IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2022, accepted February 8, 2022, date of publication February 10, 2022, date of current version February 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151000

A Systematic Analysis of 5G Networks With a Focus on 5G Core Security

QIANG TANG[1], ORHAN ERMIS[1], CU D. NGUYEN[2], ALEXANDRE DE OLIVEIRA[2], AND ALAIN HIRTZIG[2]
[1]Luxembourg Institute of Science and Technology, 4362 Esch-sur-Alzette, Luxembourg
[2]Cyberforce Department, POST Luxembourg, 2417 Luxembourg City, Luxembourg

Corresponding author: Qiang Tang (qiang.tang@list.lu)

This work was supported in the context of the RDI Law Project "POST 5G Secure Experience" by the Luxembourg Government.

ABSTRACT After many years of work, 5G standards are still under development and the corresponding technical specifications continue to evolve on the fly. At this moment, several countries have started to deploy 5G networks, and most of them have been following a Non-Standalone (NSA) path to incorporate the existing 4G and other legacy networks. Despite all the advertisement efforts, many people still do not have a clear view on how 5G can power all the promised mission-critical applications in a secure manner. In this paper, we bridge this gap by providing a concise review of some 5G's new features, including the Service Based Architecture (SBA) and key Network Functions (NFs), the new security features in User Equipment (UE) and Radio Access Network (RAN), the new trust model and security mechanisms (e.g. the 5G AKA protocol), and the newly introduced common API framework (CAPIF). Along with the review of new features, we provide our observations on the potential security concerns accompanied with the relevant research results in the literature. We finally point out some new research directions.

INDEX TERMS 5G, security, privacy, authentication and key agreement.

LIST OF ACRONYMS AND DEFINITIONS

Acronym	Description
3GPP	3rd Generation Partnership Project.
5G AKA	5G Authentication and Key Agreement.
5G-NSA	Non-Standalone 5G deployment.
AMF	Access and Mobility Management Function.
ARPF	Authentication Credential Repository . and Processing Function.
AUSF	Authentication Server Function.
BMSC	Broadcast Multicast Service Center.
CAPIF	Common API Framework.
CU	Central RAN Units.
CUPS	Control and User Plane Separation.
DPI	Deep Packet Inspection.
DU	Distributed RAN Units.
eMBB	Enhanced Mobile Broadband.
GCI	Global Cable Identifier.
GLI	Global Line Identifier.
GTP	GPRS Tunnelling Protocol.
HPLMN	Home Public Land Mobile Network.
IMSI	International Mobile Subscription Identity.
IPX	Internetwork Packet Exchange.
JOSE	Javascript Object Signing and Encryption.
JSON	JavaScript Object Notation.
LMF	Location Management Function.
MBMS	Multimedia Broadcast Multicast Services.
MCC	Mobile Country Code.
ME	Mobile Equipment.
MEC	Mobile Edge Computing.
mMTC	Massive Machine Type Communications.
MNC	Mobile Network Code.
N3IWF	Non-3GPP access Inter-Working Function.
NAS	Non-Access Stratum.
NCC	Next Hop Chaining Counter parameter.
NEF	Network Exposure Function.
NFs	Network Functions.
NFV	Network Function Virtualization.
NG-RAN	Next Generation Radio Access Network.
NGAP	NG Application Layer Signalling Protocol.
NRF	Network Repository Function.
NSA	Non-Standalone.
NSSAI	Network Slice Selection Assistance Information.

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

NSSF	Network Slicing Selection Function.
OAUTH	Open Authorization.
P-GW	Packet Data Network Gateway.
PCF	Policy Control Function.
PCRF	Policy and Charging Rules Function.
PDU	Protocol Data Unit.
PFCP	Packet Forwarding Control Protocol.
RAN	Radio Access Network.
S-GW	Serving Gateway.
SBA	Service Based Architecture.
SCEF	Service Capability Exposure Function.
SCP	Service Communication Proxy.
SDN	Software Defined Network.
SEAF	SEcurity Anchor Function.
SEPP	Security Edge Protection Proxy.
SIDF	Subscriber Identity De-concealing Function.
SMF	Session Management Function.
SMS	Short Message Service.
SMSF	Short Message Service Function.
SUCI	Subscription Concealed Identifier.
SUPI	Subscription Permanent Identifier.
TDF	Traffic Detection Function.
TEID	Tunnel Endpoint Identifiers.
TLS	Transport Layer Security.
TMSI	Temporary Mobile Subscriber Identity.
UDM	Unified Data Management.
UDM	Unified Data Management.
UDSF	Repository and Processing Function.
UE	User Equipment.
UPF	User Plane Function.
URLLC	Ultra Reliable Low Latency Communications.
VLR	Visitor Location Register.
VPLMN	Visited Public Land Mobile Network.

I. INTRODUCTION

The fifth generation (5G) cellular network is gradually deployed in some countries, mostly in Non-Standalone (NSA) mode in order to incorporate the legacy networks such as 4G. 5G has brought unprecedented promises for use cases in various verticals, benefiting from its enhanced capabilities including Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). At this moment, most existing applications are leveraging the eMBB capability while the URLLC and mMTC capabilities are yet to be fully exploited.

Although 5G does not introduce a completely new architecture from scratch (as seen in Section II), it has made remarkable changes from earlier generations. The 5G core network adopts a service-based architecture (SBA), which provides great flexibility and unlimited expandability. To cater to emerging functionalities and services, corresponding functions can be plugged into the network without any need to change the existing architecture. The SBA architecture makes it possible to explore innovative software technologies such as Software Defined Network (SDN) and Network Function Virtualization (NFV). These new technologies enable network slicing, a technology to provide on-demand and dedicated QoS and network access for customers. In contrast to previous generations, 5G aims at a seamless integration with Internet infrastructure and Web applications. To this end, 5G has avoided proprietary standards in the Telecom domain and fully embrace Internet standards like TCP/IP and HTTP/2.0. Security related, except for specific scenarios (e.g. using PRINS (Protocol for N32 Interconnect Security) in the roaming scenario), 5G adopts the widely deployed Transport Layer Security (TLS) for protecting transportation layer communications and OAuth2.0 for dealing with authorizations between network functions. The technical specifications for 5G (including the new radio and the SBA architecture) are defined under the coordination of the 3rd Generation Partnership Project (3GPP) [1].

The adoption of SBA and full embracement for Internet protocols on one hand creates all the promises of 5G and makes it an infrastructure for existing and emerging applications. On the other hand, 5G brings enormous security concerns, which impact not only the typical SMS and voice services but also can potentially cause catastrophic consequences for the new services. For example, one such new service can be 5G-powered medical robot performing remote brain surgery. As such, the 3GPP Technical Specification Group Service and System Aspects (TSG-SA) dedicates a work group, namely WG3, to define the requirements and specifying the architecture and protocols for security and privacy in 3GPP systems. Other standardization bodies and organizations, e.g. ITU-T, IEEE/IETF, ETSI, GSMA and NIST, have also been actively cooperated with 3GPP to address the security and privacy issues for 5G.

The security aspects of 5G system have been mainly addressed in several 3GPP specifications and reports. The technical specification TS 33.501 specifies the security architecture, i.e., the security mechanisms and security procedures performed within the 5G System including the 5G Core and the 5G New Radio. The 3GPP TS 33.122 document specifies the security architecture for the common API framework (CAPIF) as per the architecture and procedures defined in 3GPP TS 23.222. The technical report TR 33.811 studies on the threats, potential security requirements and solutions for the features of 5G network slicing management, and some remaining issues are further investigated in 3GPP's report TR 33.813. It is worth mentioning that GSMA has contributed to improving 5G security, e.g. its Fraud and Security Group has published the FS.36 reference document for *5G Interconnect Security*.

A. PUBLIC AND PRIVATE EFFORTS FOR 5G SECURITY STUDY

Among all, the EU has played a prominent role in investigating 5G security. In October 2019, the EU's NIS

cooperation group published a high-level report on the coordinated risk assessment of 5G networks [2]. Later this group published another toolbox report [3], aiming at identifying a possible common set of measures to mitigate the main cybersecurity risks of 5G networks, and to provide guidance for the selection of measures at national and at the union level. In December 2020, ENISA published its second edition of 5G threat landscape [4]. This report summarizes the developments in the 5G architecture, identifies the vulnerabilities and provides threat assessments. In February 2021, ENISA published a report on the security controls in 5G specifications [5]. It highlights the mandatory and optional choices for security configurations and provides recommendations on the good security practices to be considered by the operators and service providers. Besides these general reports, ENISA has also contributed to addressing specific security issues in 5G, such as the signalling security report published in March 2018 [6] and the threat landscape and good practice guide for SDN published in December 2016 [7].

The advancement of 5G security research and development has greatly benefited from research projects under the umbrella the 5G Infrastructure Public Private Partnership (5G PPP), which is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, small and medium enterprises, and research Institutions). Starting from 2015, 5G PPP has initiated three rounds of projects. In Phase 1, the project 5G-ENSURE [8] aims at setting the security vision for 5G PPP and it has contributed to the standardization via interactions with organizations such as ETSI, GSMA and ITU-T, the project CHARISMA [9] investigates converged heterogeneous advanced 5G Cloud-RAN architecture for Intelligent and Secure Media Access. In Phase 2, the project 5G-MoNArch [10] investigates how to guarantee reliable, resilient and secure 5G network services for industrial use cases such as mobile sensor connectivity (barges in the port), high reliable traffic management (connected traffic light), the project IoRL [11] develops a safer, more secure, customizable and intelligent building network that reliably delivers increased throughput (greater than 10Gbps) from access points pervasively located within buildings. In Phase 3, the project 5G-COMPLETE [12] aims at an enhanced security framework for 5G architecture based on post-Quantum cryptosystems, the project 5G ZORRO [13] investigates how Distributed Ledger Technologies (DLT) can be adopted to implement flexible and efficient distributed security and trust across the various parties involved in a 5G end-to-end service chain, the project INSPIRE-5Gplus [14] aims at advancing the security of 5G and Beyond networks via two main approaches: (1) by leveraging/extending existing assets such as Trusted Execution Environments (TEEs), Remote Attestation/Path Proof/Root Cause Analysis, and end-to-end liability management between parties, and (2) by introducing novel solutions/paradigms exploiting the potential of new trends including AI/ML and Blockchains.

B. OVERVIEW OF 5G SECURITY RESEARCH RESULTS

In addition to the public and private efforts for the 5G security, there have been many other academic and industrial research in the domain, e.g., [7], [15]–[26]. In this subsection, we briefly categorize the existing research results and summarize them below.

1) GENERAL RESULTS ON 5G SECURITY

5G introduces a new way of representation for the core network with the new Service Based Architecture (SBA). Therefore, the most prominent security issue regarding 5G security is the new threats unveiled by the 5G SBA. To this end, we first consider the survey proposed by Køien in [15]. It examines the key security technologies, such as TLS, OAuth, JOSE, for the SBA architecture, including the N32 interface application layer security in the roaming scenario. The paper highlighted that the biggest risk is from the complex nature of the protocol stacks. One particular example is the weakness in JSON specification. Due to the lack of version information in JSON format, there can be several issues with respect to the use of JSON with some relatively complex modules such as OAuth 2.0. Additionally, providing common security services, including authentication, availability, data confidentiality, key management, and privacy are critical for 5G wireless networks as described by Fang *et al.* in [16]. The study investigates the existing and newly developed security services with respect to the changing topologies presented in 5G such as heterogeneous networks, device-to-device communications, massive multiple-input multiple-output, SDNs, and Internet of Things. 5G networks provides game-changing innovations for the core enabling technologies, namely the network softwarization [27] specifically to be used for SBA, and 5G new radio [28] for much higher data rate and larger number of devices with a very low latency. Foukas *et al.* [17] studied those technologies in terms of the security perspective together with the 5G privacy concerns, among others. Additionally, they also discuss security monitoring and management of 5G networks.

2) RESULTS ON 5G SIGNALING SECURITY

As in previous generations, the security of the signalling systems is a challenging problem for 5G Core network management. In 2018, Hu *et al.* [18] investigated the security vulnerabilities with respect to 5G signalling, namely HTTP/2.0 protocol. They summarized several attacks that originate from the HTTP/2.0 protocol. In a similar direction, Positive Technologies [19] published a report, which identifies several security vulnerabilities against the Packet Forwarding Control Protocol (PFCP) and HTTP/2.0 protocols. Regarding PFCP, the following attack scenarios are proposed:

- The first attack scenario consists of sending a *Session Deletion Request* packet to the User Plane Function (UPF). The request contains only the subscriber session identifier. As a result, packet data transmission to the

victim's device will stop, but the connection to the network will remain.
- In the second scenario, packet handling settings are tampered with. Attackers need to send a *Session Modification Request* containing a DROP flag in the *Apply Action* field in the forwarding action rules. If the rules are changed successfully, those containing the TEID and IP address of the base station are deleted on the UPF. As a result, the GTP tunnel for the subscriber's downlink data is cut off, depriving the subscriber of Internet access.
- By using a *Session Modification Request*, attackers can redirect user traffic from the UPF to an attacker-controlled resource. For this, the attackers need to change the IP address in the *Outer Header Creation* field. As a result, they can access the downlink data of the subscriber, who will not be aware that the traffic is being intercepted.

With respect to the HTTP/2.0 protocol, Positive Technologies' report identified several issues surrounding the Network Repository Function (NRF): subscriber authentication vulnerabilities, subscriber profile disclosure via 5G's Unified Data Management (UDM) function, creating Protocol Data Unit (PDU) session creation by impersonating 5G's Access and Mobility Management Function (AMF). In the same time period, Positive Technologies [20] published another report based on their analysis of GPRS Tunnelling Protocol (GTP) protocols. According to the results listed in the report, the design flaw of the GTP protocol can cause serious vulnerabilities since there is no verification for the actual location of users, and hence, the home network cannot differentiate whether the ''location set'' signal coming from a subscriber in a guest network is legitimate or not. Therefore, attackers benefit from this vulnerability to deploy various attacks such as the Denial of Service (DoS) attacks against operator equipment, financial fraud, impersonation attacks, remote attacks against GPRS exchange. These threats apply to the NSA scenario of 5G and may also affect the standalone 5G as GTP is used there as well.

3) RESULTS ON 5G AUTHENTICATION PROCEDURES

In 2019, Shaik *et al.* [21] published a report, which observes that device capabilities are exchanged with the network before the authentication stage without any protection and not verified by the network. Consequently, the device capability information can be misused by an adversary to perform the following attacks against the mobile subscriber.

- Identification attacks allow an adversary to discover devices on the mobile network and reveal their hardware and software characteristics (such as model, manufacturer, version) and applications running on them;
- Bidding down attacks that hijack the device capabilities exposed on the 4G Long Term Evolution (LTE) air-interface and degrade the data-rate of a device from 27 Mbps to 3.7 Mbps and further deny Voice Over LTE (VoLTE) services to LTE subscribers and downgrade them to 3G/2G networks;
- Battery draining attacks that target NB-IoT and LTE-M devices to breakdown their power saving abilities and drain their battery life 5 times faster than the expected lifetime.

In 2019, Borgaonkar *et al.* [22] published a paper, which identifies a logical vulnerability in the specifications of 5G Authentication and Key Agreement (5G-AKA) protocol, i.e. the protection mechanism of the Sequence Number (SQN) can be defeated under specific replay attacks due to its use of Exclusive-OR (XOR) and a lack of randomness. Based on the vulnerability, the paper proposed an attack against a subscriber's location privacy. Later, Michell [23] published a paper, which provides a detailed analysis of the impact of quantum computing on the security of 5G mobile telecommunications. This involves considering how cryptography is used in 5G, particularly the 5G-AKA protocol, and how the security of the system would be affected by quantum computing. Hussain *et al.* [24] published a paper, which exploits the paging protocols in 4G and 5G and demonstrates how to launch location tracking and DoS attacks.

4) RESULTS ON 5G NETWORK SLICING AND SDN USAGE

In 2020, Olimid and Nencioni [25] focused on the network slicing security issues in 5G, from the life-cycle, intra-slice and inter-slice aspects. In a similar vein, AdaptiveMobile Security [26] published a report which provides a general review on the slicing technologies in 5G networks. Particularly, it summarizes the existing security features and the authorization processes in 5G's service-based architecture (SBA) using the NRF and Service Communication Proxy (SCP). The report presents three threats associated with 5G Core network slicing security: (1) how to gain access to resources of another slice; (2) how to perform a DoS attack from one slice onto another slice; (3) how to extract user specific information like location from another slice. ENISA's report [7] surveys the security threats against SDN technologies, which are regarded as an enabling building block for 5G networks. From the report, an API exploitation threat involves exploiting the API of a software component in order to launch different types of further attacks such as the unauthorised disclosure, compromise of integrity and/or destruction of information, or the unauthorised destruction/degradation of service. In SDN, API exploitation may relate to all the different types of APIs that may be found in an SDN. These include: (a) the Northbound API (Northbound API exploitation) that facilitates the communication between SDN controllers and SDN applications; (b) the Southbound API that facilitates the communication between SDN network elements and SDN controllers (i.e., Southbound API exploitation), and (c) the Eastbound/Westbound API that facilitates the communication between SDN controllers (i.e., Eastbound/Westbound API exploitation).

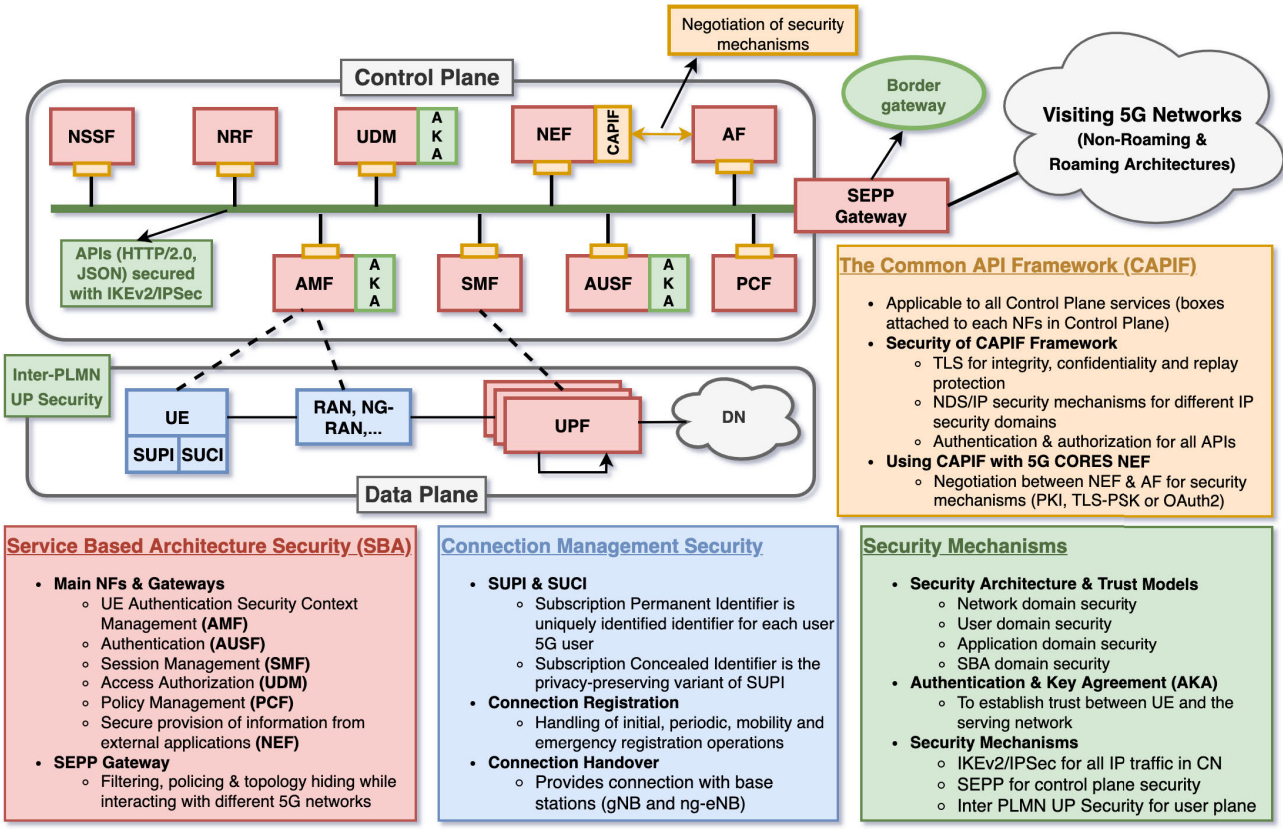


FIGURE 1. Overall view for the systematic analysis of the 5G core network security.

C. CONTRIBUTION AND ORGANISATION

5G is believed to be a key enabling infrastructure for the emerging digital transformation. Today, numerous use cases have been proposed and piloted in application areas such as smart city, smart mobility, smart manufacturing, autonomous driving, digital twin, remote surgery, and so on. Many people are very enthusiastic about the promises 5G can bring, while some others are very conservative towards the advertisements from industry. For the latter, one common question is whether 5G can power all the promised mission-critical applications in a secure manner. Even though security has been considered with a high priority in the 5G standards development and some research has been done as shown in previous subsections, it remains very hard to give a clear answer to the above question.

In this paper, we aim at providing a concise overview of the major security-related features in 5G networks based on information from several 3GPP technical specifications. The summary of the topics covered in the scope of this paper are as illustrated in Figure 1. Please note that color codes are applied for the components described in the figure, where red corresponds to the functionalities provided by SBA and the various Network Functions. Blue is used for representing the security of connection management, particularly the security features in User Equipment (UE) and its handover procedures in connection with 5G Radio Access Network (NG-RAN). Green corresponds to the new security mechanisms (e.g. the 5G AKA protocol) in both the data plane and the control plane (we also cover roaming and non-roaming scenarios in the related section). Finally, orange is used for explaining the security of the newly introduced common API framework (CAPIF), which facilitates applications to interact with NFs in 5G Core network. In more detail, our contribution is organised as follows in the rest of this paper.

In Section II, we first recap some important 4G features such as the Control and User Plane Separation (CUPS) and show how they have inspired 5G SBA. We then review some key NFs in the SBA and the gateways such as SEPP which is a bridge between different networks in roaming scenarios, followed by a brief review of the protocol stack in NG-RAN. We finally describe some security implications of the SBA. In Section III, we review three aspects in 5G connectivity management, including SUPI protection for UE, different registration processes, and the handover procedures in 5G systems and give an overview of the paging and handover procedures. We conclude with a summary of literature research on recovering SUPI and point out some other potential security issues. In Section IV, we recap the security architecture and trust models defined by 3GPP in both roaming and non-roaming scenarios and review the 5G AKA protocol and key derivation hierarchy. We also briefly describe the security mechanisms provided in 3GPP

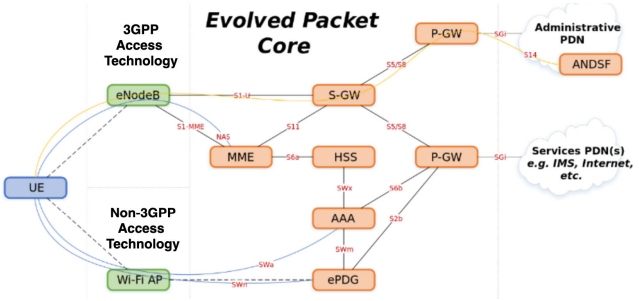


FIGURE 2. 4G EPC core (credit: Joe Deu-Ngoc).

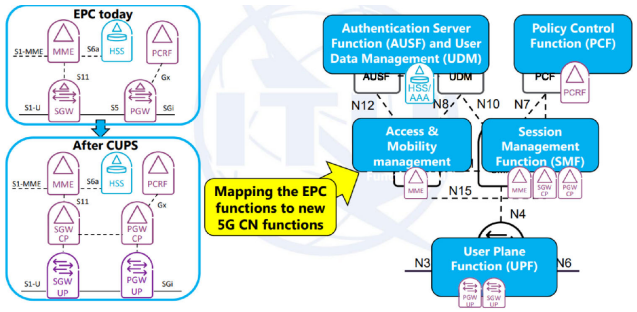


FIGURE 3. 4G CUPS (credit: ITU).

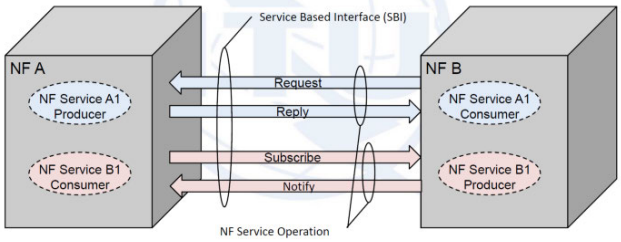


FIGURE 4. Communication between NFs (credit: ITU).

specifications and end with a summary of existing research results on 5G Core network security. In Section V, we provide an overview for the Common API Framework (CAPIF) for 3GPP northbound APIs and the relevant security mechanisms provisioned in the specifications. In Section VI, we discuss the defence strategies for 5G networks and outline some future research directions.

In addition, we list all the acronyms used throughout this paper and their definitions at the end of the paper for reference and help understand, especially, the names of various components in the 5G architecture.

II. SERVICE BASED ARCHITECTURE OF 5G CORE

The 5G Core network employs a Service Based Architecture (SBA), which divides the necessary functionalities into different network functions and provides a standard communication infrastructure based on API calls (referred to as Service Based Interface (SBI)). The SBA may make 5G Core look very different from the previous generations, but this design can be argued as an extension of the 4G LTE which is a standard developed by the 3GPP and is specified in its Release 8 document series. Particularly, the inspiration for the SBA can be found in Evolved Packet Core (EPC) shown in Figure 2, a key part of the System Architecture Evolution (SAE) network architecture designed to simplify LTE networks and establish a flat, all-IP architecture with separation of control plane and user plane traffic.

As shown in the figure, EPC has the following main components. The Mobility Management Entity (MME) is the key control node for the LTE access network. The Serving Gateway (S-GW) routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB (i.e. LTE base station) handovers and as the anchor for mobility between LTE and other 3GPP technologies. The Packet Data Network Gateway (P-GW) provides connectivity from the User Equipment (UE) to external packet data networks (PDNs) by acting as the point of exit and entry of traffic. The Home Subscriber Server (HSS) is a central database that contains user-related and subscription-related information. The Authentication Authorization Accounting (AAA) server provides access, control and security for the networks by supporting a set of protocols that mediate and track user access by authenticating, authorizing and accounting for mobile user activities.

In between 4G and 5G, one milestone is the Control and User Plane Separation (CUPS), which is shown in Figure 3 and formally appears in Release 14 specification of 3GPP. CUPS provides the architecture enhancements for the separation of functionality in the EPC's S-GW, P-GW and Traffic Detection Function (TDF). For example, the S-GW and P-GW functions were split into a control and a data plane components, namely S-GW is separated into S-GW-C and S-GW-U while P-GW is separated into P-GW-C and P-GW-U. The motivation for CUPS has been catering to the rapidly-increasing growth of traffic from smart devices, the proliferation of video and other applications that they support, and the use of USB modem dongles and personal hot-spots. In more detail, CUPS aims at meeting the critical Key Performance Indicators (KPIs) from the consumer side, including: reducing latency on application service, supporting the increase of data traffic, locating and scaling the control plane and user plane resources of the EPC nodes independently, independent evolution of the control plane and user plane functions, enabling SDNs to deliver user plane data more efficiently.

Due to this, 5G's SBA can be regarded as an evolution from CUPS, yet with a complete grouping (and redesigning) of 4G functionalities and mapping them into service-oriented NFs. As a result, the mobile operators that already had SDN/NFV in place in 4G can benefit from better network quality, easier load distribution, scalability and so on. It is worth emphasizing that service-based architectures have been widely used in the software industry as the key concept to improve the product modularity. With SBA, the communication between any two NFs is through standard

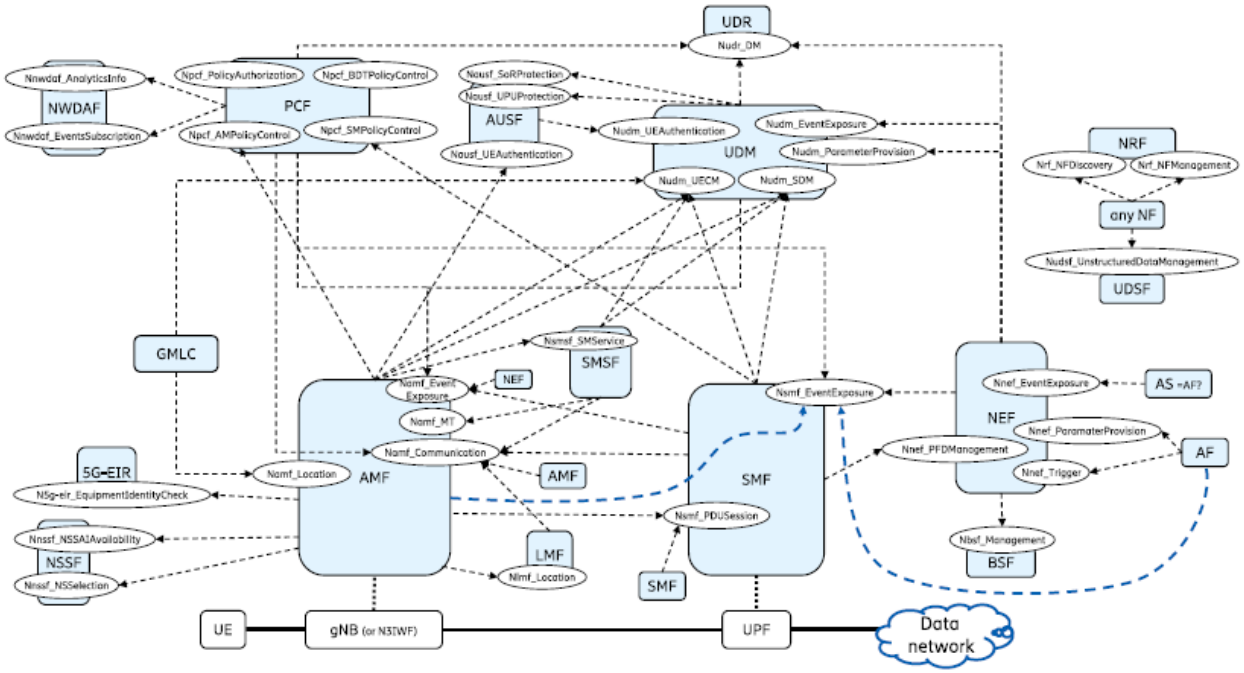


FIGURE 5. 5G NFs (credit: Rommer *et al.* [29]).

Internet protocols, e.g. TCP/IP and HTTP/2.0. The NF communication can follow either a Request-Reply model or a Subscribe-Notify model like many existing web services, as demonstrated in Figure 4. As a benefit of adopting these Internet protocols, 5G can seamlessly integrate other mature protocols, such as JSON as the application layer serialization protocol, OAuth2.0 as the authorisation protocol for NF access control, and TLS as the network layer security protection.

A. MAIN NFS AND GATEWAYS IN 5G SBA

Figure 5 highlights the interactions between main NFs in the non-roaming scenario.

The Access and Mobility Management Function (AMF) and the Session Management Function (SMF) take the main responsibility of the control plane. They, with the help from the Authentication Server Function (AUSF), covers most of the functions of MME in 4G.

- The AMF maintains a non-access stratum (NAS) signalling connection with the UE and manages the UE registration procedure, and furthermore it is responsible for mobility management including applying mobility related policies from Policy Control Function (PCF) (e.g. mobility restrictions). In particular, the AMF is responsible for authenticating UEs and managing the security contexts. The UE authentication operation is facilitated by the AUSF to obtain authentication vectors from the Unified Data Management (UDM). Overall, the AUSF facilitates subscriber authentication, during registration or re-registration within 5G. In addition, the AUSF provides security parameters to protect steering of roaming information and also provides security parameters to protect information in the UE update procedure. The AMF also acts as a proxy to relay messages between UE and other NFs. It relays session management signalling messages between UE and the SMF, relays SMS messages between UE and the Short Message Service Function (SMSF) which supports the transfer of SMS over NAS, and relays location service messages between UE and the Location Management Function (LMF) which manages the resources and timing of positioning activities.
- The SMF provides the session management functionality of the 4G MME and additionally combines some control plane functions of the S-GW-C and P-GW-C. It allocates IP addresses to the UE, handles NAS signalling for session management, sends QoS and policy information to radio access network (RAN) via the AMF, selects and controls the User Plane Function (UPF) for traffic routing. The SMF interacts with the PCF to retrieve policy data to configure the UPF for UE's PDU sessions. The UPF selection function enables Mobile Edge Computing (MEC) by selecting a UPF close to the edge of the network. The SMF acts as the interface for all communication related to offered user plane services and determines how the policy and charging for these services is applied. And, it deals with the lawful intercept from the control plane. Note that the SMF indirectly communicates with UE via AMF.

In the user plane, the UPF combines the user traffic transport functions previously performed by the S-GW and

P-GW in the 4G EPC. It anchors the UE IP addresses, and handles packet routing and forwarding. When a UE is in idle mode, downlink traffic is buffered at the UPF; the UPF signals the SMF which then signals to the AMF to start the paging procedure. The UPF may optionally integrate a Deep Packet Inspection (DPI) for packet inspection and classification, and it may optionally integrate the Firewall and Network Address Translation (NAT) functions. Moreover, the UPF serves as the mobility anchor for Intra Radio Access Technology (RAT) and Inter-RAT handovers and maintains and reports traffic statistics. Finally, it deals with Lawful intercept from user plane.

The UDM manages data for access authorization, user registration, and data network profiles. It interfaces with NFs such as AMF, AUSF and SMF so that relevant data becomes available to them. Particularly, the Authentication credential Repository and Processing Function (ARPF) is a functional element of the UDM and responsible for generating 5G Home Environment Authentication Vectors, and the Subscriber Identity De-concealing Function (SIDF) is a functional element of the UDM and responsible for decrypting a Subscription Concealed Identifier (SUCI) to reveal the subscriber's Subscription Permanent Identifier (SUPI). A stateful UDM keeps data on hand locally, while a stateless version stores data externally in the Unified Data Repository (UDR) which stores structured data such as subscriber information, application-specific data, and policy data. Overall, the UDM plays a similar role to that of HSS in 4G. In contrast, the Unstructured Data Storage Function (UDSF) supports data storage for stateless NFs.

The PCF plays a similar role as the Policy and Charging Rules Function (PCRF) in 4G, while leaving the charging service to a dedicated Charging Function (CHF). The PCF provides policy rules for control plane functions, including network slicing, roaming and mobility management. It governs the network behaviour by supporting a unified policy framework and supports the new 5G QoS policy. For example, the AMF interfaces with the PCF for retrieval of access and mobility policies and the PCF retrieves subscription information for policy decisions taken by the UDR. The PCF maintains its traditional diameter protocol-based interface to an Application Function (AF) but also enhanced it to allow for resource reservation requests using an HTTP/XML-based interface from other services. Note that trusted AFs from the perspective of the network can interact directly with the NFs, while other AFs need to rely on the Network Exposure Function (NEF)'s exposure mechanisms to carry out the communications.

The Network Repository Function (NRF) provides NF service registration and maintains NF profiles and available NF instances. It serves as a repository of the services so that it allows every NF (i.e. service consumer) to discover the services offered by other NFs (i.e. service provider). The NF profile in the NRF contains detailed information like NF type, address, capacity, supported NF services and the address of service instances. Security related, the NRF takes the role of the authorization server for the registered NFs. The Network Slicing Selection Function (NSSF) assists the AMF with the selection of the Network Slice instances that can serve a UE and it will determine the allowed Network Slice Selection Assistance Information (NSSAI) that is supplied to the device. Moreover, the NSSF may help allocate an appropriate AMF if the current AMF is not able to support all network slice instances for a given UE. The NSSF and the PCF can consume the services from the Network Data Analytics Function (NWDAF) which collects data, performs analytics and offers the data and analytical results as a service to other NFs.

The Network Exposure Function (NEF) provides a mechanism for securely exposing services and features within and outside of the 5G Core. It guarantees secure provision of information from external application to 3GPP network and translation of internal/external information. The NEF allows the NF consumer(s) to (un)subscribe to notifications of monitoring observed event and sends the notification to the NF consumer(s) when a subscribed event is detected. The NEF northbound interface (i.e. N33) is between the NEF and an AF. It specifies RESTful APIs that allow the AF to access the services and capabilities provided by 3GPP network entities and securely exposed by the NEF. To this end, NEF can also support the common API framework (CAPIF) which is summarized in Section 5. In addition to these NFs, we would like to introduce the following gateways.

- The Non-3GPP access Inter-Working Function (N3IWF) is similar to the Evolved Packet Data Gateway (ePDG) in the 4G EPC, which is a secure gateway for the UE to access non-trusted networks, such as Wi-Fi and the public Internet. One important enhancement is the transport of NAS messages from the UE over non-trusted networks and AMF selection. A 5G UE can perform a network registration from networks other than the 5G NG-RAN and when connected on, for example, 5G NG-RAN and Wi-Fi will have two, distinct active NAS connections with the AMF.
- The Service Communication Proxy (SCP) is deployed along side of NFs for providing routing control, resiliency, and observability to the core network. In the 3GPP TS 33.501 document, it is stated that for security reasons, NFs, e.g. an NF consumer and an NF producer, should indirectly communicate with each other through a SCP, instead of directly communicating with each other.

Note that we will not be able to enumerate all the NFs in this document. We recommend the readers to the 3GPP specifications (e.g. TS 23.501) for more information.

B. SEPP GATEWAY IN 5G ROAMING SCENARIOS

Figure 6 depicts the 5G System roaming architecture with local breakout and service-based interfaces within the Control Plane. It is worth emphasizing that the communication between VPLMN (Visited Public Land Mobile Network) and HPLMN (Home Public Land Mobile Network) may

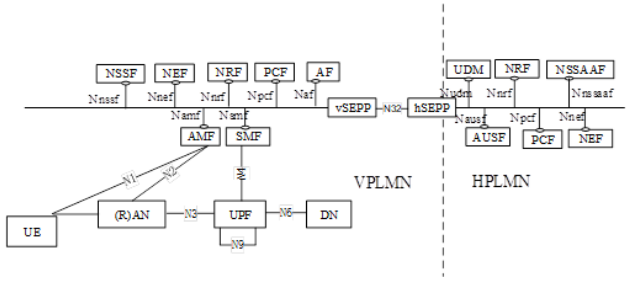


FIGURE 6. Non-roaming reference architecture (credit: 3GPP).

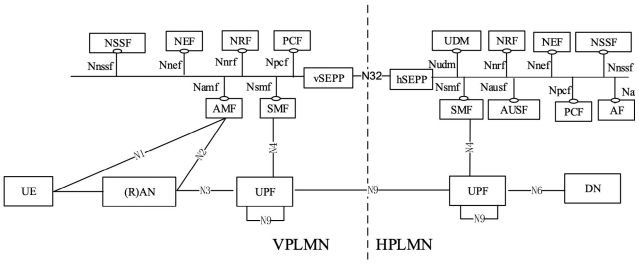


FIGURE 7. Roaming reference architecture (credit: 3GPP).

traverse over one or many Internetwork Packet Exchanges (IPXs). For simplicity, such IPXs have been omitted in the figure. And, the following figure depicts the 5G System roaming architecture in the case of home routed scenario with service-based interfaces within the Control Plane. And, Figure 7 depicts the 5G System roaming architecture in the case of home routed scenario with service-based interfaces within the Control Plane. To ensure interconnect security, the Security Edge Protection Proxy (SEPP) is introduced as an entity that resides at the perimeter of each PLMN. It is used to protect control plane traffic that is exchanged between different 5G PLMNs, by performing message filtering, policing and topology hiding for all API messages. It ensures end-to-end confidentiality and/or integrity between source and destination networks for all 5G interconnect roaming messages, e.g. through the PRINS protocol. More details are given in Section IV.

C. 5G NG-RAN ARCHITECTURE

Defined in 3GPP TS 38.300, the NG-RAN architecture is illustrated in Figure 8. An NG-RAN node is either:

- a gNB, providing New Radio (NR) user plane and control plane protocol terminations towards the UE; or
- an ng-eNB, providing Evolved Universal Terrestrial Radio Access (E-UTRA) user plane and control plane protocol terminations towards the UE.

The gNBs and ng-eNBs can be interconnected with each other by means of the Xn interface. The Xn control plane interface (Xn-C) supports the following functions: Xn interface management and UE mobility management including context transfer and RAN paging; Dual connectivity. The gNBs and ng-eNBs are also connected by means of the Next Generation (NG) interfaces to the 5G Core, more specifically to the AMF by means of the NG-C interface and to the UPF

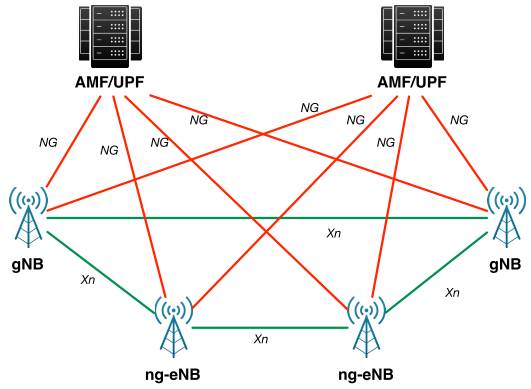


FIGURE 8. RAN architecture.

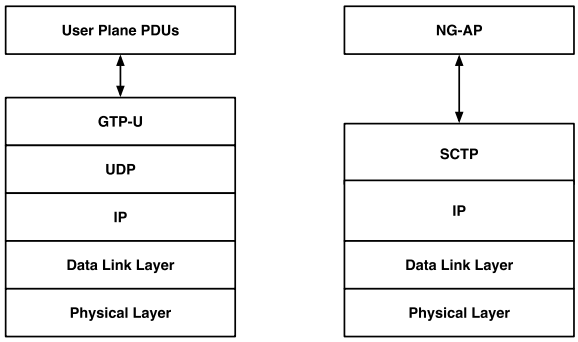


FIGURE 9. RAN protocol stack.

by means of the NG-U interface (see 3GPP TS 23.501 for more details).

The NG-U and Xn-U interfaces adopt the same protocol stack, shown in the figure below. The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs. The NG-C and Xn-C interfaces adopt the same protocol stack, shown in Figure 9. The transport network layer is built on IP transport. For the reliable transport of signalling messages, SCTP is added on top of IP, to provide guaranteed delivery of application layer messages and meet the scalability requirements. For NG-C, the application layer signalling protocol is referred to as NG-AP (NG Application Protocol); and for Xn-C, the application layer signalling protocol is referred to as Xn-AP (Xn Application Protocol).

D. SUMMARY

Compared with 4G, there are many more NFs in 5G. Most NFs are further made of multiple microservices for the purpose of upscaling and downscaling of services. Moreover, the 5G Core services and features have been made available to outside applications through the NEF, e.g. through the CAPIF framework as described in Section V. To support the flexibility of SBA deployment, it is expected that SDN and NFV technologies will be heavily used to instantiate these NFs. Moreover, orchestration platforms such as Kubernetes [30] will be used to cope with the deployment challenges in 5G, by automating NF deployment, scaling,

and management. These new softwarization technologies inevitably bring a wide range of vulnerabilities into the 5G networks, particularly the Core network. Such vulnerabilities include bugs in the software, programming vulnerabilities such as buffer overflow, side channel information leakage in virtualized network functions, implementation vulnerabilities such as imperfect/wrong implementation of authentication, and so on. For instance, as mentioned in Section I-B, ENISA has provided a long list of security vulnerabilities in SDN [7]. Køien has also pointed out that vulnerabilities in software implementation could pose serious threat to 5G networks [15].

In a long period of time, the Telecom industry has employed a ''security by obscurity'' approach. For the early generations such as 2G and 3G (especially earlier stages such as 2.5G), it has worked well due to two facts: understanding the working of the systems and mastering the attack skills are an obstacle, and incentives are relatively low as the networks mainly carry voice and SMS data. However, things have changed dramatically since 4G which start to use IP-based architecture and carry richer set of data services. In the past few years, we began to see that more and more cyberattacks (e.g. denial of service attacks) have been reported against the 4G networks. From previous subsection, we know that the communications in both the 5G Core and the RAN are all through IP networks. One could argue that employing the well-known and widely-tested IP-based Internet protocols could reduce the security risks for 5G since proprietary protocols are notoriously vulnerable to security threats. Unfortunately, this is partly true, because it also implies that an attacker can launch zero-day attacks once a vulnerability has been found in IP-based protocols or their implementations. One such protocol is TLS which is the most important one to secure the 5G networks and has been reported with a large number of security issues [31], e.g. the Heartbleed vulnerability [32] in the open-sourced implementation OpenSSL [33]. Suppose that an attacker has exploited this vulnerability and compromised the AMF, UDM or NEF, it will be catastrophic to the 5G Core network.

Overall, the SBA architecture brings both opportunities and security vulnerabilities to the 5G networks and the applications on top. Nevertheless, the concrete security risks are determined by the specific construction of a 5G network and the building blocks for this construction (e.g. how SDN is used), as well as practical situations including the configurations and deployed security countermeasures.

III. 5G CONNECTION MANAGEMENT

The Connection Management is used to establish and release the Control Plane signalling connection between the UE and the AMF. The Registration Management is used to register or deregister a UE with the 5G system and establish the user context. The Mobility Management functions are used to keep track of the current location of a UE. The detailed procedures for Connection, Registration and Mobility Management functionality appear in 3GPP TS 23.502.

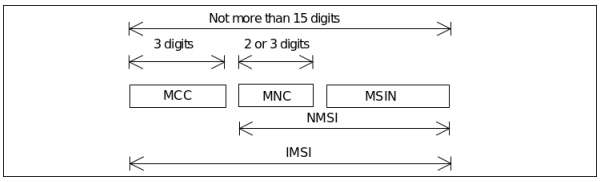


FIGURE 10. 5G IMSI format (credit: 3GPP).

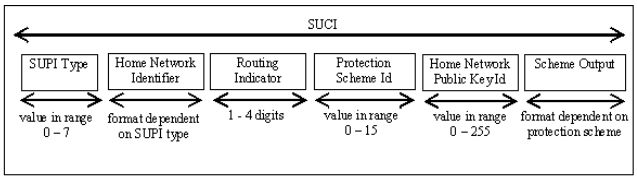


FIGURE 11. 5G SUCI format (credit: 3GPP).

A. SUPI AND SUCI

In GSM/UMTS/EPS systems (i.e. 2/3/4G), a unique International Mobile Subscription Identity (IMSI) is allocated to each mobile subscriber. Meanwhile, for privacy protection, the Visitor Location Register (VLR), Serving GPRS Support Node (SGSN) and MME may allocate Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers. As shown in Figure 10, an IMSI is formed with three elements. Mobile Country Code (MCC) consists of three digits, uniquely identifying the country of domicile of the mobile subscription. Mobile Network Code (MNC) consists of two or three digits, uniquely identifying the home PLMN of the mobile subscription within its country of domicile, or it identifies together with MCC and Network Identifier (NID) the mobile subscription's Stand-alone Non-Public Network (SNPN). Mobile Subscriber Identification Number (MSIN) identifies the mobile subscription within a PLMN or SNPN.

In 5G, a globally unique Subscription Permanent Identifier (SUPI) is allocated to each subscriber in the system and provisioned in the UDM/UDR. It is defined in 3GPP specifications TS 23.003 and TS 23.501, and it has several types: an IMSI, a network specific identifier, a Global Line Identifier (GLI), or a Global Cable Identifier (GCI). The SUPI is used only inside 3GPP system, and plain-text transmissions of the SUPI over the radio interface is not allowed for both protecting privacy and combating fraud. In many occasions, the Subscription Concealed Identifier (SUCI), a privacy-preserving version of SUPI, will be used. The UE generates a SUCI using an Elliptic Curve Integrated Encryption Scheme (ECIES) -based protection scheme with the public key of the Home Network (HN) that is securely provisioned to the USIM during the USIM registration. The format of SUCI is shown in Figure 11.

If the SUPI type value is 0, then it stands for IMSI. In this case, Home Network Identifier is composed of MCC and MNC. The Routing Indicator consist of 1 to 4 decimal digits assigned by the home network operator

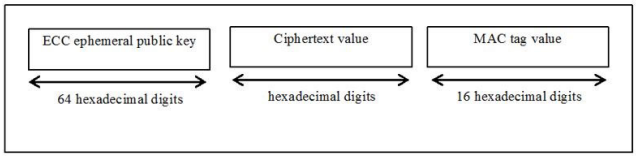


FIGURE 12. 5G ECIES output format (credit: 3GPP).

and provisioned within the USIM. The Protection Scheme Identifier, consisting in a value in the range of 0 to 15, indicating a null scheme, or a non-null scheme specified in Annex C of 3GPP TS 33.501, or a protection scheme specified by the home PLMN. Home Network Public Key Identifier, consisting in a value in the range 0 to 255. It represents a public key provisioned by the home PLMN or SNPN and it is used to identify the key used for SUPI protection. The Scheme Output consists of a string of characters with a variable length or hexadecimal digits, dependent on the used protection scheme. For example, the protection scheme of ECIES Profile A leads to the the Scheme Output shown in Figure 12.

When IMSI is used as the SUPI, its first two elements (i.e. MCC and MNC) are transmitted in plain-text format and only the MSIN element is concealed by the protection. The concealing and de-concealing are graphically summarized in Figure 13.

B. 5G CONNECTION REGISTRATION

Registration is the first procedure the UE executes after being switched on. The procedure is performed to make it possible to receive services from the network. But the Registration procedure is also performed during the time the UE is connected to the network. There are several types of the Registration procedure:

- Initial Registration: used by the UE to connect to the network after power-on.
- Periodic Registration: used by the UE that is in CM-IDLE state to show to the network that the UE is still there. The periodicity is based on a time value received from the AMF.
- Mobility Registration: used by the UE in case it moves out of the *Registration Area*, or when the UE needs to update its capabilities or other parameters that are negotiated in Registration procedure with or without changing to a new *Tracking Area*.
- Emergency Registration: used by the UE when it wants to register for emergency services only.

In EPS, the first case was supported using the *Initial Attach* procedure while the second and third cases were supported using *Tracking Area Update* procedure. In 5G however, the three cases are supported using the Registration procedure. One benefit with that approach is that a mobility registration can be handled as an initial registration, with full authentication. The full procedure for UE registration is described in the clause 4.2.2 of 3GPP TS 23.502. In a nutshell, it performs as in Figure 14.

When a UE tries to register for the first time (i.e. initial registration), UE encrypts SUPI into SUCI and sends an Initial Registration Request with SUCI to a selected AMF, which further forwards this SUCI to AUSF and UDM. Then, mutual authentication between UE and its home network (represented by the UDM), e.g. via the 5G-AKA mentioned in Section IV. Note that the mutual authentication for AMF is done via the co-located SEAF. If the authentication is successful, the AMF obtains the corresponding SUPI and other key materials resulted from the AKA. Finally, the AMF generates a Global Unique Temporary Identifier (GUTI) for this SUPI and keeps the GUTI to SUPI mapping for further registrations or PDU session requests. The purpose of the 5G-GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the 5G System. It also allows the identification of the AMF/network and can be used by the network and the UE to establish the UE's identity during signalling between them. Particularly, 5G-GUTI can be used to identify the UE in other types of registrations, such as those due to mobility. In short, GUTI is 80 bits long core network identifier, shown in Figure 15.

It is also worth mentioning that 5G-S-TMSI is a shortened version of the 5G-GUTI, comprising of the AMF Set ID, AMF Pointer and 5G-TMSI. It is used in 5G paging process. When a device does not have any ongoing data transmissions, it enters an IDLE state in order to preserve battery. If new data arrives for the device, the network probes the IDLE device by sending a so-called "paging" message and the device correspondingly responds.

C. 5G CONNECTION HANDOVER

In the inter-5G setting, handover in 5G happens when a UE moves from the premise of a source NG-RAN to a target NG-RAN. Note that there is also the case that handover can happen in other scenarios, e.g. between NG-RAN and eNB. We skip these scenarios here. There are two types of inter-5G handovers.

- Xn-handover: The Xn-based inter NG-RAN handover is used to hand over a UE from a source NG-RAN to target NG-RAN using the Xn interface. In this type of handover, the AMF is unchanged. The source NG-RAN includes the UE 5G security capabilities in the handover request message containing the current ciphering and integrity algorithms, and the target NG-RAN selects the algorithm according to its local configuration. The chosen algorithms are indicated to the UE in the Handover Command message if the target NG-RAN selects different algorithms. If the UE does not receive any information, it should continue to use the current algorithms. In the handover, the target NG-RAN sends the UE's 5G security capabilities received from the source NG-RAN to the AMF. The AMF will verify that the UE's 5G security capabilities received from the target NG-RAN are the same as the UE's 5G security capabilities in its local storage. If there is a mismatch, the

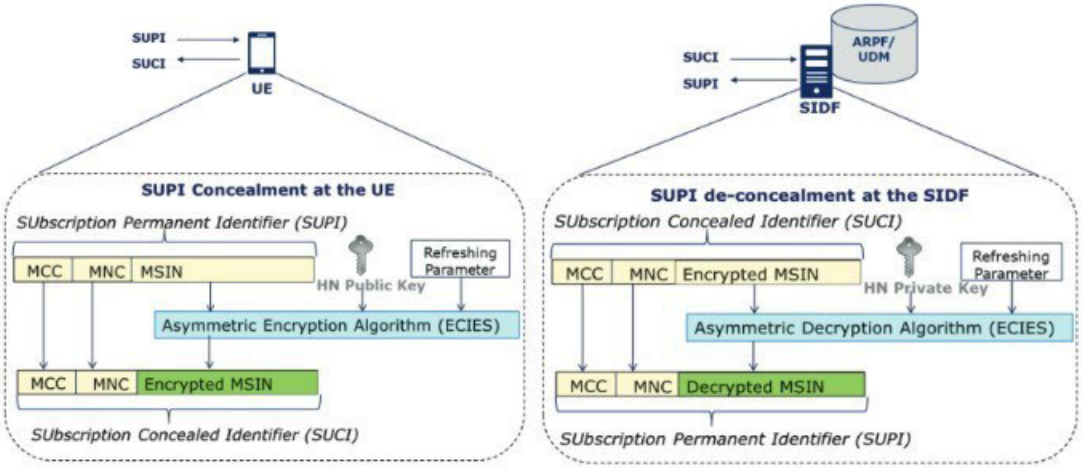


FIGURE 13. From SUPI to SUCI (credit: prasad *et al.* [34]).

AMF will send its locally stored 5G security capabilities of the UE to the target NG-RAN. In addition, the AMF may log the event and may take necessary following-up steps. During the handover, the AMF will interact with the SMF to check whether the existing UPF should be changed for the UE.

- N2-handover: In this case, the handover is through the N2 interface between NG-RAN and AMF. Similar to Xn handover, the source NG-RAN and the target NG-RAN negotiate the handover of a UE, with all messages routed through the AMF(s). Note that in the handover, the network's policy may determine the current AMF must be changed so that a target AMF should be selected. Then, UE and the involved NG-RAN exchange session values and possibly lead to a re-keying of K_{AMF} (see details in Section IV-B).

D. SUMMARY

In contrast to 4G, the subscriber identifier such as SUPI will not be transmitted in plaintext outside the 5G Core network. This has greatly reduced the threats from IMSI-catchers. The new registration and handover procedures gives the 5G Core network (via AMF) finer control for managing the mobility of UEs. Moreover, it gives more home control to protect UEs in the roaming scenarios from spoofed visited networks. Note that, in 3G and 4G, a fake visited network can send forged signalling messages to the home network to obtain a UE's IMSI and location. To counter such threats, operators need to deploy rule-based or machine learning based fraud detection solutions in practice. These types of attacks become much more difficult in 5G.

Hussain *et al.* [24] demonstrated how to exploit the paging protocols 5G and to recover a victim UE's SUPI (i.e. IMSI). The proposed attack relies on several assumptions. One is that the attacker needs to know some soft identity of the UE, e.g. the phone number. Another is that the attacker can physically track the user to obtain some paging frame index (PFE) data via their ToRPEDO attack. Yet another assumption is that the attacker should know the ECIES public key of the victim's home network so that it can encrypt any guessed SUPI. In theory, the attack can work when all these assumptions hold. Note however the last assumption is questionable when the USIM in the UE is usually required to be tamper resistant.

From the description, we notice that the registration process is rather complex and involve many NFs. In addition, it requires cryptographic operations in the Core network, such as the UDM/ARPF. This may raise a concern of DoS attacks, particularly in use cases under the umbrella of Massive Machine Type Communications (mMTC). Similarly, DoS attacks could also be a concern for use cases under the umbrella of Ultra Reliable Low Latency Communications (URLLC), particularly when handovers need to be performed in the presence of active attackers. These are interesting areas of future investigation.

IV. TRUST MODEL AND SECURITY ARCHITECTURE AND MECHANISMS

The security related topics of 5G are mainly captured in the 3GPP TS 33.501 document. Before going into the security features, we first recap some security concepts which are widely used in 5G specifications.

The *security context* refers to the state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network. The "5G security context data" can include the 5G NAS security context, and the 5G AS security contexts for 3GPP access and non-3GPP access. The 5G NAS security context refers to the key K_{AMF} with the associated key set identifier, the UE security capabilities, the uplink and downlink NAS COUNT values. The AS security context for 3GPP access refers to the cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network

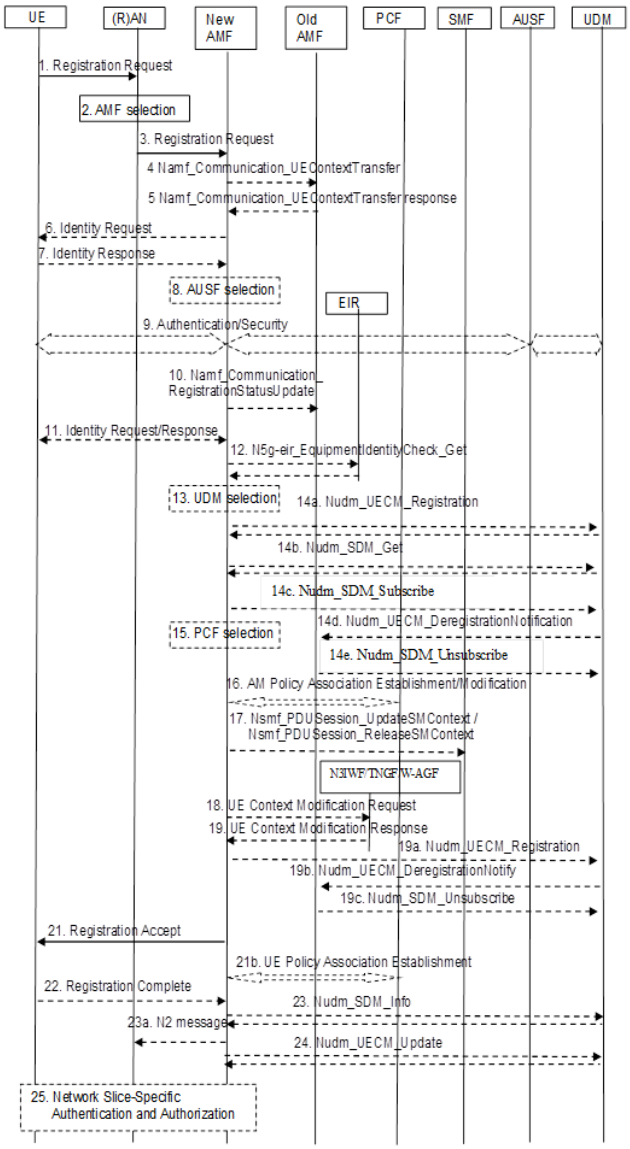


FIGURE 14. 5G registration (Credit: 3GPP).

side, UP security activation status and the counters used for replay protection. The AS security context for non-3GPP access refers to the key K_{N3IWF}, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec Security Association. The keys K_{AMF} and K_{N3IWF} are defined in Section IV-B. In 5G, the UE *5G security capability* means its security capabilities for 5G AS and 5G NAS, where security capabilities refer to the set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

A. SECURITY ARCHITECTURE AND TRUST MODELS

Figure 16 illustrates five security domains in 5G. The security features for these security domains are summarized in the following.

- (I) Network access security: This security domain includes a set of security features that enable a mobile equipment (ME) to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access. In particular, these features aim at preventing against attacks on the radio interfaces. In addition, there is one feature focusing on the security context delivery from serving network to access network for the access security.
- (II) Network domain security: This security domain includes a set of security features that enable network nodes to securely exchange signalling data and user plane data.
- (III) User domain security: This security domain includes a set of security features that secure the user access to ME.
- (IV) Application domain security: This security domain includes a set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.
- (V) SBA domain security: This security domain includes a set of security features that enables NFs of the SBA architecture to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces.

In fact, 5G also include a set of features on the visibility and configurability of security. These features enable the user to be informed whether a security feature is in operation or not. It is reflected by the fact that the AUSF provides security parameters to protect steering of roaming information and also provides security parameters to protect information in the UE update procedure.

In 5G terms, Mobile Equipment (ME) and the USIM together form the UE, where the Universal Subscriber Identity Module (USIM) is a trust anchor and resides in a tamper proof universal integrated circuit card (UICC). The USIM/UE stores at least the long-term key(s) and the subscription identifier SUPI. These values are used to uniquely identify a subscription and to mutually authenticate the UE and the home network. The trust model between USIM/UE and the home network in the non-roaming scenario is shown in Figure 17. On the home network end, ''trust'' is illustrated in multiple layers. In 5G, one particular feature is that the RAN can separated into Distributed Units (DU) and Central Units (CU), where DU and CU together form gNB (i.e. the 5G base-station). By design, the DU is not intended to have any access to customer communications because it is likely to be deployed in unsupervised sites. In contrast, the CU terminates the Access Stratum (AS) security and will be deployed in safeguarded sites. In 5G Core network, the AMF serves as termination point for Non-Access Stratum (NAS) security. According to the 3GPP TS 33.501, the AMF is collocated with the SEcurity Anchor

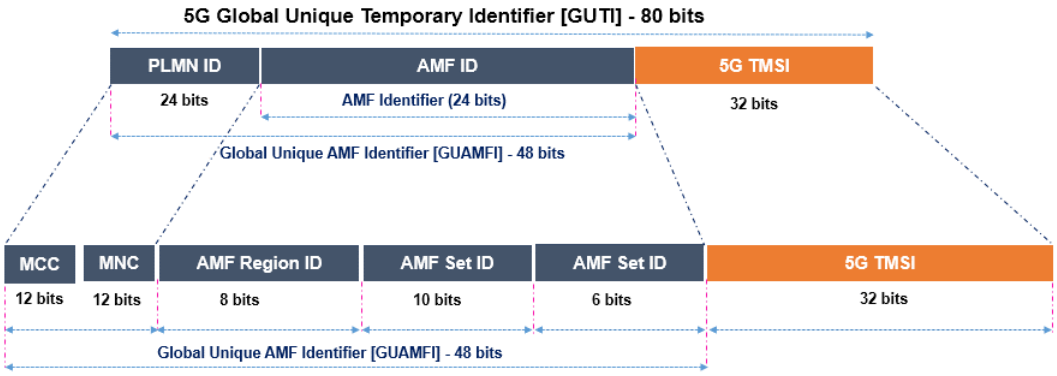


FIGURE 15. 5G GUTI format (credit: Techplayon).

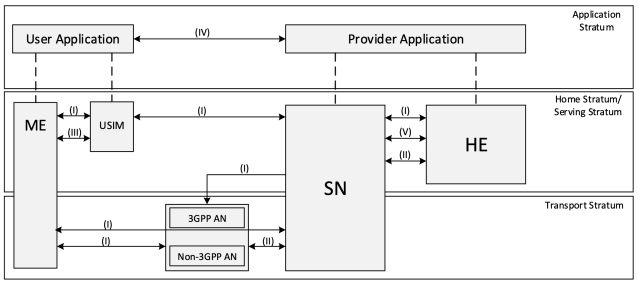


FIGURE 16. 5G security architecture (credit: 3GPP).

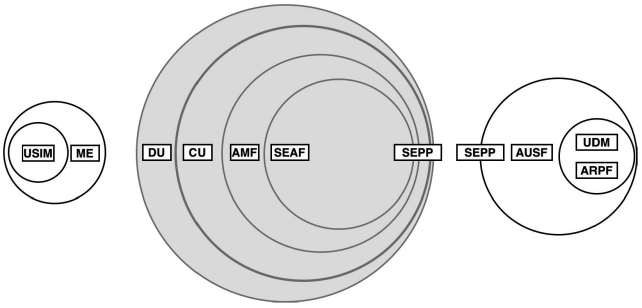


FIGURE 18. Trust model (roaming) (credit: 3GPP).

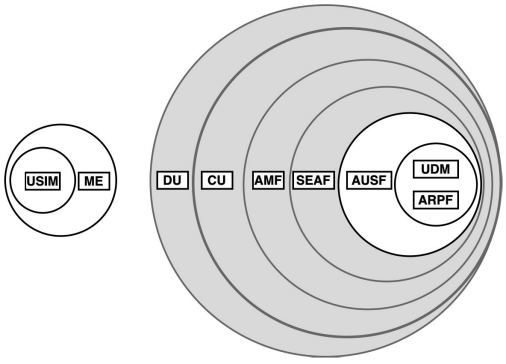


FIGURE 17. Trust model (non-roaming) (credit: 3GPP).

Function (SEAF) that holds the root key (known as anchor key) for the visited network in the roaming scenarios. Nevertheless, this security architecture is future proof, as it allows separation of AMF and SEAF in a future evolution if necessary.

In the roaming architecture, the home and the visited networks are connected through SEcurity Protection Proxy (SEPP). This new design makes 5G immune to a number of existing attacks, such as the key theft and rerouting attacks in SS7 and network node impersonation and source address spoofing in signalling messages in Diameter. The AUSF keeps a key for reuse, derived after authentication, in case of simultaneous registration of the UE in different access network technologies, i.e. 3GPP access networks and non-3GPP access networks such as IEEE 802.11 Wireless Local Area Network (WLAN). The trust model on network side is shown in Figures 18.

B. AUTHENTICATION AND KEY AGREEMENT IN 5G

Authentication and key agreement (AKA) mechanisms are used in 5G to establish the trust between UE and the serving network, which can be either the home network or a visited network. They are mandatory for a UE to access any mobile network. Such mechanisms are referred to as the primary AKA in the 5G specifications. In addition, secondary authentication mechanisms may be required when a UE tries to access an external data network (DN). In this following, we focus on the primary AKA only while the secondary AKA can be found in the 3GPP TS 33.501 document. The purpose of the primary AKA is to enable mutual authentication between the UE and the home network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. The primary AKA has the following two phases.

In Phase 1, as shown in Figure 19, the UE initiates the process and selects authentication method. The UE first sends a registration request (N1 message) to the SEAF that contains a concealed identifier SUCI or 5G-GUTI which is a temporary identity assigned by the network during a previous session. On receiving a registration request from the UE, the SEAF sends an authentication request message to the AUSF with the serving network (SN) name and either SUPI, if available and 5G-GUTI is valid, or SUCI. The SN name is a concatenation of service code and the Serving Network

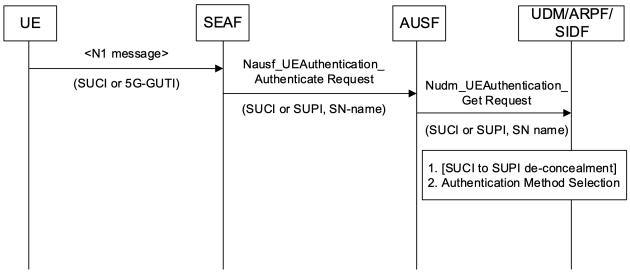


FIGURE 19. Phase 1 of authentication (credit: 3GPP).

Identity. Upon receiving the authentication request, the AUSF checks whether the requesting SEAF is authorized to use the SN name which is a form of home control in 5G. If the serving network is not authorized to use the SN name, the AUSF respond with ''serving network not authorized'' in the authentication response. The authentication information request from AUSF to UDM/ARPF/SIDF includes the SUCI or SUPI and the SN name. When necessary, SIDF is invoked to de-conceal the SUPI from SUCI, as shown in Figure 13. Based on SUPI and the subscription data, the UDM/ARPF choose the authentication method to be used.

In Phase 2, there are two options for the AKA protocol. In the following, we assume the new 5G-AKA protocol which is summarized in Figure 20. As a side note, if the UE is roaming in a visited network, then the SEAF is from this visited network but the AUSF and UDM/ARPF are still from UE's home network. We briefly summarize the authentication procedure below while the details can be found in the 3GPP TS 33.501 document.

1) For each *Nudm_Authenticate_Get* Request, the UDM/ARPF shall create a 5G Home Environment Authentication Vector (HE AV), which consists of the value tuple $(RAND, AUTN, XRES^*, K_{AUSF})$.
2) The UDM shall then return the generated 5G HE AV to the AUSF and indicate that it is to be used for 5G AKA in a *Nudm_UEAuthentication_Get* Response. If a SUCI has been included in the *Nudm_UEAuthentication_Get* Request, the UDM will include the SUPI in the *Nudm_UEAuthentication_Get* Response after de-concealment of SUCI by SIDF.
3) The AUSF shall store the $XRES^*$ temporarily together with the received SUCI or SUPI.
4) The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the $HXRES^*$ from $XRES^*$ and K_{SEAF} from K_{AUSF}, and replacing the $XRES^*$ with the $HXRES^*$ and K_{AUSF} with K_{SEAF} in the 5G HE AV.
5) The AUSF shall then remove the K_{SEAF} and return the 5G SE AV, i.e. $(RAND, AUTN, HXRES^*)$, to the SEAF in a *Nausf _UEAuthentication_Authenticate* Response.
6) The SEAF shall send $(RAND, AUTN)$ to the UE in a NAS message Authentication Request. This message shall also include the key set identifier ngKSI that will be used by the UE and AMF to identify the K_{AMF} and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The ME shall forward the *RAND* and *AUTN* received in NAS message Authentication Request to the USIM.
7) After receiving the *RAND* and *AUTN*, the USIM shall verify the freshness of the received values by checking whether *AUTN* can be accepted as described in the 3GPP TS 33.102 specification. If so, the USIM computes a response *RES*. The USIM shall return (RES, CK, IK) to the ME. The ME then shall compute RES^* from *RES* and K_{AUSF} from $CK||IK$. Then, the ME shall calculate K_{SEAF} from K_{AUSF}.
8) The UE shall return RES^* to the SEAF in a NAS message Authentication Response.
9) The SEAF shall then compute $HRES^*$ from RES^*, and then compare $HRES^*$ and $HXRES^*$. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in the specifications. If the UE is not reached, and the RES^* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.
10) The SEAF shall send RES^* in a request message named *Nausf _UEAuthentication_Authenticate* to the AUSF.
11) When the AUSF receives RES^* from the SEAF, it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF shall store the K_{AUSF}. The AUSF shall compare the received RES^* with the stored $XRES^*$. If the RES^* and $XRES^*$ are equal, the AUSF shall consider the authentication as successful from the home network point of view. The AUSF shall inform the UDM about the authentication result.
12) The AUSF shall notify the SEAF in a *Nausf _UEAuthentication_Authenticate* Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the K_{SEAF} shall be sent to the SEAF in the *Nausf _UEAuthentication_Authenticate* Response. In case the AUSF received a SUCI from the SEAF in the authentication request, and if the authentication was successful, then the AUSF shall also include the SUPI in the *Nausf _UEAuthentication_Authenticate* Response message.

If the authentication is successful, the key K_{SEAF} shall become the anchor key in the sense of the key hierarchy as shown in Figure 21. Then the SEAF shall derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI. The SEAF shall provide the ngKSI and the K_{AMF} to the AMF. If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and K_{AMF} to the AMF after it has received the *Nausf _UEAuthentication_Authenticate* Response message containing K_{SEAF} and SUPI; no commu-

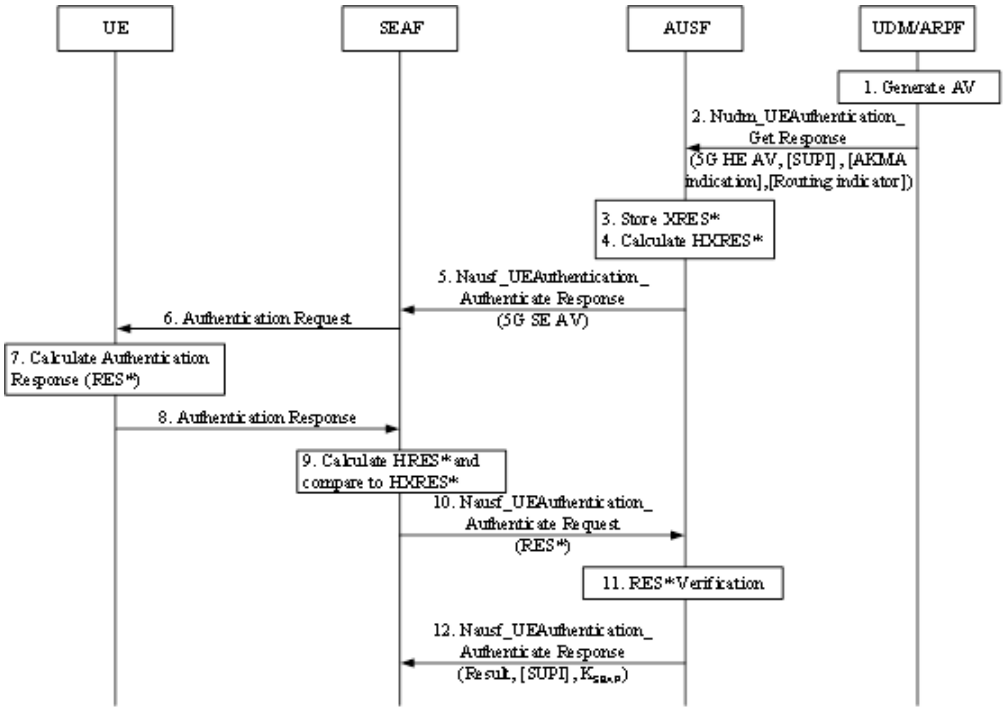


FIGURE 20. 5G-AKA protocol (credit: 3GPP).

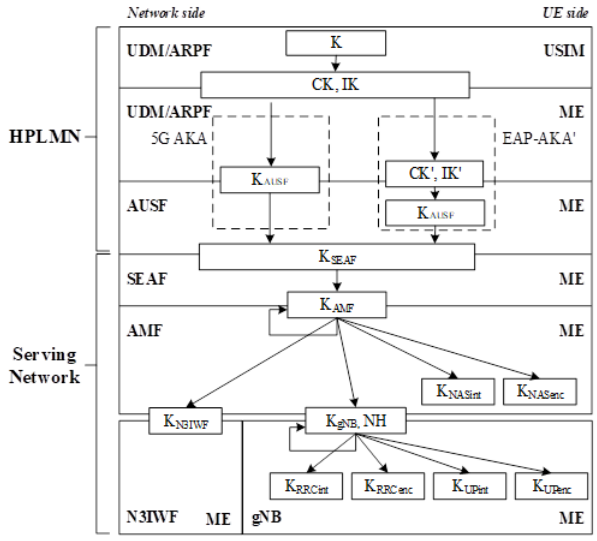


FIGURE 21. Key derivation in 5G (credit: 3GPP).

nication services will be provided to the UE until the SUPI is known to the serving network. It is worth noting that if the UE is roaming in a visited network then the AMF is from this visited network. The AKA procedures bind the K_{SEAF} to the serving network, by including the parameter SN name into the chain of key derivations. It prevents one serving network from claiming to be a different serving network, and thus provides implicit serving network authentication to the UE.

As shown above, the keying material generated by the primary AKA results in an anchor key K_{SEAF}. Keys for more than one security context can be derived from the K_{SEAF} without the need of a new authentication run. For example, K_{N3IWF} to establish security communication between the UE and a N3IWF gateway used in non-3GPP access. The key derivation on the UE and network sides are summarized in Figure 21.

Besides 5G-AKA, EAP-AKA' is the second option for performing the primary authentication. The EAP framework is specified in RFC 3748. It defines the following roles: peer, pass-through authenticator and back-end authentication server. The back-end authentication server acts as the EAP server, which terminates the EAP authentication method with the peer. EAP-AKA' is specified in RFC 5448. In the 5G system, when EAP-AKA' is used, the EAP framework is supported in the following way: the UE takes the role of the peer, the SEAF takes the role of pass-through authenticator, and the AUSF takes the role of the backend authentication server. More details can be found in 3GPP TS 33.501 document.

C. 5G INTRA- AND INTER-NETWORK SECURITY MECHANISMS

When 2G was developed, no security solution was specified to protect traffic in the core network. This is reasonable since these networks were only running circuit-switched traffic and were controlled by a small number of operators. With the introduction of 3G, the signalling and User Plane traffic started to run over IP networks, where protocols are open, and the networks are accessible not only to the Telecom operators but also to other entities. To this end, 3GPP has developed specifications for protecting IP-based traffic inside a core network and between core networks of different operators. The specification for protecting IP-based control-plane traffic is called Network Domain Security for

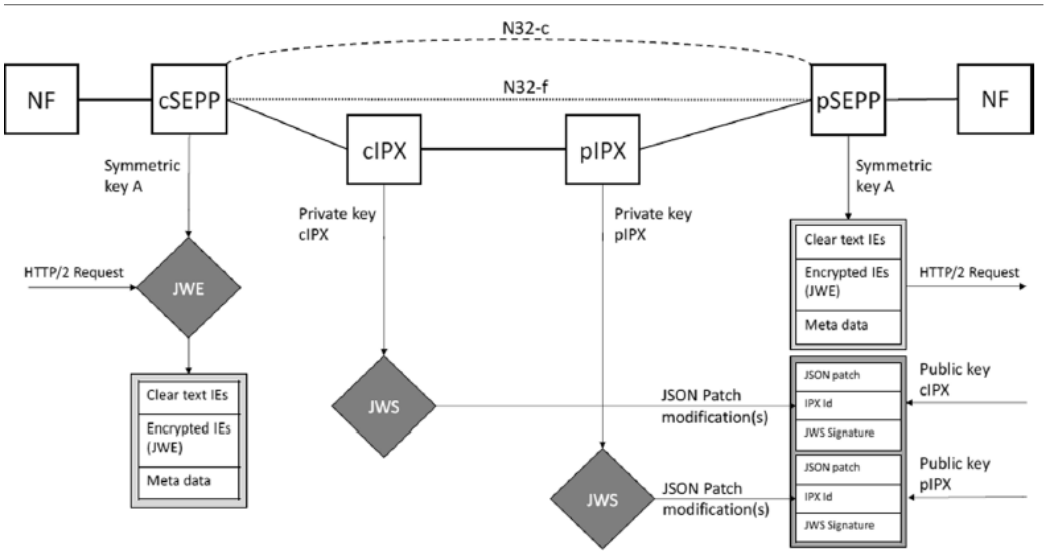


FIGURE 22. N-32 between SEPPs (credit: 3GPP).

IP-based Control Planes (NDS/IP) and is defined in the 3GPP TS 33.210 document. It was initially developed for 3G and later evolved for 4G to cover primarily IP-based Control Plane traffic such as those from Diameter and GTP-C. IKEv2/IPSec is the key cryptographic foundation for NDS/IP, and makes it generally applicable to any kind of IP traffic including HTTP/2.0 used in 5G core network. NDS/IP adopts the concept of security domains, which are networks managed by a single administrative authority. For example, a telecom operator can define its whole network as a security domain, or it can divide its network into multiple security domains. Essentially, security domain preserves the same level of security. On the border of a security domain, the operator places a Security Gateway (SEG) to protect the control-plane traffic that comes in and goes out, i.e. all NDS/IP traffic from network entities of one security domain is routed via an SEG before exiting that domain toward another security domain. Here, the role of SEG is similar to that of SEPP in 5G. The traffic between two SEGs is protected using IPsec in the tunnel mode, while the IKEv2 is used to set up the IPsec security associations between the SEGs. It is worth noting that NDS/IP can also be used to protect the user plane traffic other than the control plane signalling traffic.

To protect user plane messages, Inter-PLMN UP Security (IPUPS) is proposed and located at the perimeter of the PLMN. IPUPS is a functionality of the UPF that enforces GTP-U security on the N9 interface between UPFs of the visited and home PLMNs. At the perimeter of the 5G Core network, the SEPP gateway protects control plane messages and enforces inter-PLMN security on the N32 interface, shown in Figure 22. The SEPP implements application layer security for all the service layer information exchanged between two Network Functions (NFs) across two different PLMNs. On receiving service layer messages from a given NF, the SEPP protects the messages before sending them over the N32 interface. Similarly, on receiving a message over N32 interface the SEPP forwards the message to appropriate NF after security verification. The SEPP provides integrity protection, confidentiality protection of parts of message and replay protection. Mutual authentication, authorization, negotiation of cipher suites and key management are also parts of SEPP security functions. It also performs topology hiding and spoofing protection. Note that the application layer security protocol for the N32 interface is called PRINS in the 3GPP TS 33.501 document.

The security mechanisms for service-based interfaces are specified in clause 13 of 3GPP TS 33.501. As specified in clause 13.1, TLS shall be used for the security protection of messages at the transport layer for the service-based interfaces if network security is not provided by other means. As specified in clause 13.4.1, OAuth 2.0 may be used for authorization of NF service access. All NFs and the NRF shall support the OAuth 2.0 authorization framework with ''Client Credentials'' grant type as specified in clause 4.4 of IETF RFC 6749, except that there is no ''Authorization'' HTTP request header in the access token request. The NRF shall act as the Authorization Server providing ''Bearer'' access tokens (see IETF RFC 6750) to the NF service consumers to access the services provided by the NF service providers. If an NF service (i.e. API) receives an OAuth 2.0 access token in the ''Authorization'' HTTP request header field, the NF service shall validate the access token, its expiry and its access scope before allowing access to the requested resource, as specified in clause 7 of IETF RFC 6749.

D. SUMMARY

Compared to 4G and earlier generations, 5G has security as one of its design objectives in its development. From

the previous description, we can see the enhancements from every segment of the ecosystem: UE, RAN, and the Core. Many existing attacks against 4G networks have been made harder or infeasible in 5G benefiting from these enhancements, and security has become a selling point in many new 5G-based services. From our analysis of the 3GPP specifications, we acknowledge that security has been addressed very carefully and leveraged many lessons from the IT industry. However, it is too early to say that security is guaranteed for 5G and the applications on top. 5G network is very complex, but 3GPP specifications only cover some security aspects while leaving many aspects open.

- The first one is that every 5G network will have its own Core design, e.g. how the NFs are located, duplicated, and implemented. Different designs will exhibit very different security properties and resilience levels to cyberattacks, e.g. the resistance to DoS attacks. Analysis to this end can only be done on a case by case basis.
- The second one is that many features have been made mandatory in implementations, but their usage are optional and up to the network operators. For example, an operator may choose not use TLS but use some proprietary authentication method in some environments. This means the actual security guarantees will depend on the policies and configurations in the network. ENISA's report [5] made a good summary on this.
- Digital certificates are the main ingredients to perform entity authentication and enable the security protocols such as TLS and OAuth 2.0. However, in 3GPP specifications, certificate management has been treated as an out of scope subject. This means that the network operators need to find their own solutions to address this notoriously difficult problem. Considering the fact that a forged certificate will allow an attacker to control the NFs in 5G Core, it is of paramount importance to adopt a secure certificate management solution and enforce the appropriate policies.
- The adoption of IP-based protocols exposes 5G Core to remote cyber-attacks. For example, an attacker could try to access a specific NF like AMF or UDM in order to carry out some malicious activity. Such attacks could be facilitated by malicious and colluding internal personnel from the operator's IT team, e.g. the personnel could expose the IP address of the NF to the attacker and leak other information such as firewall configurations. Compared with 4G, these attacks are more likely to happen but harder to prevent in practice.
- Network slicing is a core technology to exploit the full potential of 5G networks, and a dedicated NF called NSSF has been dedicated to managing slice instances in a 5G network. Despite the current security mechanisms, researchers have shown that various types of threats exist. For instance, Olimid and Nencioni [25] theoretically presented several network slicing security issues in 5G, from the life-cycle, intra-slice and inter-slice aspects. AdaptiveMobile Security published a report [26] which enumerates three attack scenarios including user data extraction, DoS attacks and illegitimate data access in slices. Indicated in its report, new approaches are required to mitigate these vulnerabilities.
- At this stage, 5G has mostly been deployed along the Non-Standalone (NSA) path, to make full use of the existing 4G and other legacy networks. In addition, some 4G protocols such as GTP are also used in 5G networks. Therefore, it is possible that the vulnerabilities in the legacy networks and protocols will cause threats to the 5G Core network. For example, Positive Technologies [20] has demonstrated how to exploit the GTP protocol to mount a number of attacks against 5G Core network, e.g. DoS attacks, fraud and impersonation attacks.
- Being the main protocol for mutual authentication between UE and 5G Core, the 5G AKA protocol has been investigated by researchers. Basin *et al.* [35] formally verified the 5G AKA protocol using the security protocol verification tool Tamarin, and concluded that the protocol specification misses relevant security assumptions as well as other details like key confirmation. Therefore, in certain contexts, some vulnerabilities (e.g. privacy) may exist. The authors also commented on message redundancies and the use of SQN in the protocol. Borgaonkar *et al.* [22] exploited some logical drawback in generating the AUTH parameter to develop attacks against a subscriber's location privacy. Very recently, Wang, Zhang and Xie [36] proposed a countermeasure against the above attack by leveraging the already deployed key encapsulation mechanism of ECIES, namely using the shared key established by this mechanism to encrypt the challenges from the Home Network (HN). It is unclear whether this countermeasure will be adoptd by 3GPP. Michell [23] investigated how the security of 5G AKA protocol would be affected by quantum computing.

V. THE COMMON API FRAMEWORK (CAPIF)

In 3GPP, there are multiple northbound API-related specifications (e.g. APIs for Service Capability Exposure Function (SCEF) defined in 3GPP TS 23.682, APIs for the interface between Multimedia Broadcast Multicast Services (MBMS) service provider and Broadcast Multicast Service Center (BMSC) defined in 3GPP TR 26.981). Aiming at a unified northbound API framework to cover different duplicated API specifications and avoid inconsistency between them, 3GPP has developed the common API framework (CAPIF) that includes common aspects applicable to any northbound service APIs. It was first delivered in Release 15 and then enhanced in Release 16 and Release 17 (in the 3GPP TS 23.222 document).

Figure 23 shows the reference point based functional model for the CAPIF. The CAPIF core function in the PLMN trust domain supports service APIs from both the PLMN trust domain and the 3rd party trust domain which usually has business relationship with the PLMN. The API exposing

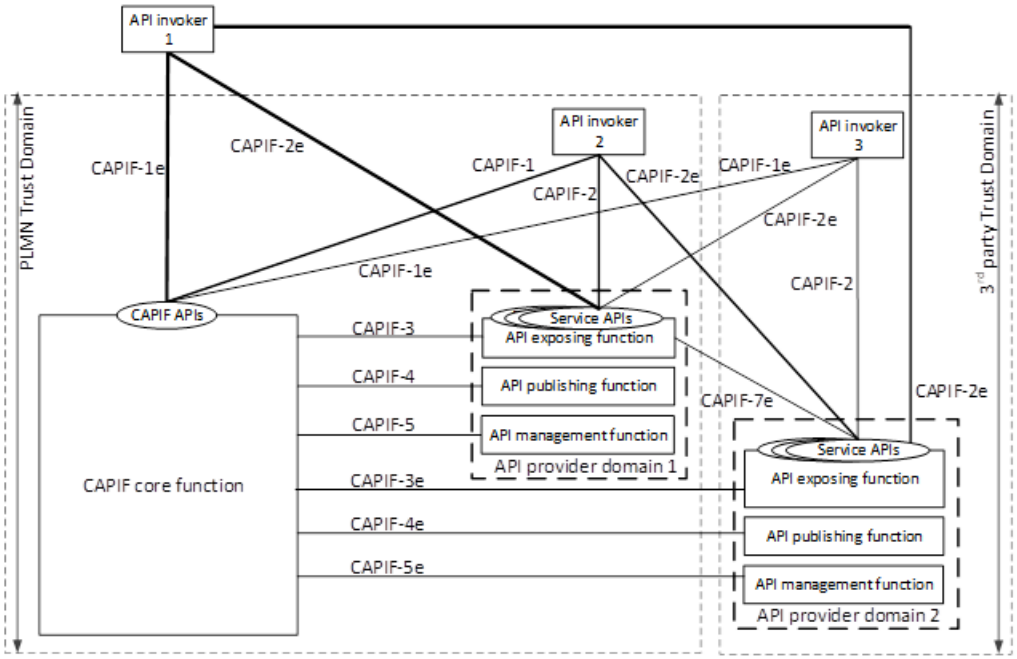


FIGURE 23. CAPIF architecture (credit: 3GPP).

function within the PLMN trust domain and the 3rd party trust domain can provide the service APIs to all potential API invokers. The invokers may exist within the PLMN trust domain, or within the 3rd party trust domain, or outside of both trust domains. Inside a trust domain (e.g. the PLMN trust domain), the API invoker interacts with the CAPIF core function via CAPIF-1 interface and invokes the service APIs via CAPIF-2 interface. In contrast, the API invoker 1, which is from outside the trust domains, interacts with the CAPIF core function via CAPIF-1e interface and invokes the service APIs via CAPIF-2e interface. The API exposing function, the API publishing function and the API management function of any trust domain can interact with the CAPIF core function. If they are from the PLMN trust domain then the interfaces are CAPIF-3, CAPIF-4 and CAPIF-5, otherwise the interactions are via CAPIF-3e, CAPIF-4e and CAPIF-5e interfaces. In addition, the API exposing functions can interact with each other via either CAPIF-7 or CAPIF-7e interface depending on whether or not they are in the same trust domain. The diagram in Figure 24, provided in the Annex A of 3GPP TS 23.222, shows an informal illustration of the CAPIF operations, which occur between different actors involving the API invoker, the CAPIF core function, the API exposing function, the API publishing function and the API management function.

A. SECURITY OF CAPIF FRAMEWORK

The 3GPP TS 33.122 document defines the security architecture together with the security features and mechanisms for CAPIF. It is stated that TLS shall be used to provide integrity protection, replay protection and confidentiality protection for the CAPIF-1, CAPIF-2, CAPIF-3, CAPIF-4, CAPIF-5 and CAPIF-7 interfaces, as well as for the CAPIF-1e, CAPIF-2e and CAPIF-7e interfaces. Note that the support of TLS is mandatory, but it is optional for the domain administrator to use it depending on its own policy. For the CAPIF-3e, CAPIF-4e and CAPIF-5e interfaces, NDS/IP security mechanisms shall be used to secure communication between different IP security domains.

Authentication and authorization are required for all API invokers. For an API invoker that is not from the PLMN trust domain, the CAPIF core function shall utilize the CAPIF-1e, CAPIF-2e and the CAPIF-3 interfaces to onboard, authenticate and authorize the API invoker before granting service access. When the API invoker is from the PLMN trust domain, the CAPIF core function shall perform authentication and authorization of the API invoker via the CAPIF-1, the CAPIF-2 and the CAPIF-3 interfaces before granting service access. Authentication and authorization of API invokers (both internal and external to the PLMN trust domain) are detailed in clause 6 in 3GPP TS 33.122.

B. USING CAPIF WITH 5G CORE'S NEF

According to 3GPP TS 29.222, which describes the protocols for NEF Northbound interface between the NEF and an AF, when CAPIF is used with an NEF that is used for external exposure, the NEF shall support the following:

- the API exposing function and related APIs over CAPIF-2/2e and CAPIF-3/3e reference points;
- the API publishing function and related APIs over CAPIF-4/4e reference point;

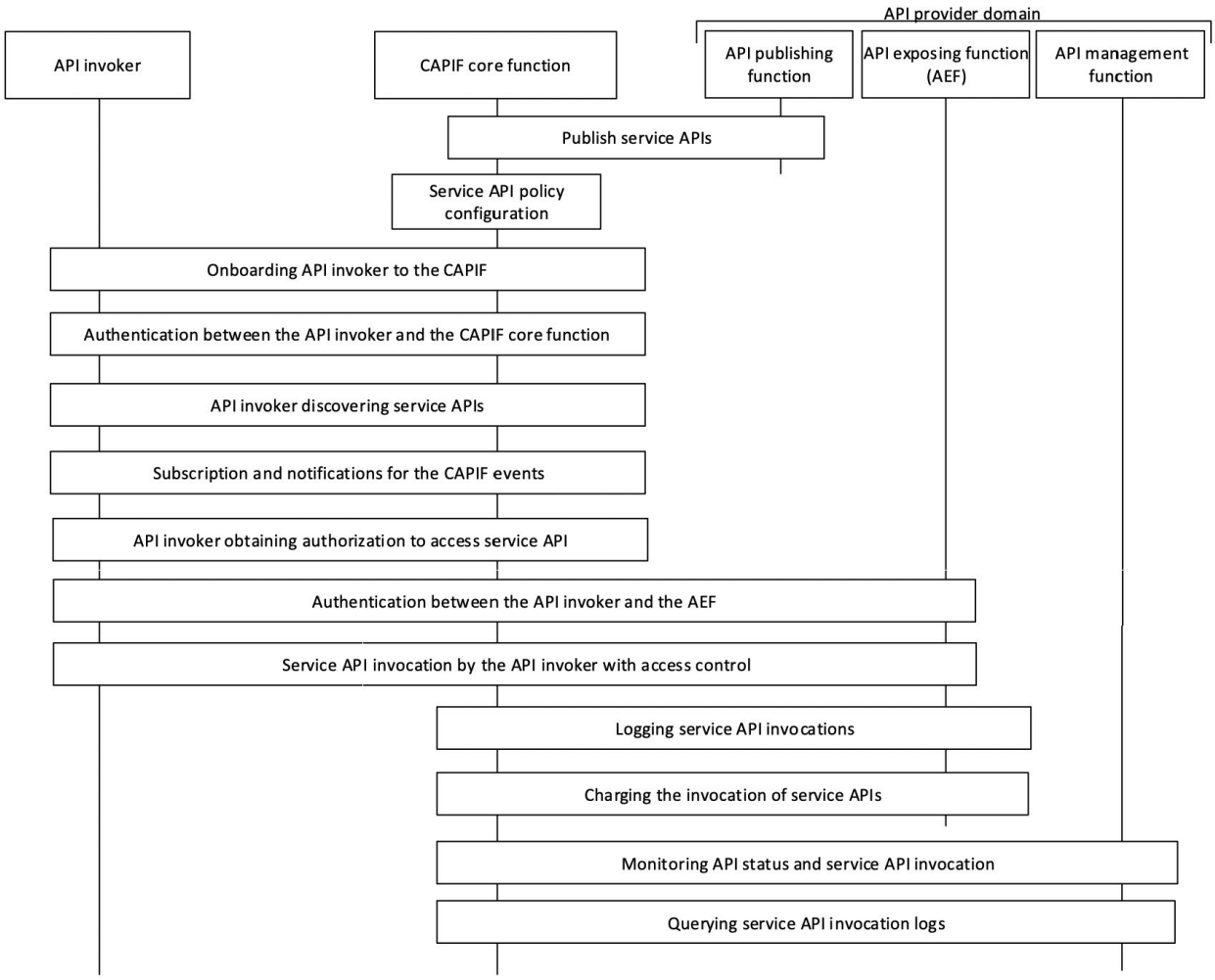


FIGURE 24. CAPIF flow (credit: 3GPP).

- the API management function and related APIs over CAPIF-5/5e reference point; and
- at least one of the security methods for authentication and authorization, and related security mechanisms.

Security related, when CAPIF is used for external exposure, before invoking the API exposed by the NEF, the AF as API invoker shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with CAPIF core function and ensure the NEF has enough credential to authenticate the AF. If PKI or TLS-PSK is used as the selected security method between the AF and the NEF, upon API invocation, the NEF shall retrieve the authorization information from the CAPIF core function. The access to the NEF northbound APIs may be authorized by means of the OAuth 2.0 protocol, where the CAPIF core function plays the role of the authorization server. If OAuth 2.0 is the selected security method between the AF and the NEF, the AF shall obtain a "token" from the authorization server before consuming services offered by the NEF northbound APIs.

C. SUMMARY

Exposing the 5G Core capabilities to API invokers (within or outside trust domains) is critical to the verticals that use 5G as the underlying infrastructure. On the other hand, as we have mentioned before, this also exposes the vulnerabilities of 5G Core to the outsider attackers and make the network more fragile. For instance, NEF could become an attack victim if it is used by the CAPIF in deployment. On the positive side, the unification of northbound APIs under the same CAPIF framework helps standardise the workflow and the security protection towards the Core network. It is open research area to investigate further how CAPIF will affect the security of 5G Core.

VI. DEFENDING 5G NETWORKS FROM OPERATORS' PERSPECTIVE

5G is a major evolution in telecommunications that enables the future Internet of Things and powers new mission-critical use cases. The industry has embraced security right from the design, various security mechanisms have been introduced

throughout the 5G specification releases. Moreover, public and private organisations have contributed a significant effort in reviewing and identifying potential security vulnerabilities in the design and potentially in the deployment of 5G networks.

The principle of ''security by design'' and ''defence in depth'' have never been as important and adopted as with the design and deployment of 5G networks, when comparing 5G with the development of the previous generations of mobile networks. However, they are only parts of a bigger security landscape that includes also operational and organisational security. Surprisingly, to the best of our knowledge, there has been no work or report investigating the defending aspects and opportunities in 5G networks. 5G comes with complex technology stacks, vulnerabilities and weaknesses are no-doubt exit in production. It is crucial to continuously monitor and maintain visibility in the networks to detect and mitigate attacks. Hence, in this section we discuss different points regarding defending a 5G network in production.

A. LEVERAGING NEW DEVICES

The 5G design includes a number of built-in security components. For instance, The Service Communication Proxy (SCP) is deployed along side of NFs for providing routing control and observability to the core network. The Security Edge Protection Proxy (SEPP) is introduced at the perimeter of each PLMN to perform message filtering and topology hiding for all API messages. Such components give rise to invaluable operational logs and security traces that should/shall be ingested and processed from day one into the Security Information and Event Management (SIEM) of an MNO to detect attacks and anomalies in real-time. Besides, the UPF may integrate a Deep Packet Inspection (DPI) for packet inspection and classification. The insights from such a DPI can also be an asset for the SIEM.

The design decision to go all on IP, softwarisation, and containerisation enables the adoption of a wilder spectrum of security monitoring solutions, those that traditionally serve only IT networks can now be extended to monitor the 5G core and its interfaces to RAN. For instance, ''Container Security'' is no longer considered only in IT world but now extended to telecom world. Also, unlike in the previous generations of telecom networks that run on dedicated signalling protocols (e.g., Diameter, GTPC, SS7), 5G — especially 5G core — runs on JSON/HTTP2 APIs, which is widely used in the computer industry. Thus, this allows more defending players to join-force in protecting 5G networks.

B. OPPORTUNITIES AND CONSIDERATIONS

On the detection of attacks against 5G networks, we advocate the use of the recent advances in the field of deep machine learning to detect anomalies, which are often an indicator of cyber-attacks or network failures. The algorithms introduced in recent years, such as AutoEncoder or Generative Adversarial Networks [37], [38], scale well with the amount of data in telecom networks. They also perform well in detecting anomalies without much prior knowledge of potential or known attacks. Hence, they can detect new (0-day) attacks that have not been documented or observed. This is important in the deployment of 5G as it is at the same time new and complex.

As briefly discussed in the previous subsection, there is a shift from telecom world to IT. This opens an opportunity for new techniques that can combine holistically multiple data sources from different protocol stacks, different network generations. It is envisioned that a defence technique or tool that harvests data from GTP, Diameter, and 5G core API/HTTP2 will likely champion catching the yet-to-devised attacks.

Furthermore, an operator can proactively deploy security mediums that are well-known in IT to have a better visibility in 5G networks. Honeypots, network traps, intrusion detection systems will be a viable tool. For instance, we can deploy a honeypot playing the role of a Network Repository Function (NRF) to capture malicious service discovery activities. Originally, a NRF maintains NF profiles and serves as a repository of the services for service consumers to discover the services offered by other NFs. An envisioned NRF honeypot might expose a similar, yet mocked-up, interfaces and functionalities but with the goal of determining reconnaissance activities. This allows to catch attackers who play the role of a service consumer and try to discover sensitive services/servers in a network.

REFERENCES

[1] *The 3rd Generation Partnership Project (3GPP)*. Accessed: Nov. 10, 2021. [Online]. Available: https://www.3gpp.org/

[2] ENISA. (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[3] N. C. Group. (2020). *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*. [Online]. Available: https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf

[4] ENISA. (2020). *ENISA Threat Landscape for 5G Networks Report*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[5] ENISA. (2021). *Security in 5G Specifications—Controls in 3GPP*. [Online]. Available: https://www.enisa.europa.eu/publications/security-in-5g-specifications

[6] ENISA. (2018). *Signalling Security in Telecom SS7/Diameter/5G*. [Online]. Available: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

[7] ENISA. (2016). *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*. [Online]. Available: https://www.enisa.europa.eu/publications/sdn-threat-landscape

[8] *5G Enablers for Network and System Security and RESILIENCE (5G-ENSURE) Project*. Accessed: Nov. 10, 2021. [Online]. Available: http://www.5gensure.eu/

[9] *Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access (CHARISMA) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://www.charisma5g.eu/

[10] *5G Mobile Network Architecture for diverse Services, Use Cases, and Applications in 5G and Beyond (5G-MoNArch) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://5g-monarch.eu/

[11] *Internet of Radio-Light (IoRL) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://iorl.5g-ppp.eu/

[12] *A Unified Network, Computational and Storage Resource Management Framework Targeting End-to-End Performance Optimization for Secure 5G Multi-Technology and Multi-Tenancy Environments (5G-COMPLETE) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://5gcomplete.eu/

[13] *Zero-Touch Security and Trust for Ubiquitous Computing and Connectivity in 5G Networks (5GZORRO) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://www.5gzorro.eu/

[14] *INtelligent Security and PervasIve tRust for 5G and Beyond (INSPIRE-5Gplus) Project*. Accessed: Nov. 10, 2021. [Online]. Available: https://www.inspire-5gplus.eu/

[15] G. M. Køien, "On threats to the 5G service based architecture," *Wireless Pers. Commun.*, vol. 119, no. 1, pp. 97–116, Jul. 2021.

[16] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[17] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[18] X. Hu, C. Liu, S. Liu, W. You, and Y. Zhao, "Signalling security analysis: Is HTTP/2 secure in 5G core network?" in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2018, pp. 1–6.

[19] Positive Technologies. (2020). *5G SA Core Security Research*. Accessed: Nov. 10, 2021. [Online]. Available: https://positive-tech.com/knowledge-base/research/5g-sa-core-security-research/

[20] Positive Technologies. (2020). *Threat Vector: GTP Vulnerabilities in LTE and 5G Networks 2020*. Accessed: Nov. 10, 2021. [Online]. Available: https://positive-tech.com/knowledge-base/research/gtp-2020/

[21] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, May 2019, pp. 221–231.

[22] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols," *Privacy Enhancing Technol.*, vol. 2019, no. 3, pp. 108–127, 2019.

[23] C. J. Mitchell, "The impact of quantum computing on real-world security: A 5G case study," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101825.

[24] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, Feb. 2019, pp. 1–15.

[25] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[26] (2020). *A Slice in Time: Slicing Security in 5G Core Networks*. Accessed: Nov. 10, 2021. [Online]. Available: https://info.adaptivemobile.com/5g-network-slicing-security

[27] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.

[28] S.-Y. Lien, S.-L. Shieh, Y. Huang, B. Su, Y.-L. Hsu, and H.-Y. Wei, "5G new radio: Waveform, frame structure, multiple access, and initial access," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 64–71, Jun. 2017.

[29] S. Rommer, P. Hedman, M. Olsson, L. Frid, S. Sultana, and C. Mulligan, *5G Core Networks: Powering Digitalization*. New York, NY, USA: Academic, 2019.

[30] Cloud Native Computing Foundation. (2022). *Kubernetes (K8s) Production-Grade Container Orchestration*. [Online]. Available: https://kubernetes.io/

[31] *Transport Layer Security (TLS)*. Accessed: Nov. 10, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Transport_Layer_Security

[32] *The Heartbleed Bug*. Accessed: Nov. 10, 2021. [Online]. Available: https://heartbleed.com/

[33] *OpenSSL Cryptography and SSL/TLS Toolkit*. Accessed: Nov. 10, 2021. [Online]. Available: https://www.openssl.org/

[34] A. R. Prasad, S. Arumugam, and S. B. Zugenmaier, "3GPP 5G security," *J. ICT Standardization*, vol. 6, pp. 137–158, May 2018.

[35] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 1383–1396.

[36] Y. Wang, Z. Zhang, and Y. Xie, "Privacy-preserving and standard-compatible AKA protocol for 5G," in *Proc. 30th USENIX Secur. Symp., USENIX Secur.*, M. Bailey and R. Greenstadt, Eds. Berkeley, CA, USA: USENIX Association, 2021, pp. 3595–3612.

[37] A. Borghesi, A. Bartolini, M. Lombardi, M. Milano, and L. Benini, "Anomaly detection using autoencoders in high performance computing systems," in *Proc. AAAI Conf. Artif. Intell.*, vol. 33, Jul. 2019, pp. 9428–9433.

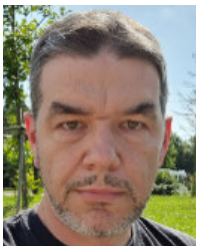
[38] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org

QIANG TANG received the Ph.D. degree from Royal Holloway, University of London, U.K. He is currently a Senior Research Scientist at the Luxembourg Institute of Science and Technology (LIST). His research interests include applied cryptography, DLT/blockchain-enabled security design, and the privacy issues in machine learning.

ORHAN ERMIS received the Ph.D. degree from the Department of Computer Engineering, Boğaziçi University, Turkey, in 2017. He is currently a Postdoctoral Researcher at the Luxembourg Institute of Science and Technology (LIST). His research interests include privacy enhancing technologies, applied cryptography, network security, and machine learning applications for security.

CU D. NGUYEN received the Ph.D. degree in artificial intelligence and software engineering from the University of Trento, Trento, Italy, in 2009. He is currently working at Post Luxembourg as a Security Expert and a Data Scientist. Before joining POST Luxembourg, he was a Researcher at the University of Luxembourg and has published more than 50 scientific papers to prestigious international conferences and journals. His research interests include machine learning research and development and its application in fraud and telecom security domain.

ALEXANDRE DE OLIVEIRA joined at POST Luxembourg as a Telecom Security Expert with Labs and Innovation at Cyberforce. After more than four years traveling around the world part of P1Security as a Telecom Security Expert and a Main Developer of PTA and the VKB, he took the decision to bring his knowledge and a more long-term approach into a telecom operator. Part of Cyberforce and responsible of the telecom security, he is involved in improving on long term the global security posture of the telecom network but also co-leading the development of TIDS and TSS.



ALAIN HIRTZIG received the M.Sc. degree in electrical engineering from the University of Liège, Belgium. He is currently heading the Cyberlabs Team, Post Luxembourg. Since joining POST Luxembourg, he has been active as a Networks and Security Engineer and later as a Security Architect involved on the design and implementation of strategic projects.