currently, data rates are falling toward the edge of the cell, where the level of interference is higher and the signal level is lower.
- Cognitive radio (CR) technology: If CR technology were used for 5G mobile systems, then the user equipment could search the radio spectrum in which it was located and select the optimal access network, modulation scheme and other self–configuring parameters to receive the best connection and optimal performance.
- Wireless and dynamic ad–hoc networking: With many different access schemes, it will be possible to connect with others nearby and provide ad–hoc wireless networks for much faster data flow.

[2] https://www.radio-electronics.co.uk/articles/connectivity/5g-mobile-wireless-cellular/technology-basics.php

[3] https://www.digitaltrends.com/mobile/5g-vs-lte/

- Smart antennas: Another important element of any 5G mobile system will be smart antennas. When used, it will be possible to change the beam direction and allow more direct communication and limit interference and increase the overall capacity of the cell.

2. SECURITY ASPECTS OF 5G

One of the most difficult security tasks of 5G networks refers to privacy. 5G networks enable new types of applications and services and allow connecting more devices to the network, encouraging malicious users to steal and share personal information. For example, health applications collect very sensitive data about our bodies, car applications will monitor our movements and smart city applications will collect information about our way of live.

In addition to the above, with low latency and high bandwidth, 5G integrates cloud–based services, network virtualizations, personal and industrial IoT (Internet of Things) and edge platforms. This creates a problem, because more connected users and devices mean there are more things that can become uncontrollable.

Briefly, 5G might contain certain security risks for:

- It's a relatively new and in practice insufficiently tested set of complex technologies.
- It enables the movement and access of much larger quantities of data and thus increases the attack possibilities. The increased volume and diversity of information makes 5G more attractive to potential attackers who have malicious intentions. The increased number of connected devices means more potential targets for attacks. If just one of devices isn't configured correctly, then it might be possible for cybercriminals to steal data or launch a more widespread attack using botnets.
- Users will depend on it more than 4G for vital (mission–critical) communications (for instance, remote control of critical infrastructure, vehicles and medical devices and procedures).

The trustworthiness in general of the 5G system is dependent on five main security properties: communication security, identity management, resilience, privacy and security assurance. The specified properties provide a reliable platform that enables a large number of new services to be created. In 5G security area, several essential topics can be identified:

- Security assurance – The Network Equipment Security Assurance Scheme (NESAS) is jointly formulated by GSMA and 3GPP (3rd Generation Partnership Project) for evaluation of mobile network security. Developed according to security standards pertaining to vendors' product development, this scheme provides a baseline to evidence that network equipment satisfies a series of security requirements. Currently, 3GPP has initiated security evaluation of multiple 5G network equipment and major equipment vendors and operators are actively participating in the NESAS standard formulation.[4]
- Identity management – In this area, an identity is treated in two ways: as device identity and service identity. Each device (or physical) identity is globally unique and may be assigned to a device by the manufacturer. Service identities are assigned by service providers or networks. A physical identity may correspond to one or more service identities.[5]
- Network security – In modern network structure it is possible to identify four parts in general: access network (transmits data from user's phone to the mast), core network (processes the data and sends it back; the most sensitive part of the network as it handles all main customer data), transport network (sends this from the mast to the core network) and interconnect network. Each network part consists of three planes, each of which is related to specific type of traffic: the control plane carries the signaling traffic, the user plane carries the payload (actual traffic) and the management plane carries the administrative traffic. In the context of security, all planes can be exposed to special types of threats. There are also certain threats which can affect all three planes at the same time.
- Flexible and scalable security architecture – The introduction of the concept of virtualization and dynamic configurations in 5G environment has imposed usage of more flexible and dynamic security architectures. New flexible solutions do not necessarily create a conflict between usability and security. For example, new versions of network APIs allow service chaining (or service function chaining (SFC) – capability that uses software–defined networking (SDN) to create a service chain of connected network services and connects them in a virtual chain)[6], while retaining end–to–end encryption of data.
- Energy–efficient security – The implementation of energy efficient security schemes (used for key generation, processes of encryption and decryption) for data consolidation and aggregation on the way to the traffic destination represents one of the most needed factors in wireless networks.
- Cloud security – Cloud security (or cloud computing security), consists of a set of policies, controls, procedures and technologies that work together to protect cloud–based systems, data and infrastructure.[7] Network functions

[4] Huawei, Partnering with the Industry for 5G Security Assurance, https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf

[5] Huawei, 5G Security: Forward Thinking, https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf

[6] https://www.sdxcentral.com/networking/virtualization/definitions/what-is-network-service-chaining/

[7] https://www.forcepoint.com/cyber-edu/cloud-security

virtualization (NFV), based on cloud approach, fundamentally changed the architecture, security and implementation of telecommunications networks.

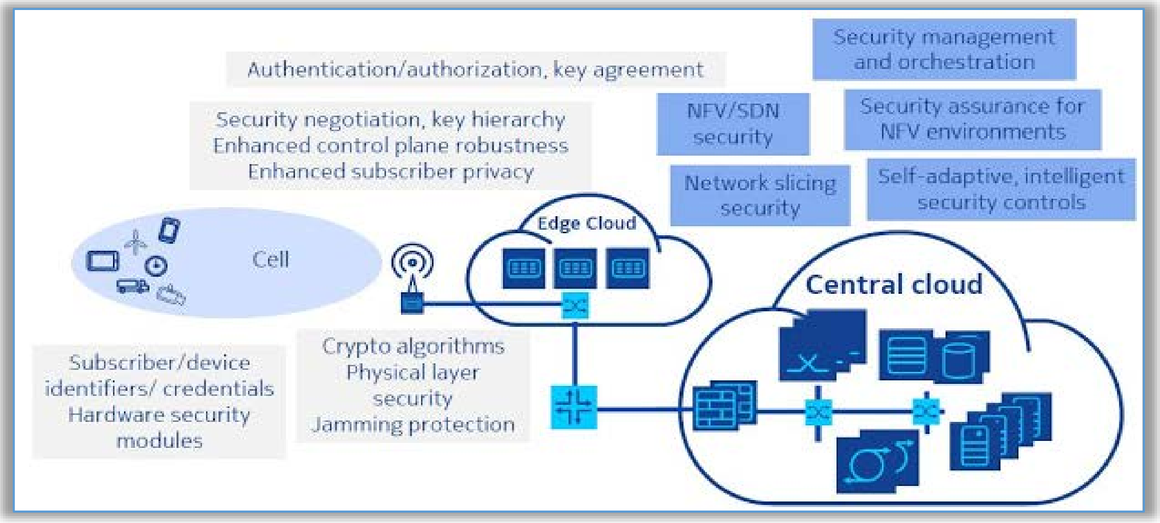
Security management and orchestration
Authentication/authorization, key agreement
Security negotiation, key hierarchy
Enhanced control plane robustness
Enhanced subscriber privacy
NFV/SDN security
Security assurance for NFV environments
Network slicing security
Self-adaptive, intelligent security controls
Edge Cloud
Cell
Central cloud
Subscriber/device identifiers/ credentials
Hardware security modules
Crypto algorithms
Physical layer security
Jamming protection

Figure 1. Elements of a 5G security architecture[8]

Bearing in mind the capability of IoT devices to bypass a central router when exchanging data, which makes them more difficult to monitor as well as more vulnerable to direct attacks, security experts rightly warn of an increased risk of distributed denial–of–service (DDoS) attacks and proximity service (ProSe) intrusions on 5G IoT environments. A large number of decentralized small networks are a serious task in terms of keeping each system updated and capable of counteracting rapidly evolving cyber–attacks.[9] Higher bandwidth may cause more potential risks, as a consequence of expected increase in the number of potentially vulnerable connected devices (unauthorized access).

Diversity of malicious software and network attacks present a complex security situation. A study conducted by ETH Zurich, the University of Lorraine and the University of Dundee [6] have found “critical gaps” in 5G connections, which allow interception of telecommunication traffic and data theft. In accordance with this study, the reason for this is possible because “security goals are underspecified” and there exists a “lack of precision” in the 3GPP standards.[10]

Besides this, a group of researchers from Purdue University and the University of Iowa [7] have found three new security attacks in 4G and 5G, which can be used to intercept phone calls and track users' locations. The first attack is called "Torpedo", which is focused on paging protocol that carriers use to notify a phone before a call or text message comes through. The second is called "Piercer", which allows an attacker to determine an international mobile subscriber identity (IMSI) on the 4G network. The third attack is a kind of cracking attack, which uses brute force on encrypted IMSI number in both 4G and 5G networks.[11]

One of the important goals in 2G and 3G security was to avoid sending IMSI in text format over the air and thus preventing malicious users from eavesdropping (in which area the user is located and what services they are using). This was avoided by using the 32–bit TMSI (Temporary Mobile Subscriber Identity), which is valid in only one location area. With this 32–bit TMSI, the subscriber introduces himself or is called. The TMSI is updated at least during each change of location area or within a predetermined period of time. Also, the mobile network can change the TMSI whenever it wants. Changed TMSI is always sent encrypted so the attacker cannot know when the change occurred. The TMSI is stored on the phone or on the smart card, but unlike the IMSI number, it is not factory–assigned to the smart card.

4G/LTE technologies use temporarily identities called Globally Unique Temporary Identity (GUTI). Unlike an IMSI, a GUTI is not permanent and is changed into a new value whenever generated and identifies the mobile device to the LTE network. 5G implements a more advanced form of network security called IMSI encryption. All traffic data which is sent over 5G network is encrypted, integrity protected and subject to mutual authentication e.g. device to network.[12]

3. 4G vs 5G SECURITY

In 4G/5G technology, five security feature groups can be defined. Each of these groups meets certain threats and accomplishes certain security objectives (Figure 2.):

[8] Nokia Solutions and Networks, http://www.vde-itg-kommunikationsnetze.de/images/stories/Fachtagungen/zdn2019/07_5G_Security_Nokia_ZdN_2019_presented.pdf

[9] https://www.telit.com/blog/5g-iot-security-issues-solutions/

[10] https://www.idginsiderpro.com/article/3315626/5g-and-6g-wireless-technologies-have-security-issues.html

[11] https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

[12] https://www.ericsson.com/en/security/a-guide-to-5g-network-security

- Network access security (I) – the set of features that provide secure access to services and which in particular protect against attacks on the (radio) access link.
- Network domain security (II) – the set of features that enable nodes to securely exchange signaling data, user data (between AN (Access Network) and SN (Serving Network) and within AN) and protect against attacks on the wired network.
- User domain security (III) – the set of features that secure access to mobile stations.
- Application domain security (IV) – the set of features that enable applications in user and in provider domain to securely exchange messages.
- Visibility and configurability (V) – the set of features that inform the user whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

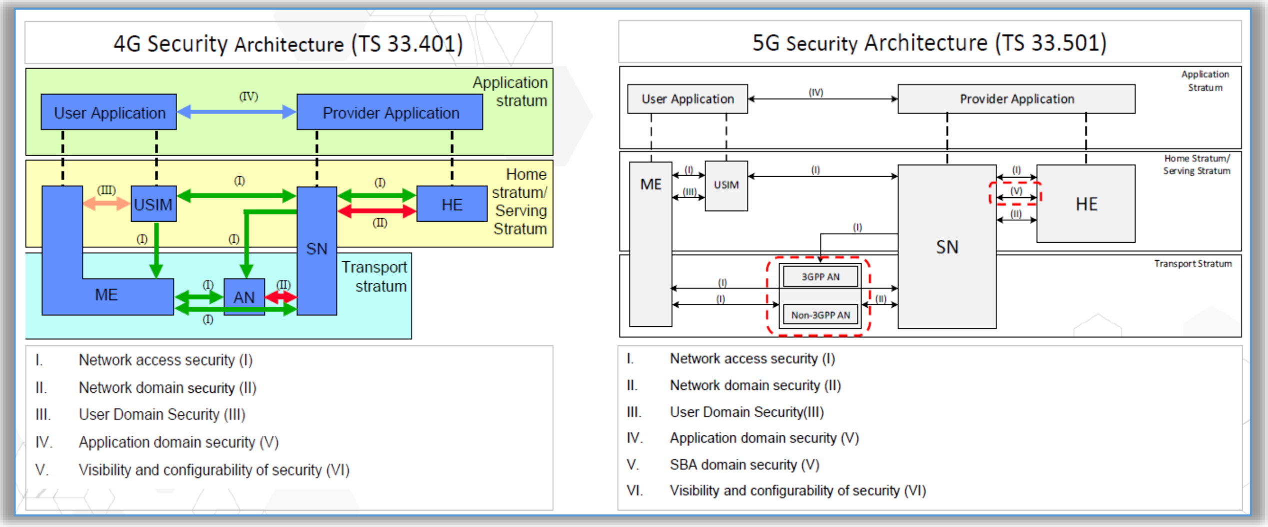
4G Security Architecture (TS 33.401)
User Application
(IV)
Provider Application
Application stratum
(III)
USIM
(I)
(I)
HE
(II)
Home stratum/ Serving Stratum
(I)
(I)
SN
Transport stratum
ME
(I)
AN
(II)
(I)
I. Network access security (I)
II. Network domain security (II)
III. User Domain Security (III)
IV. Application domain security (V)
V. Visibility and configurability of security (VI)
5G Security Architecture (TS 33.501)
User Application
(IV)
Provider Application
Application Stratum
ME
(I)
(III)
USIM
(I)
(I)
(V)
(II)
HE
Home Stratum/ Serving Stratum
(I)
SN
Transport Stratum
(I)
(I)
3GPP AN
Non-3GPP AN
(II)
I. Network access security (I)
II. Network domain security (II)
III. User Domain Security(III)
IV. Application domain security (V)
V. SBA domain security (V)
VI. Visibility and configurability of security (VI)

Figure 2. 4G vs 5G security architecture[13]
(ME – Mobile Equipment, HE – Home Equipment, USIM – Universal Subscriber Identity Module)

Comparing both security architectures, the following enhancements in 5G can be identified:
1. In case of access network (AN), 3GPP and non–3GPP access networks are treated more equally.
2. In communication between SN and HE, a new interface for Service–based Architecture (SBA) is added.

Authentication and key management are fundamental processes to the security of cellular networks because they provide mutual authentication between users and the network and derive cryptographic keys to protect both signalling and user plane data. 5G security is built around 5G AKA (Authentication and Key Agreement) protocol, an enhanced version of the protocol already used by 3G and 4G networks.[14]

There are two known weaknesses in 4G EPS–AKA:[15]

1. The authentification of user equipment (UE) is sent over mobile networks without encryption. Although a temporary identifier (GUTI) may be used to hide a user's long–term identity, it has been shown that GUTI–allocation has two security lacks: GUTIs are not changed often enough as necessary and their allocation can be predicted. More importantly, the UE's permanent identity may be sent in form of plain text in an authentification response (RES) message when responding to an authentification request message from a network.
2. A HE generates authentication vectors (AV) during communication with a serving network (SN) as a part of UE authentication, but it is not a part of the authentication decision. This decision is made exclusively by the SN.

5G–AKA differs from 4G EPS–AKA in several aspects:

- Authentication components are different because of the new SBA. Specifically, the SIDF (Subscription Identifier De–concealing Function) component does not exist in 4G.
- In case of 5G, UE uses the public key of the home network to encrypt subscription permanent identifier (SUPI) before it is sent to a network. In 4G, the UE sends its permanent identifier as clear text, allowing it to be stolen by either a malicious network (for instance, fake base station – IMSI catcher) or an attacker over the radio links (if communication is not protected). IMSI catchers work by tricking devices into connecting to them instead of the real base station, exploiting the fact that under GSM (Global System for Mobile Telecommunications) standard, devices prioritize closer and stronger signals.

[13] https://blog.3g4g.co.uk/2018/03/5g-security-updates-march-2018.html
[14] https://nakedsecurity.sophos.com/2019/02/04/security-weaknesses-in-5g-4g-and-3g-could-expose-users-locations/
[15] https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

- According to 3GPP specifications, the SUPI should not be transferred in clear text over NG–RAN except routing information (Mobile Country Code (MCC) and Mobile Network Code (MNC). The Packet Data Convergence Protocol (PDCP) can be used for the wireless interface and IPsec for transmission to guarantee the confidentiality and integrity of users' data.[16]
- The home network (for example, the authentication server function (AUSF) which does not exist in 4G) makes the final decision on UE authentication in 5G. In addition, results of authentication are also sent to unified data management (UDM) to be logged. In 4G, a home network is contacted during authentication only to generate authentication vectors. It does not make any decisions about the authentication.
- Key structure is longer in 5G than in 4G because of the implementation of two additional keys: K_{AUSF} (used to derive other keys for authentication and encryption) and K_{AMF} (Access and Mobility Management Function).

The figure 4 clearly integrates the major 5G security issues.

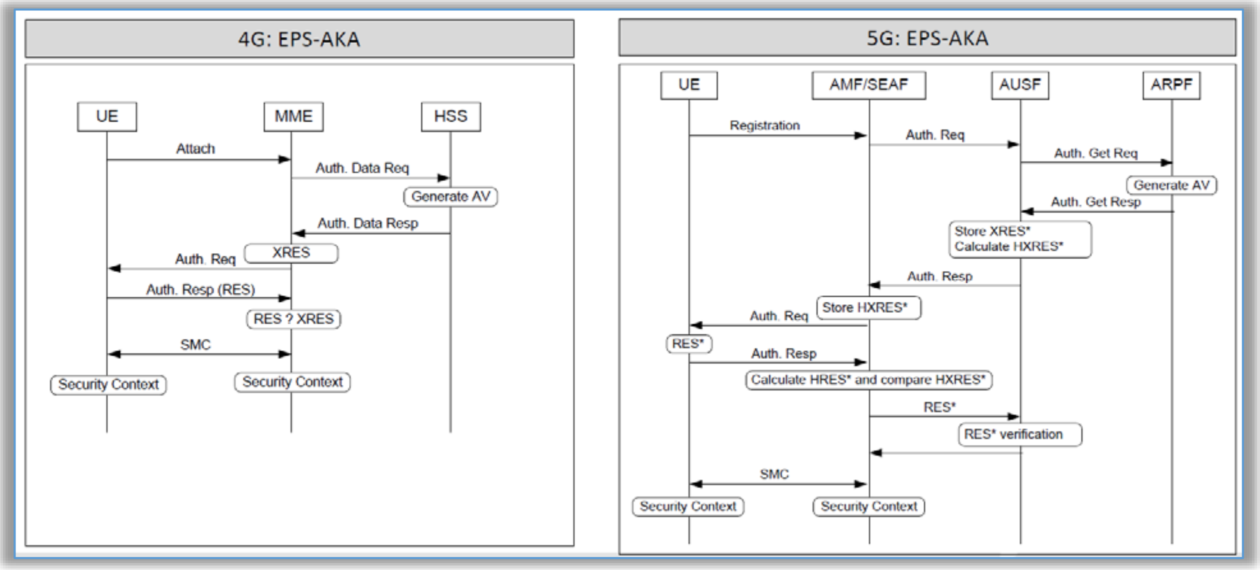

Figure 3. 4G and 5G authentication schemes[17]

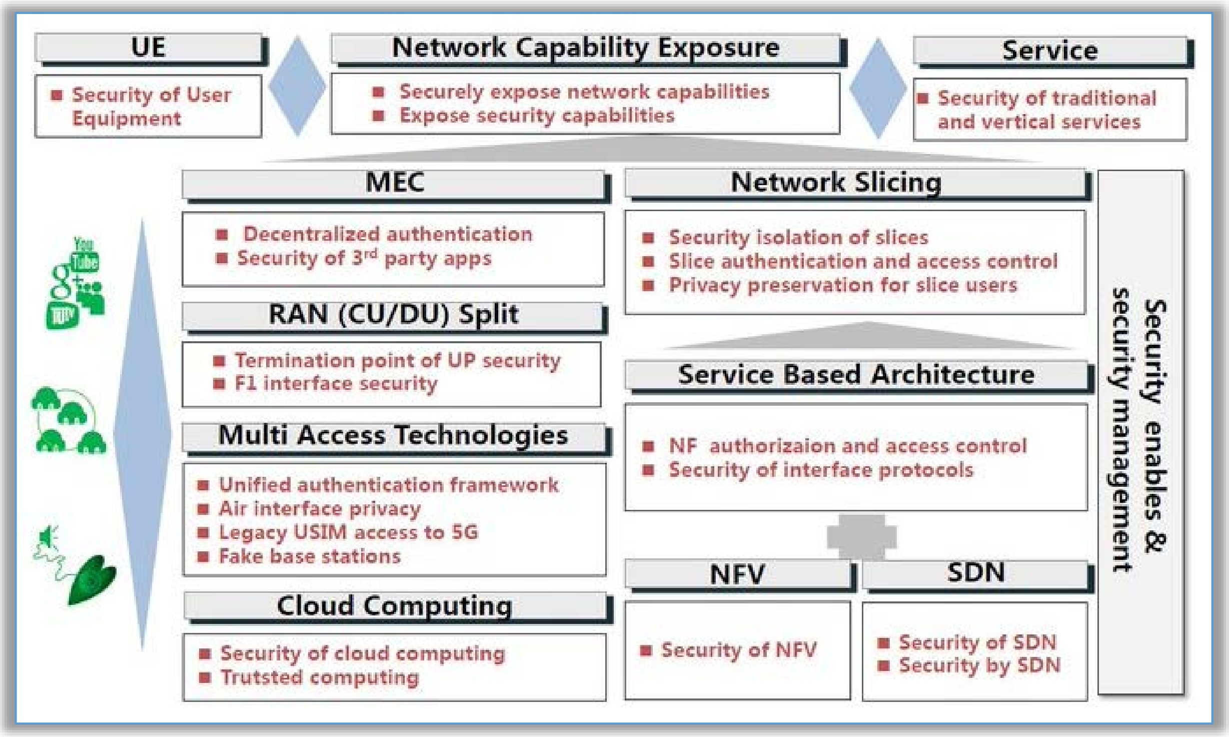
UE
Security of User Equipment
Network Capability Exposure
Securely expose network capabilities
Expose security capabilities
Service
Security of traditional and vertical services
MEC
Decentralized authentication
Security of 3rd party apps
Network Slicing
Security isolation of slices
Slice authentication and access control
Privacy preservation for slice users
RAN (CU/DU) Split
Termination point of UP security
F1 interface security
Service Based Architecture
NF authorizaion and access control
Security of interface protocols
Multi Access Technologies
Unified authentication framework
Air interface privacy
Legacy USIM access to 5G
Fake base stations
Cloud Computing
Security of cloud computing
Trutsted computing
NFV
Security of NFV
SDN
Security of SDN
Security by SDN
Security enables & security management

Figure 4. Major 5G security issues[18]

[16] https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf

[17] https://blog.3g4g.co.uk/2018/03/5g-security-updates-march-2018.html

[18] https://blog.3g4g.co.uk/2018/03/5g-security-updates-march-2018.html

4. CONCLUSIONS

Generally speaking, the majority of 5G security threats and challenges are the same as those in 4G security. But even so, consideration must be given to the security challenges brought to 5G networks by new services, architectures and technologies. For instance, consideration must be provided to access authentication for third–party slicing service providers in terms of new services. 3GPP standards take into account security threats and new 5G architecture solutions (network slicing and SBA). Another security area that needs to be considered is the determination of resource assets, particularly as 5G cloud architecture is commonly accepted. Furthermore, the effect they have on traditional cryptographic algorithms requires to be considered as new techniques such as quantum computing.

5G authentication improves 4G authentication in a number of fields, including a unified authentication structure, better UE identity protection, improved control of home network and more key separation within their derivation. But authentication in 5G is not without deficiencies. User tracking ability in 5G, for instance, may still be feasible.[19]

Among the potential risks, the use of products from unreliable manufacturers is highlighted, whereby it is important that different countries install networks with different security possibilities. In addition, vulnerabilities due to improper installation, configuration, and management, as well as "inherited" security problems from the LTE network, must be addressed. It is also recommend taking into account the risks of lack of interoperability between systems and technologies, which may also pose a major problem, as some manufacturers tend to use own specific devices that may limit the customer's ability to include devices from other manufacturers.

References

[1] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu, "FBS–Radar: Uncovering Fake Base Stations at Scale in the Wild", Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2017).

[2] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean–Pierre Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems", Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (Feburary 2016).

[3] 3GPP, "3GPP System Architecture Evolution (SAE) – Security Architecture" (Release 15), technical specification (TS) 33.401, v15.2.0 (September 2018).

[4] 3GPP, "Security Architecture and Procedures for 5G System" (Release 15), technical specification (TS) 33.501, v15.5.0 (September 2018).

[5] Byeongdo Hong, Sangwook Bae, and Yongdae Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier", Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2018).

[6] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, "A Formal Analysis of 5G Authentication", Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18) (October 2018).

[7] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, Elisa Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information", Network and Distributed System Security (NDSS) Symposium, San Diego, 2019.

ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665

5, Revolutiei, 331128, Hunedoara, ROMANIA
http://annals.fih.upt.ro

[19] https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication