Aspects of 5G Security

Daniel Nelle
University of Potsdam,
Potsdam, Germany
dnelle@uni-potsdam.de

ABSTRACT

With the 5G rollout to the general public underway, it is insightful to examine the improvements and changes the new standard brings regarding security, not only in comparison with its predecessor, 4G, but also in the context of new functions and use-cases. This paper will take a brief look at the new service-based security architecture of 5G, explain how the new authentication prodedure increases security through identity protection and home network control and finally analyze how the much anticipated feature of network slicing might be protected in a 5G environment.

1 INTRODUCTION TO 5G

Mobile carriers across the globe are increasingly rolling out 5G to end users while device manufacturers are announcing more and more devices capable of using the new standard. This happens against a background of political noise generated by governments trying to limit China's influence in the markets it sells its mobile equipment to. A significant part of the population has thus heard of this technology, claimed by some to be poised to change our lives throughout the next decade. Most of those familiar with the term 5G from advertisements and evening news coverage, however, seem to associate it with higher data rates and see it as the final blow to loading bars on high-definition content and choppy images of relatives/ colleagues in video calls.

While increased data rates certainly are one of 5G's outstanding features, it is unlikely that it was this improvement that caused opinion leaders to declare it to have such profound impact on the 2020's. We thus begin this short treatise on aspects of 5G security with a brief introduction to the standard and its features and only then will turn to the architecture and some of the mechanisms intended to make it safer and more flexible than its predecessor, 4G. Afterwards we will examine one of the other features of 5G, network slicing, more closely and look at the implications this technology has from a security perspective. Finally, we will summarize our findings in a brief conclusion.

1.1 What is 5G?

5G is a mobile standard specified by the 3rd Generation Partnership Project (3GPP), an umbrella term for a number of standards organizations developing mobile communication protocols. Its chief features are composed of four use cases which will allow an improvement to existing or enable completely new applications, often related, but not limited to, the Internet of Things (IoT), or, to employ a broader term, the *Internet of Everything*. The most prominent feature is enhanced Mobile Broadband (eMBB), which will allow peak data rates of 10 GB/s [10] and will be what most people will have direct contact with through mobile devices such as smartphones. Massive Machine-Type Communications (MMTC) is supposed to allow an excess of one million connections per square kilometer [10], thus enabling interconnected, sensor-rich environments such as "smart" factories and cities. Ultra-Reliable Low-Latency Communications (URRLC) aims at latencies lower than one millisecond and 99,9999% reliability [10], paving the way for applications such as Vehicle-to-vehicle (V2V) communications. Compared to 4G it is conceived as a Service Based Architecture (SBA) [6], where control plane functionality and data repositories are provided by means of interconnected Network Functions (NFs). Those expose their services through well-defined Representational State Transfer (REST) Application Programming Interfaces (APIs) and thus enable the respective components to be virtualized and distributed [6]. This in turn permits *network slicing*, where resources on the mobile network can be offered in an Infrastructure-as-a-service (IaaS) manner, much like popular cloud operators already do with compute and regular network services.

1.2 5G Architecture

Figure 1 gives a rough overview of the 5G architecture. Pictured in the middle is the 5G Core (5GC), which houses the aforementioned NFs, such as the Authentication Mobility Function (AMF)/Session Management Function (SMF), responsible for authentication in a roaming context, User Plane Function (UPF), managing connections to Data Networks (DNs), the Non-3GPP Interworking Function (N3IWF), serving as an endpoint to untrusted non-3GPP access, and the Authentication Server Function (AUSF), another component involved in authentication. The node captioned *5G NF* is a placeholder for all other possible NFs, such as functions related to V2V. On the far left of Figure 1 some of the devices expected to be connecting to the 5G core are pictured, together with two possible access methods: The wireless variant via a Radio Access Network (RAN), a mode most

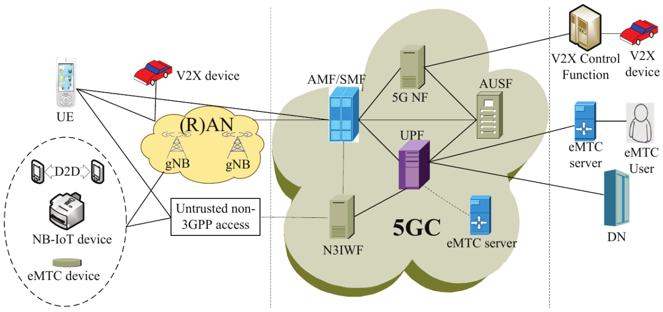

Figure 1: 5G Architecture [4]

users will associate with how their mobile phone gets a network signal, where the device establishes a radio connection with a base station, called Next generation NodeB (gNB) in a 5G context [2]. Additionally, 5G allows so-called *untrusted non-3GPP access* via Wi-Fi and cable connections, where the corresponding NF serves as an intermediary. A range of devices other than regular mobile handsets (called called User Equipment (UE) here), is expected to be part of the network. Those include, but are not limited to, Device-to-device (D2D) communications enabled devices, Narrow Band IoT (NB-IoT) devices, enhanced Machine Type Communication (eMTC) devices and Vehicle-to-everything (V2X) enabled smart cars.

2 5G SECURITY ARCHITECTURE

Figure 2 shows 5G schematically from a security perspective and adds roaming to the picture, where a device connects to its Home Public Land Mobile Network (PLMN) through a Visited PLMN. End users know this scenario from when they are traveling abroad and using their mobile devices or, in some countries, when their phone uses a different carrier's network because the own carrier does not provide coverage in a given area. The AUSF is located in the home network and plays a central role in the authentication process of a UE wanting to join a network. It relies on the User Data Management (UDM) for keys and other services, which this provides through two functions: The Authentication Credential Repository and Processing Function (ARPF), responsible for selecting an appropriate authentication method as well as computing keys [5] and the Subscriber Identity De-concealing Function (SIDF), taking care of encrypting and decrypting the UE's unique identifier. The SMF is located in the visited network and provides session management as well as DHCP and IP allocation services. The AMF is located in the visited network, too, and plays the most important function here, since it acts as a middleman between UE and the home network [1]. It is co-located with the Security Anchor Function (SEAF) holding the anchor key for the visited network, from which all other keys are derived [1]. The UPF

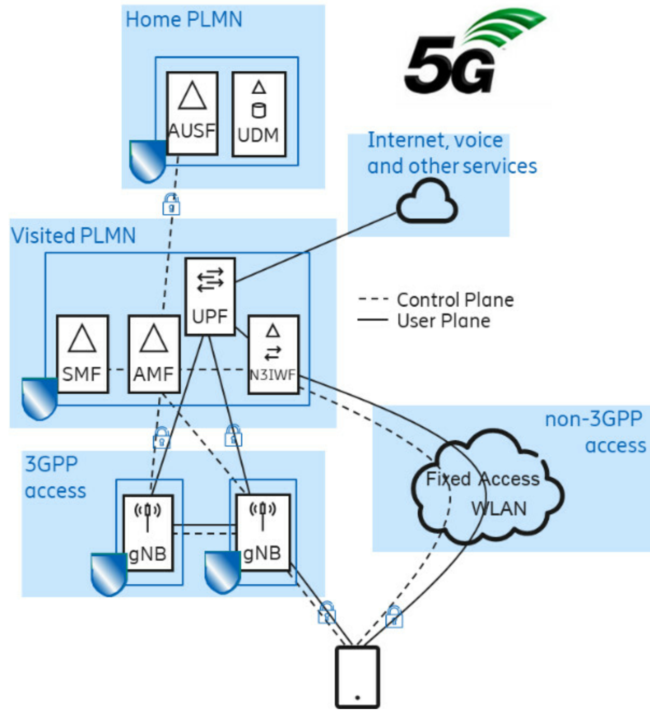

Figure 2: 5G Security Architecture [7]

manages packet routing and forwarding and is thus responsible for connecting the user to services such as the Internet. The N3IWF acts as a VPN endpoint for connections not established via a 5G radio connection. A gNB, usually depicted as one component, in fact consists of a Distributed Unit (DU) and a Central Unit (CU). The former is a "dumb" component unable to access any data it forwards and is intended to be deployed to remote sites vulnerable to illegal access, while the latter is where *access stratum security* is terminated and which is intended for locations where access can be more strictly controlled. This means that data encrypted for wireless transmission over the RAN is decrypted here [1]. As the padlocks on the links indicate traffic and control messages are encrypted when being transferred between access stratum, visited network and home network while data exchanged between the UPF and the Internet is not.

3 5G ACCESS

The 5G access procedure is improved in several ways compared to its predecessor. Support for multiple authentication methods allows a wider variety of use cases and enables equipment without a Universal subscriber identity module (USIM)(aka SIM-card) to participate in the network. A major improvement is better identity protection, because the SUbscription Permanent Identifier (SUPI), an identifier hardcoded onto the SIM-card, now is always encrypted using

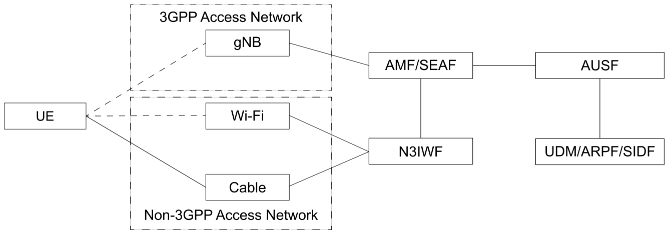

Figure 3: Security Contexts [3]

the home network public key. Another big advancement is enhanced home network control through the authentication procedure. While in 4G the visited network had to be trusted, 5G puts the final responsibility on the home network and gives it the power to verify an authentication attempt by requiring proof of the UEs participation in the exchange. Before that, an attacker could feign the presence of an UE in the network and thus carry out a man-in-the-middle attack. However, with all the improvements in place, tracking of a UE might still be possible [3]. In the following sections we will examine how increased security and privacy is achieved in 5G more closely.

3.1 5G Authentication Framework

In order to allow 5G authentication to be open as well as access-network agnostic, a unified authentication framework depicted in Figure 3 has been defined for 5G. It makes it mandatory to implement at least two authentication options: 5G Authentication and Key Agreement (AKA) as well as (Extensible Authentication Protocol (EAP)-AKA'). EAP support ensures the openness requirement is met, while the introduction of the N3IWF allows access to the 5G core over untrusted alternatives such as Wi-Fi and cable by putting the traffic through IPsec tunnels [3]. The framework also supports the establishment of several security contexts with only one authentication pass, thus allowing a device to move between 3GPP and non-3GPP seamlessly without the overhead of another authentication [3]. Finally, support for EAP-Transport Layer Security (TLS) is possible, which allows equipment without a USIM to participate. We will examine 5G-AKA more closely in a later section.

3.2 Increased Privacy

Figure 4 shows how a subscriber's identity is protected through encryption in 5G. The SUPI, a unique identifier, consist of Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Idendification Number (MSIN) [8]. Since the former two components have to be readable and are not considered sensitive information, only the MSIN is protected. On the UE the home network public key is used to encrypt the MSIN via an asymmetric encryption algorithm to

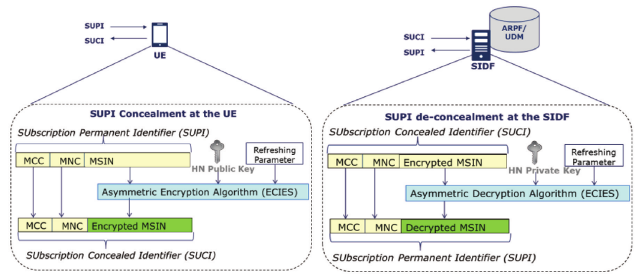

Figure 4: SUPI Encryption and Decryption [8]

produce the SUbscription Concealed Identifier (SUCI) [1]. This protected identifier is used for transmissions over unsafe channels. Only after a successful authentication the visited network gains access to the decrypted form. On the other side, in the home network, the SIDF, which is hosted by the UDM, is able to decrypt the MSIN by using the home network private key. This scheme prevents i.e. an attack via a fake base station, where the attacker could insert herself between subscriber and home network and thus carry out a man-in-the-middle attack [8].

3.3 5G Authentication and Key Agreement

Let us now take a closer look at the 5G AKA message exchange depicted in Figure 5. We will see where the aforementioned improvements, namely identity protection and home network control, come into effect [3].

(1) The SEAF starts the authentication procedure after receiving any signalling message from the UE. This message should include a SUCI or Globally Unique Temporary Identifier (GUTI). For the sake of brevity, we will focus on the former case.
(2) The SEAF starts the procedure by sending a request to the AUSF.
(3) The SEAF verifies the request is authorized and forwards the request to the UDM.
(4) The UDM decrypts the SUCI in the SIDF and lets the ARPF select the appropriate authentication method, 5G-AKA in our case.
(5) The UDM initiates AKA by sending an authentication vector consisting of an AUTH token, a XRES (expected response) token, a key K_{AUSF} and the SUPI, if it was included earlier, to the AUSF.
(6) The AUSF stores the key K_{AUSF} and computes a hash of XRES, called HXRES.
(7) The AUSF passes the AUTH token and HXRES to SEAF. **Note how the SUPI is not sent here**.
(8) The SEAF forwards the AUTH token to the UE.

[1]Spelled *Sushi*

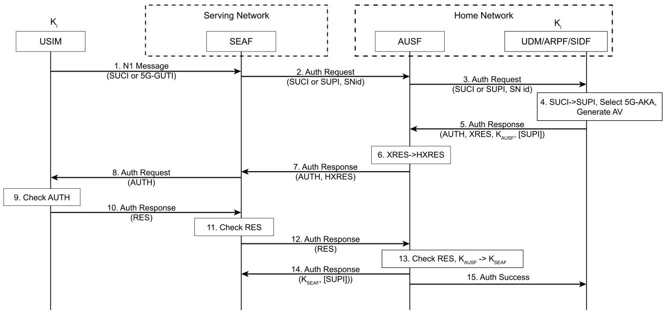

Figure 5: 5G AKA Message Flow [3]

(9) The UE validates the AUTH token with the secret key it shares with the home network. If this validation succeeds, from the UEs perspective, the authentication has succeeded.
(10) The UE sends a RES token to the SEAF.
(11) The SEAF validates the RES token.
(12) The SEAF sends the RES token to the AUSF.
(13) The AUSF validates the RES token. **The final decision about whether the procedure succeeded is made here, in the home network!** If the token is valid, a key K_{SEAF} is computed from the stored K_{AUSF}.
(14) The AUSF sends K_{SEAF} and SUPI to the SEAF. **Note how the SUPI is only sent here, after the procedure succeeded.**
(15) The UDM is informed of the outcome for logging.

Steps 7, 13 and 14 show how increased privacy and home control are achieved.

3.4 Key Hierarchy

Figure 6 shows the key hierarchy in 5G. After concluding the AKA message exchange, the SEAF derives the *anchor key* K_{AMF} and deletes K_{SEAF} immediately. The new key is then passed to the AMF, which is located together with the SEAF. The AMF can now derive all the other keys needed for access stratum (K_{gNB}) and non-access stratum (K_{NASint}, K_{NASenc}) security as well as a key for non-3GPP access (K_{N3IWF}). Since the root key K is shared between the home network and the UE, because it houses the USIM, onto which the key is hard-coded, the UE can derive any key in the hierarchy and thus possesses a complete set of keys [2].

4 SLICING

4.1 What is Slicing?

Network slicing is understood as the creation of independent logical networks on shared infrastructure by means of Software Defined Networking (SDN) and Network Function Virtualization (NFV). While the former separates the control

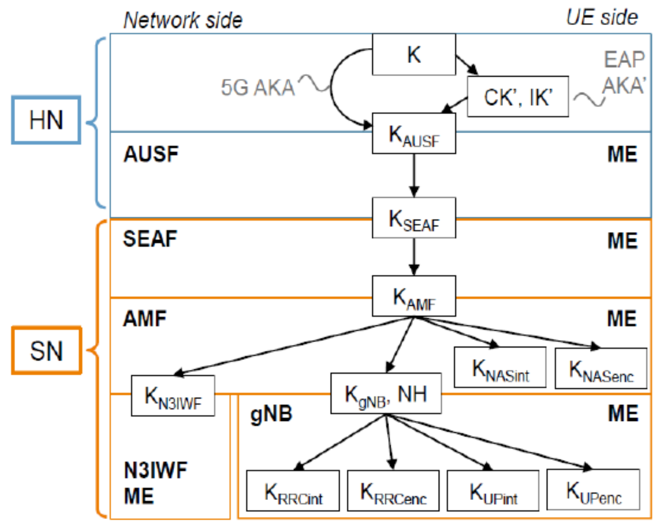

Figure 6: 5G Key Hierarchy [8]

from the forwarding plane and thus allows centralized administration of network resources via a protocol such as OpenFlow, the latter decouples network functions i.e. firewalls, from specialized hardware by emulating the corresponding functions on regular servers through software. Slicing is intended to do to 5G what IaaS providers such as Amazon EC2 or Microsoft Azure do to regular network and compute resources [9]. Naturally, this involves a broad spectrum of actors, from hardware manufacturers to mobile network operators. Protecting sensitive data sent over a network slice from third parties thus becomes an almost impossible feat, since the mobile network operator renting out a slice to a customer in any case will have the ultimate authority over infrastructure and access to at least metadata. In the following a couple of possible approaches to ensure varying degrees of isolation from [9] will be briefly outlined.

4.2 Slice Isolation and Security

4.2.1 Over-the-top Isolation. One possible means of protecting data sent through an untrusted network is Over-the-top (OTT) security, meaning isolation by through technologies such as a Virtual Private Network (VPN). Authentication can be performed in the user plane, which, however, implies a prior admission of the user trying to authenticate herself into the network slice without knowing whether she actually has the credentials needed for a secure connection. To avoid this problem, the control plane can be used [9]. This type of isolation requires two sets of credentials, namely one for OTT security and one for the mobile network, thus putting additional overhead on the entity renting a network slice from a mobile operator, as credentials have to be issued and maintained in a database. OTT security offers confidentiality and integrity protection against the mobile operator, but comes with drawbacks attached: The mobile operator can still siphon off significant amounts of metadata such as a user's location, identity, connection time and duration, etc. Additionally, no resource isolation can be guaranteed, meaning that the tenant renting a slice can not know whether he is actually allocated the resources he is paying for or whether he might be sharing excess resources with another client of the mobile operator. This is relevant in a scenario where a tenant pays for a specific amount of resources to be available on short notice, i.e. in an emergency/ peak load scenario.

4.2.2 Private 5G Network. As the authors of [9] point out, full isolation from the operator without own infrastructure is not possible. A straightforward solution to this problem is to deploy a private network, including base stations, a 5G core and a data network, where the whole network and all devices are managed by the owner without participation of a mobile operator. This approach is feasible for huge industrial actors owning large sites or factories. In order to ensure wireless coverage over the area of the site, unlicensed spectrum would have to be used or frequencies would have to be leased from a mobile operator for geographically constrained on-site operations, since the spectrum on which mobile networks operate is heavily regulated and auctioned off to mobile operators for high prices. Such a solution would grant the highest degree of isolation, leaving only direct attacks on radio interfaces as well as deliberate backdoors as possible vectors for security breach. It comes, however, at the cost of significant overhead and is thus only suitable for organizations with the corresponding resources [9].

4.2.3 Private-Public Network. Figure 7 shows the schematics of a private/ public network mix which corresponds to a home/ visited network scenario in a regular public mobile network context. The tenant operates his own private 5G network as described above, but enables devices that leave the area covered by this private network to connect to the home network by means of roaming. A possible use case might be employees' mobile devices or vehicles, which spend time on-site as well as off-site but need constant access to some kind of Industry 4.0 data network. The improvements to 5G authentication described earlier allow for authentication between the home network's AUSF and the off-site device. Owing to the fact that the 5G security framework allows the establishment of several security contexts with only on authentication pass, the AUSF can use one key for OTT security between the home network 5G core and the device, while the visited network's AMF has another key for control plane communication with the roaming device. This approach makes the maintenance of an additional credentials database on the tenants side obsolete and hides metadata

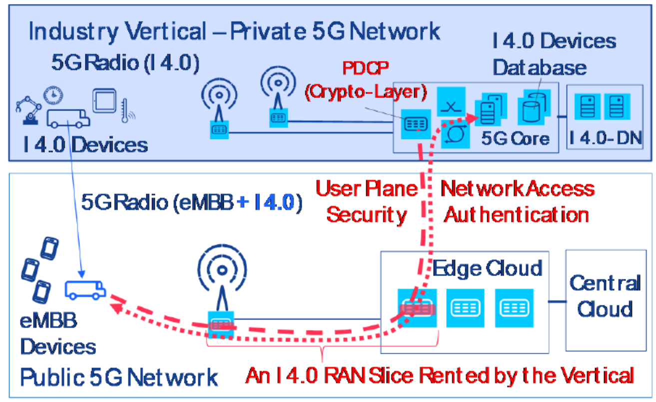

Figure 7: Private-Public Network Split [9]

from third parties, as long as the mobile equipment is kept on-site. In the roaming scenario, the metadata is still exposed to the mobile operator [9].

4.2.4 Private Network with Public RAN Slice. Another approach can be seen in Figure 8. Here, a tenant only rents a slice of a public RAN for off site operations, while still having a full private network on-site. We can see that more functions are delegated to the private network, as there is no mobile carrier operated AMF present anymore. This function, too, now is part of the private network's 5G core. Isolation is achieved by encrypting the data until it reaches the private network, thus preventing the mobile operator from listening. This is achieved by implementing the Packet Data Convergence Protocol (PDCP), which usually would be located at the gNBs CU (we recall that access stratum security is terminated there) in the private network, a solution allowed by the 5G standard [9]. The PDCP is responsible, among others, for data encryption and decryption. With such an approach, all credentials would be stored exclusively in the private network and therefore well protected. The private network, however, would have to manage mobility for its devices, as there is no mobile carrier operated AMF anymore. Additionally, devices would still have to somehow identify themselves to the RAN for it to decide which slice they should be attached to.

4.2.5 Gateway Core Network. The last approach, pictured in Figure 9, is suitable for organizations without a large enough site to warrant the establishment of a private 5G network, but with possibly a large network of critical IoT devices whose communications are to be isolated on an own slice, while ensuring connectivity to the Internet via eMBB. Here, RAN and AMF are provided by the mobile operator. The critical IoT slice is managed by a private 5G core, thus keeping sensitive data, including credentials and user plane keys, on private infrastructure. Another slice is responsible

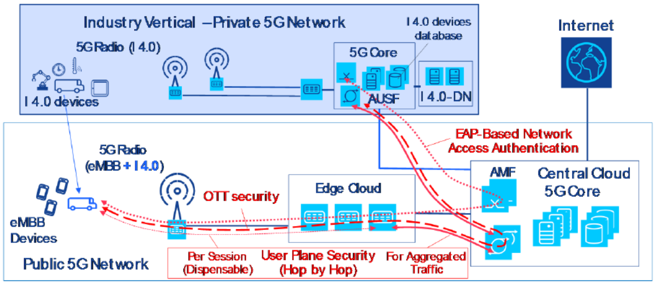

Figure 8: Private Network with Public RAN Slice [9]

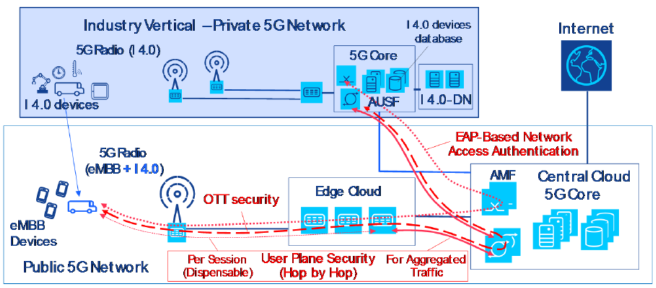

Figure 9: Gateway Core Network Approach [9]

for internet connectivity via eMBB and managed by a 5G gateway core operated by the mobile operator. This way critical communication is isolated against third parties, while the devices still have access to public parts of the network, such as Internet. As with the other approaches, the issue of metadata being visible to the operator persists.

4.2.6 Summary. In summary it is evident that flexibility in the form of greater coverage/ the possibility to roam outside of privately owned sites has to be bought at the expense of isolation. Conversely, an increase in privacy usually entails a significant increase in overhead, as more functions usually offered by a mobile network operator have to be taken care of. In all cases, except for the completely private network, metadata can be easily acquired by the mobile network operator.

5 CONCLUSION

5G offers several improvements over its predecessor 4G. The SBA allows for flexibility and can be leveraged to virtualize and decentralize the 5G core, while leaving open the possibility of adding new functionality. SUPI encryption and increased home network control achieved through the home network's AUSF having the final say in authentication significantly increase privacy and security, among others preventing man-in-the-middle attacks with false base stations. The new security framework enables participants without USIM powered devices to connect to the network as well as access through Wi-Fi/ cable through the newly introduced N3IWF. Seamless switching of access methods is enabled through the establishment of several security contexts with only one authentication pass. Slicing as a revenue model for mobile operators may proliferate, however, it comes with concerns regarding isolation of the respective tenants renting resources on the network.

REFERENCES

[1] 3GPP. Security architecture and procedures for 5G System. Technical Specification (TS) 33.501, 3rd Generation Partnership Project (3GPP), 03 2020. Version 15.8.0.
[2] 3GPP. System Architecture for the 5G System. Technical Specification (TS) 23.501, 3rd Generation Partnership Project (3GPP), 03 2020. Version 15.9.0.
[3] Cablelabs. A Comparative Introduction to 4G and 5G Authentication. https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication. Accessed: 2020-06-04.
[4] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong. A survey on security aspects for 3gpp 5g networks. *IEEE Communications Surveys Tutorials*, 22(1):170–195, 2020.
[5] Ericsson. Overview: Security architecture in 5G and LTE/4G systems. https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview. Accessed: 2020-06-04.
[6] Metaswitch. What is the 5G Service-Based Architecture (SBA)? https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-service-based-architecture-sba. Accessed: 2020-06-20.
[7] Anand R. Prasad, Sivabalan Arumugam, Sheeba B, and Alf Zugenmaier. 3GPP 5G Security. https://www.3gpp.org/news-events/1975-sec_5g. Accessed: 2020-06-04.
[8] Anand R. Prasad, Sivabalan Arumugam, Sheeba B, and Alf Zugenmaier. 3gpp 5g security. *Journal of ICT Standardization*, 6(1):137–158, 2018.
[9] P. Schneider, C. Mannweiler, and S. Kerboeuf. Providing strong 5g mobile network slice isolation for highly sensitive third-party services. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2018.
[10] IEEE Spectrum. 3GPP Release 15 Overview. https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview. Accessed: 2020-06-20.