5G SECURITY

TS Division, TEC

Contents

1. Introduction

The 5G wireless networks will provide very high data rates and higher coverage with significantly improved Quality of Service (QoS), and extremely low latency. With extremely dense deployments of base stations, 5G will provide ultra-reliable and affordable broadband access everywhere not only to cellular hand-held devices, but also to a massive number of new devices related to Machine-to-Machine communication (M2M), Internet of Things (IoT), and Cyber-Physical System (CPSs). 5G is not a mere incremental advancement of 4G but an integration of new technologies to meet the ever growing demands of user traffic, emerging services, existing and future IoT devices.

The development of the Fifth Generation (5G) wireless networks is gaining momentum to connect almost all aspects of life through the network with much higher speed, very low latency and ubiquitous connectivity. Due to its crucial role in our lives, the network must secure its users, components, and services. The security threat landscape of 5G has grown enormously due to the unprecedented increase in types of services and in the number of devices.

The security solutions and architectures used in previous generations (i.e. 3G and 4G), apparently, will not suffice for 5G. For example, virtualization and multi-tenancy in which different, and possibly conflicting, services share the same mobile network infrastructure were not common before. The latency requirements, such as authentication latency in vehicular communication or Unmanned Aerial Vehicles (UAVs) were not that much critical. Hence it can be stated that, the security architectures of the previous generations lack the sophistication needed to secure 5G networks. New technological concepts or solutions that will be used in 5G to meet the demands of increasingly diverse applications and connected devices. For example, the concepts of cloud computing, Software Defined Networking (SDN), and Network Function Virtualization (NFV)are considered to be the potential problem solvers in terms of costs and efficiency.

The main reason for new security solutions and architecture is the dynamics of new services and technologies in 5G. Therefore, security solutions should be envisioned to cope with diverse threats on various services, novel technologies, and increased user information accessible by the network.

This paper focusses on comprehensive security architecture and capabilities in 5G, security challenges along with proposed countermeasures to handle to those security threats.

2. Security review in previous Generations:

First Generation cellular systems used analog signal processing and was designed primarily for voice services. Due to the nature of analog communications, it was difficult to provide efficient security services for 1G. This advance phone service did not use encryption and thus there was no security of information or telephone conversations. Hence, practically the whole system and users were open to security challenges such as eavesdropping, illegal access, cloning, and user privacy.

Second Generation has introduced the authentication and encryption based protection using the SIM for encryption key management. But 2G had several security limitations or weaknesses.

In 2G the operators can only authenticate the UEs in a unilateral mechanism, whereas the UEs had no option to authenticate the operator. Therefore, it was possible for a false operator to impersonate the original operator and perform a man-in-the-middle attack. Moreover, the encryption algorithms were also reverse engineered and the ciphering algorithms were subject to several attacks. GSM did not provide data integrity against channel hijacking in the absence of encryption, and were also vulnerable to DoS attacks. Further 2G systems did not have the capability of upgradation in their security capabilities.

Third Generation or 3G systems as they reformed have upgraded its security architecture to address the security vulnerabilities of previous generations. It has included the security capabilities of 2G but upgraded the 2G security limitations by introduction of UMTS Authentication and Key Agreement (AKA) protocol. UMTS supports bilateral authentication which removes the threat of a false base station. The access security feature includes user identity confidentiality that ensures that a user cannot be eavesdropped on a radio access link. The user identity confidentiality also needs to support user location confidentiality and user untraceability. To achieve these objectives, the user is identified by a temporary identity or by a permanent encrypted identity.

Subsequently in LTE-Advanced that form part of fourth Generation (4G), for handling security 3GPP has introduced some more security features involving Access Security, Network domain security, User domain security, Application domain security, and visibility and configurability of security. The Evolved Packet System-AKA (EPS-AKA) had one major enhancement over UMTS-AKA which is called cryptographic network separation. This feature limits any security breach in a network and also limits the possibility of spreading attacks across the network. This is achieved by binding any EPS-related cryptographic keys to the identity of the Serving Network (SN), to which the keys are delivered. This feature also enables the UE to authenticate the SN. A new key hierarchy and handover mechanism has been introduced to secure the mobility process in LTE. However due to early termination point of encryption, the eNodeB has become more vulnerable to physical attacks, DoS attacks, Passive attacks. However, 3GPP has introduced stringent requirements on eNodeB by including secure setup and configuration of base station SW, secure key management and secure environment for handling the user and control plane data. However existing security mechanisms are not suitable for new services and devices such as in IoT which are addressed in 5G. The tabular comparison of Security in 4G and 5G are as follows:

Function	4G	5G
Access Agnostic Authentication	Non-Access Agnostic	Unified Authentication
Authentication Credentials	Only AKA credentials	AKA credentials or Certificate for IOT/Private Networks
Authentication Protocol	EPS-AKA over 4G NAS	5G-AKA over 5G NAS or EPA-AKA'/EAP-TLS over 5G NAS
Security Protocol for Authentication credentials	UICC	UICC or eUICC
Home control for Authentication	Not Supported	Supported (Home PLMN involved in Authentication and holds the key)
Integrity protection for User Plane Traffic	Not Supported	Supported (Optional to use)

User Plane security	Enabled/disabled for overall mode	Per PDU based Selective protection
Subscription Identity Protection	IMSI is not protected if there is no security context	SUPI is always protected using Asymmetric cryptography
Network Domain Security	IPSec (Point to Point Architecture)	TLS/Application Layer Protection (SBA)
Steering of Roaming	OTA based (Optional to use)	New native solution using control plane (mandatory to implement, optional to use) + OTA based (Optional to use)

Source: Ericsson

Table 1: Comparison of Security in 4G Vs 5G

3. Security in 5G:

5G is considered a new ecosystem connecting nearly all aspects of the society, vehicles, home appliances, health care, industry, businesses, etc., to the network. It will provide ubiquitous broadband services, enable connectivity of massive number of devices in the form IoT, and entertain users and devices with high mobility in an ultra-reliable manner. Due to this 5G may be subjected to introduction of new array of threats and security vulnerabilities will cause a major challenge to both present and future networks. Therefore, security of 5G and systems connected through 5G carries extreme importance and must be considered right from the design phases.

The radio part of 5G needs extreme spectrum efficiency, cost effective deployment, effective coordination, interference cancellation and dynamic radio topologies. Since the core will use SDN and NFV technologies to separate the user and control plane which will enable the dynamic network function placement. Additionally, SDN will separate the control and network plane and centralizing the network control may also create loopholes for security vulnerabilities. Additionally, the security challenges associated with NFV, SDN and Network slicing such as inter-federated conflicts and resource hijacking needs proper investigation.

3.1 5G Security Architecture:

3GPP TS 33.501 V15.4.0 (2019-05) is the latest specification published by SA3 for 5G security. It defines the security architecture, features and mechanisms for the 5G system and the 5G core. In addition, it covers the security procedures performed within the 5G system, including the 5G core and the 5G New Radio (NR).3GPP has specified the security architecture of 5G as illustrated in figure below including the following network architectural concepts on using the following domains:

a. **Network access security (I):** Comprises the set of security features that enables a UE to securely authenticate and access network services. Access security includes security of 3GPP and non-3GPP access technologies, and delivery of security context from SN to the UE.

b. **Network domain security (II)**: Comprises of a set of security features that enables network nodes to securely exchange signalling and user plane data.

c. **User domain security (III)**: Consists of security features that enables secure user access to UE.

d. **Application domain security (IV):** Includes security features that enables applications (user and provider domains) to securely exchange messages.

e. **Service Based Architecture (SBA) domain security (V**): Comprises of security features for network element registration, discovery, and authorization, as well as security for service-based interfaces.

f. **Visibility and configurability of security (VI):** Includes security features that inform users whether security features are in operation or not.

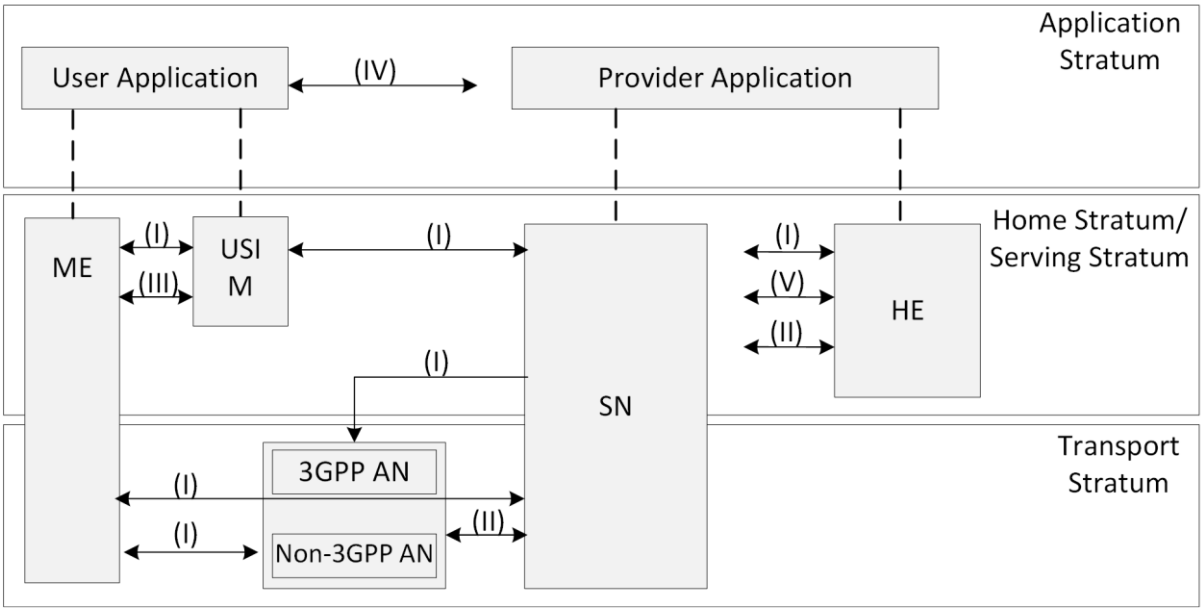

Fig 1: 5G Security Architecture as per 3GPP TS 33.501

3.2 5G Security Features as defined by 3GPP:

The features which are defined by 3GPP for ensuring and enhancing Security in 5G are as follows:

3.2.1 INCREASED HOME CONTROL:

This feature have been introduced to address vulnerabilities found in 3G and 4G networks where networks could be spoofed by sending false signalling messages to the home network to request the International Mobile Subscriber Identity (IMSI) and location of a device thus to intercept voice calls and text messages.

This is used for Authentication of the device location when the device is roaming. It allows the home network to verify the device that whether the device is actually in the serving network when the home network receives a request from a visited network for device authentication.

3.2.2 UNIFIED AUTHENTICATION FRAMEWORK

Authentication in 5G networks will be access agnostic. The same authentication methods will be used for both 3GPP and non-3GPP access networks such as 5G radio access and Wi-Fi access.

3.2.3 SECURITY ANCHOR FUNCTION (SEAF)

Security Anchor Function (SEAF) is introduction of concept of an anchor key which allows for the re-authentication of the device when it moves between different access networks or serving networks without having to run the full authentication method (for example, Authentication and Key Agreement (AKA). This reduces the signalling load on the home network Home Subscriber Server (HSS) during various mobility services. The SEAF and the Access and Mobility Management Function (AMF) could be co-located or separated. In 3GPP Release 15, the SEAF functionality is co-located with the AMF.

3.2.4 SUBSCRIBER IDENTIFIER PRIVACY

In 5G, network operators allocate a unique identifier being defined as SUPI which is similar to IMSI in 4G. This is a globally unique Identifier allocated for each subscriber provisioned in the Unified Data Management/User Data Repository (UDM/UDR). The SUPI is used only inside 3GPP system. Examples for SUPI formats include the IMSI and Network Access Identifier (NAI).

The SUPI is never disclosed over the air in the clear when a mobile device is establishing a connection. In order to enable roaming scenarios, the SUPI shall contain the address of the home network (for example, the Mobile Country Code [MCC] and Mobile Network Code [MNC] in the case of an IMSI-based SUPI). For interworking with the Evolved Packet Core (EPC), the SUPI allocated to the 3GPP UE shall always be based on an IMSI to enable the UE to present an IMSI to the EPC.

A Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI which is used until the device and network are authenticated instead of disclosing the SUPI. This is introduced to offer the enhanced security protection and subscriber identification Security in 5G. Subsequently Subscription Identifier De-Concealing Function (SIDF) is responsible for de-concealing the SUPI from the SUCI. The SIDF uses the private key part of the privacy-related home network public/private key pair that is securely stored in the home operator's network. The de-concealment shall take place at the UDM. Access rights to the SIDF shall be defined, in such a manner that a network element of the home network is allowed to request SIDF.

The UE shall generate a SUCI using a protection scheme with the raw public key that was securely provisioned in control of the home network. The UE shall not conceal the home network identifier, such as the MCC or MNC. The UE shall include a SUCI only to the 5G Non-Access Stratum (NAS) messages such as UE is sending a registration request message of type "initial registration" to a PLMN for which the UE does not already have a 5G- Globally Unique Temporary Identifier (GUTI), the UE shall include a SUCI to the Registration Request message.

This procedure has been defined to prevent IMSI catchers (also known as false base stations, or Stingrays) from retrieving the subscriber’s identity. This is accomplished by forcing a device either to attach to the Rogue Base Station (RBS) or perform attachment process to operator’s Base Station while sniffing the unencrypted traffic over the air.

3.2.5 SECURITY EDGE PROTECTION PROXY (SEPP)

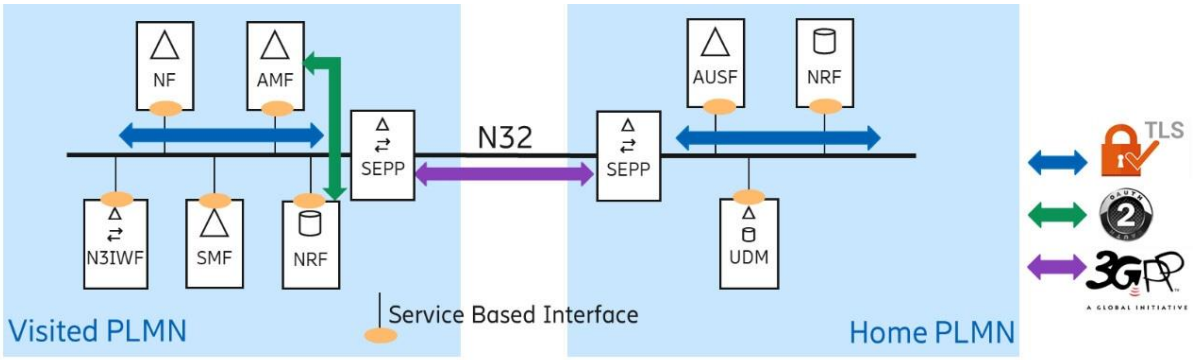

Fig 2: Source: Ericsson

5G system architecture implements Security Edge Protection Proxy (SEPP) at the perimeter of the Public Land Mobile Network (PLMN) network or across two operators. All signalling traffic across operator networks is expected to transit through these security proxies. SEPP receives all service layer messages from the Network Function (NF) and protects them before sending them out of the network on the N32 interface. Additionally, it receives all messages on the N32 interface and after verifying security where present, it forwards them to the appropriate network function.

It also Perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network. It also handles the key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs. It has the capability of hiding the topology by limiting the internal topology information visible to external parties. It differentiates between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications. It implements anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers.

An attacker could attempt a bidding down attack by making the UE and the network entities believe that the other side does not support a security feature, even when both sides do support a security feature. A SEPP can help ensure that a bidding down attack, in the above sense, can be prevented. Bidding down attack is the attack through which attacker force the other side to think that it is is not using the advance security feature and thereby decreasing the Quality of Service.

3.2.6 AUTHENTICATION FRAMEWORK:

A complete separate authentication framework has been introduced in 5G in order to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the KSEAF, which is provided by the Authentication Server Function (AUSF) of the home network to the SEAF of the serving network. The UE and the serving network shall support Extensible Authentication Protocol and Key Agreement (EAPAKA) and 5G AKA authentication methods.

3.2.7 BINDING OF ANCHOR KEY TO SERVING NETWORK:

The primary authentication and key agreement procedures shall bind the anchor key KSEAF to the serving network. The binding to the serving network prevents one serving network from claiming to be a different serving network, and thus provides implicit serving network authentication to the UE. This implicit serving network authentication shall be provided to the UE regardless of the access network technology, so it applies to both 3GPP and non-3GPP access networks. The anchor key binding shall be achieved by including a parameter called "serving network name" into the chain of key derivations that leads from the long-term subscriber key to the anchor key.

3.2.8 5G GLOBALLY UNIQUE TEMPORARY IDENTIFIER:

The AMF in 5G allocates a 5G Globally Unique Temporary Identifier (5G-GUTI) to the UE that is common to both 3GPP and non-3GPP access. The same 5G-GUTI for accessing 3GPP access and non-3GPP access security context within the AMF for the given UE. An AMF may re-assign a new 5G-GUTI to the UE at any time. A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The AMF sends a new 5G-GUTI to the UE in a registration accept message after receiving registration request message of type "initial registration" or "mobility registration update" or “periodic registration update” from a UE.

The 5G Serving Temporary Mobile Subscriber Identity (S-TMSI) is the shortened form of the GUTI to enable more efficient radio signalling procedures.

3.2.9 UE-ASSISTED NETWORK-BASED DETECTION OF FALSE BASE STATION:

The UE in Radio Resource Control (RRC) CONNECTED mode sends measurement reports to the network in accordance with the measurement configuration provided by the network useful for detection of false base stations or SUPI/5G-GUTI catchers.

3.3 Standardisation activities in Security in 5G:

Different key organisations are either working or developed the immense contributions in the field of 5G security. The brief of some of work and related milestone are elaborated below in tabulated form:

Standardization Bodies	Workgroups	Major security areas in focus	Milestones
3GPP	Service and System Aspects Security Group (SA3)	Security architecture, RAN security, authentication mechanism, The subscriber privacy, network slicing	TR 33.899 Study on the security aspects of the next generation system, TS 33.501: Security architecture and procedures for 5G System
5GPPP	5GPPP Security WG	Security architecture, The subscriber privacy, The authentication mechanism	5G PPP Security Landscape (White Paper) June 2017
IETF	12NSF, DICE WG, ACE WG, DetNet WG	Security solutions for massive IoT devices in 5G, User privacy, Network security functions (NSFs)	RFC 8192, RFC 7744, Deterministic Networking (DetNet) Security Considerations

NGMN	NGMN 5G security group (NGMN P1 WS1 5G security group)	Subscriber privacy, Network slicing, MEC security	5G security recommendations: Package 1 and 2, and 5G security: Package 3
ETSI	ETSI TC CYBER, ETSI NFV SEC WG, ESTI MEC ISG	Security architecture NFV security, MEC security, privacy	ETSI GS NFV-SEC 010, ETSI GS NFV-SEC 013 ETSI GS NFV-SEC 006 and ETSI GS MEC 009
NIST	Security working group	IoT security guidelines and assessment	Draft Interagency Report, NISTIR 8200

Source: Refer Ref. at (v)

Table 2: Standardisation activities in Security in 5G

Including this the Ericsson, Nokia and other Network equipment manufacturers have published several reports providing interesting insights in the 5G security requirements and challenges, the security architecture transformation and promotion of 5G security standardization and their security ecosystem.

On the basis of study conducted worldwide including standard organisations, different Security challenges along with solutions or possible security approaches to counter the security challenges are elaborated in the following Sections.

4 5G Security Risks:

4.1 Weak Slices Isolation and connectivity:

A weak slicing Isolation connection may adversely affect the entire 5G security. The sensitive data stored in the slicing could be exposed to applications running in other slices services, through side channel attacks. Side Channel attack is a class of attack on cryptographical implementation. Supposing two slices respectively use two VNF instances (i.e., virtual machines (VMs)) in the same hardware, a malicious VM in one slice may extract sensitive information from a victim VM in the other slice. Specifically, if the two slices have very different security levels, this attack could create a significant benefit for the attacker. This risk is even higher since isolation is distributed over each of the security domains of the underlying 5G security architecture. Therefore, a specific policy of resource allocation is desired to cope with the potential Side Channel attacks among different slices in 5G RAN.

4.2 Traffic embezzlement due to recursive/additive virtualization:

The double level of virtualization delivered by the combination of SDN/NFV in 5G infrastructures may allow traffic capture and rerouting. That is, inconsistency between Orchestrator abstraction, SDN control abstraction and the physical and network resources may allow third parties to capture /embezzle/alter control plane and user plane, without any knowledge nor detection by the operator of the whole infrastructure.

4.3 Network Slicing Security Threats:

Network slicing enables the management of multiple logical networks as virtually independent business operations on a common physical infrastructure. In practice, this corresponds to the idea that the mobile network could be partitioned into a set of resources that might be virtual. Each one is called a "slice" that can be allocated for different purposes. For example, a slice can be allocated to a mobile virtual network operator (MVNO), an enterprise customer, an IoT domain, or some other convenient set of services (for example, mobility as a service). A network slice extends the access point name (APN) concept used in the mobile network today.

This architecture enables operators to offer optimal support for different types of services for different types of customer segments. The key benefit of network slicing technology is it enables operators to provide networks on an as-a-service basis, which enhances operational efficiency and resilient network services.

Several Security Issues/Threats pertaining to Network Slicing are as follows:

i. The primary factors leading to threats in network slicing is improper isolation between the network slices (Inter-Slice Isolation) and improper isolation between the components of the same slice (Intra-Slice Isolation). A threat could be migrated between the slices if one of the devices in the IoT slice gets infected by a malware using a vulnerability in the IoT device which can also impact the critical slices (such as V2X slice).

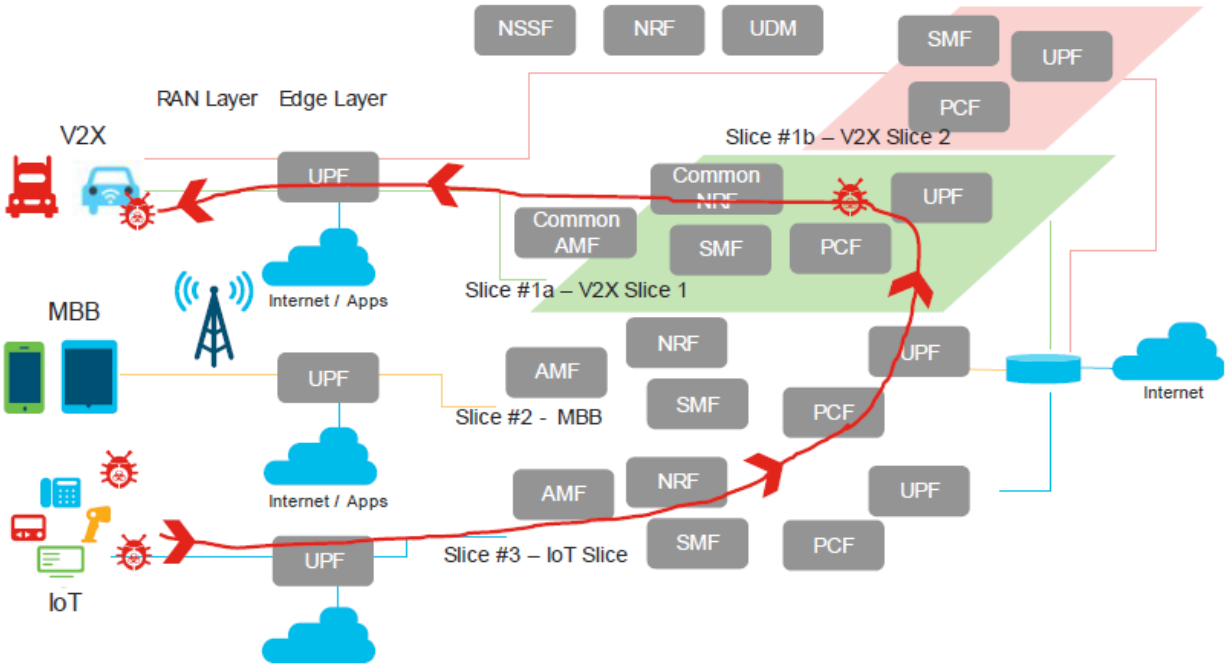

Fig 3: Network Slicing Security Threats (Source: The evolution of Security in 5G-5G America White paper)

As **per fig** 3 above, the attack can be increased by allowing the malware to have the ability to deplete the resources of the slice, subsequently causing DoS (Denial of Service) to the actual subscriber. An attacker may also exhaust resources common to multiple slices, causing denial of service or service degradation in other slices as well. This leads to severe degradation in the offered network services. As a cloud native architecture, 5GC (5G Core) has all the functions

virtualized that provide the added flexibility required for network slicing. However, this leads to another threat vector. Side channel attacks, coupled with improper isolation between network slices, may also lead to data exfiltration which may be proved as critical in sensitive parts of the mobile network such as billing, charging and subscriber authentication layers.

ii. As per Fig4 below, another scenario wherein the slices and the components within the slice are not adequately isolated, the attacker could access other slice components using the infected device or endpoint in another slice. In the below figure effected device is allowing the attacker access to the slice resources. Ultimately, the other slices are exposed and data exfiltration proceeds to an external server (a C&C centre, for example). Once the attacker gathers all the network's information behind the firewall, they could launch an attack on subscribers based on the leaked information. Furthermore, the attacker could use the information for fraudulent financial gains.

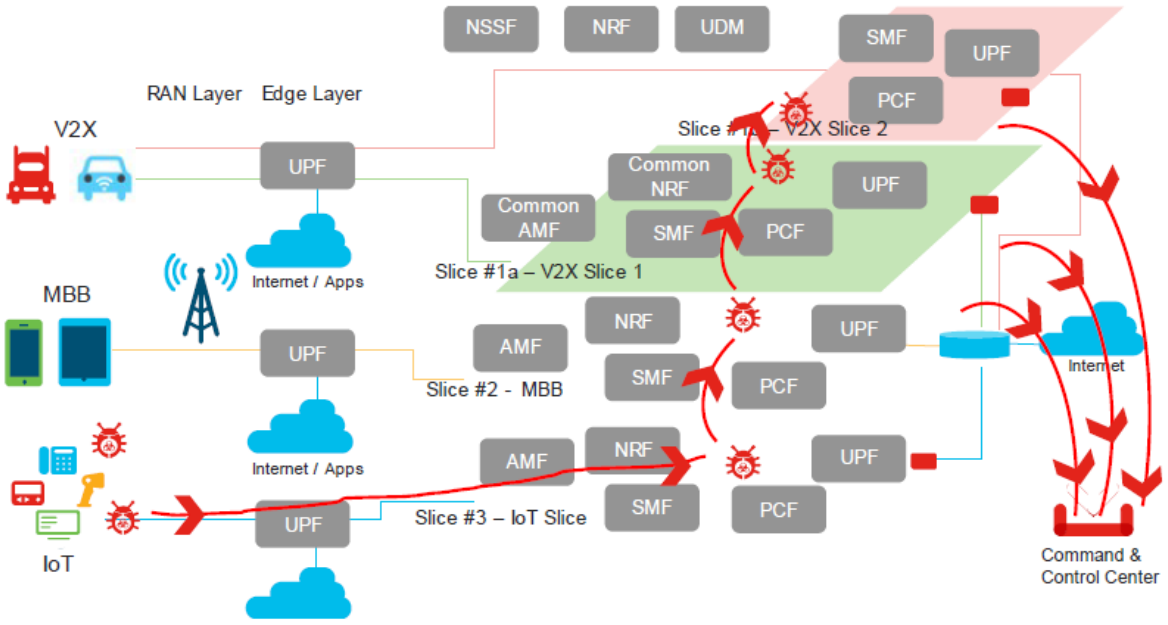

Fig 4: 5G Segmentation threat (Source: The evolution of Security in 5G-5G America White paper)

Through Network slicing customized service is being offered to customers based on operator's policies, to provide standardized APIs to create, modify, delete, monitor, and update the services of network slices. Hence slice Management contains adequate threat vectors if not secured properly.

Insufficient secure slice management interfaces, may provide attacker to gain access to the management interface. That access allows attackers to create network slice instances requiring significant network resources or a large number of network slice instances. As a result, the network resources are exhausted, leading to Denial of Service (DoS) attacks. Attackers could incite fraudulent activities, like false charging, by replaying management messages. An attacker may also eavesdrop on the transmission of supervision and reporting data and extract sensitive information to execute attacks of running network slice instances.

iii. 5G systems are fundamentally service-oriented. Different slices will be offered to different enterprise customer with different industry/vertical having diverse requirements. For eg , remote health care requires resilient security while IoT may only require lightweight security. Different E2E security capabilities may include strength of security algorithms, ways to derive and negotiate secret keys, and mechanisms for protecting confidentiality and integrity, etc.

Differentiated services running over individual network slices over a common infrastructure need isolation.

For virtual network slices each handling a different category of application that involve flexible resource orchestration—there is a clear need to isolate slices from each other. Resources (CPU, memory, storage, and etcetera) in use by one slice should not be accessed by infrastructure components serving other slices.

For instance, patients in a health care slice would prefer to only allow their doctors to access their health data. Such data should never be accessed by users in other slices. Note that the isolation criteria are equally applicable to virtual network slices with the same category of application. For instance, two healthcare enterprises A and B may be served by the same virtual network slice (or same category) but would require complete isolation of data from each other.

An attacker may adversely impact overall availability of resources common to multiple slices by exhausting specific resources in one slice, even with isolation. This would amount to a DoS attack with effects that permeate beyond the specific slice under direct attack.

iv. 5G architecture, especially 5G network slicing, is fundamentally designed to allow a wide variety of apps to thrive and grow. Apps served over E2E network slices would exchange a plethora of user device and network-specific information (user IDs, device IDs, user preferences, user locations, sensitive user information, financial/billing data, and etcetera). Potential erosion of privacy due to leakage of sensitive information between slices that coexist on the same infrastructure and must be adequately addressed.

v. Susceptibility to Side Channel Attacks: Side channel attacks occur when an attacker is capable of gathering actionable information about cryptographic secrets by observing the implementation of a platform (for example, power consumption, runtime, etc.) and exploit information to induce attacks or modify the cache. Many side channel attacks rely on statistical analysis of platform metadata that is typically exchanged (or available) in the clear. Network slices are susceptible to side channel attacks just like regular (non-virtual) platforms.

4.4 Multi Access Edge Computing Vulnerabilities:

Edge computing is an evolution of cloud computing that enables application hosting and data processing to move from centralized data centers to the network edge, closer to mobile applications and will play the critical role in 5G Service offerings. This will also help in reducing the latency. It decentralizes the data infrastructure so that the compute functions are pushed further to the network edge, closer to the data, in geographically separate areas.

ETSI has also prepared a set of technical standards for MEC which support multiple diverse technologies, including 5G NSA, distributed computing, and the virtualization of networking equipment and computing servers to ensure interoperability in an open ecosystem.

However due to heterogeneity and diversity of the MEC environment variety of new vectors for malicious attacks and privacy compromises that could constitute a major threat to the entire MEC system.

4.5 Distributed Core Attack Surfaces

Although the CUPS (Control and User Plane Separation) is not the strict 5G feature but it created the new trust boundaries and interfaces pertaining to separate control and user plane can be targeted to enable the launch of DoS and DDoS attacks as demonstrated in below figure.

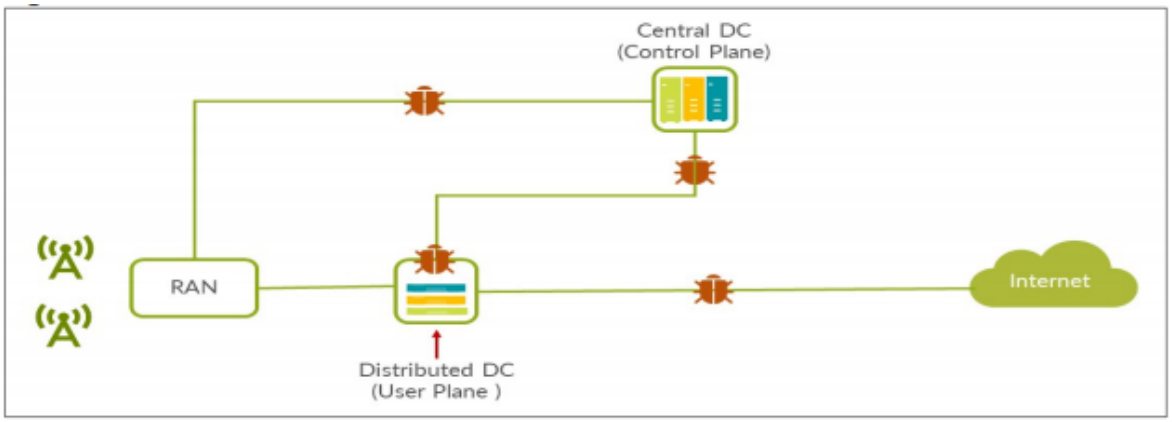

Fig 5: Source: 5G Security Strategy Considerations (Juniper Networks)

4.6 Virtualisation Threats:

While developing the management interfaces related to virtual functions, improper implementation related to NVF security functions may lead to vulnerabilities to access, storage and interception of Network Management data. Vulnerabilities related to improper layer protection for data transferred over internal interfaces, improper authorisation mechanisms on authorisation Server.

4.7 Software Defined Network Security Threats:

Network build using SDN and NFV differs from traditional networks and control is being transferred from single device controllers to distributed device controllers along with pooling of different infrastructures. Along with this switching to NFV/SDN causes the change is Network infrastructure and introduction of Network Orchestrator which can lengthen the chain of trust and introduction of new risks.

4.8 Other Vulnerabilities in Core Network:

The brief of some other Vulnerabilities which may arises due to flawed implementation in of Core Network are as follows:

i. Improper Protection of Service Based Interfaces:

Improper transport layer protection for NF mutual authentication and NF layer protection may lead to disclosure and tampering of sensitive information.

ii. Vulnerabilities due to weak implementation of AMF Security Functionalities:

Flawed AMF implementation can cause the security vulnerabilities in the following scenarios:

- If the gNB does not send the UE 5G security capabilities, the AMF cannot able to verify the 5G security capabilities same as the UE security capabilities that the AMF has stored, the attacker may force the system to accept a weaker security algorithm than the

system is allowed, forcing the system into a lowered security level making the system easily attacked and/or compromised.
Hence a flawed AMF implementation accepting insecure or invalid UE security capabilities may put User Plane and Control Plane traffic at risk, without the operator being aware of it.

- If NULL ciphering algorithm and/or NULL integrity protection algorithm of the UE security capabilities is accepted by the AMF, all the messages will not be confidentiality and/or integrity protected. The attacker can easily intercept or tamper control plane data and the user plane data. This can result in information disclosure as well as tampering of data.

iii. Vulnerabilities in implementation of UDM Security functionalities:

If the UDM does have the capability of storing the authentication status of UE, the increased home control of 5G could not be supported, which is useful in preventing certain types of fraud. For eg. In scenarios when a malicious AMF desires to access the system, it sends the request for its registration via a UE. In these cases, if the UDM does not stored the authentication status or incorrect authentication status, the registration request from malicious AMF may be accepted by UDM.

iv. Vulnerabilities in implementation of SMF security functionalities:

SMF verifies that the security policy received from the ng-eNB/gNB is the same as that stored locally at the SMF. If the SMF fails to check, security degradation of User Plane traffic may occur. For example, if the UP security policy received from the ng-eNB/gNB indicates no security protection, while the local policy mandates the opposite, and SMF uses the received security policy without validation, then the user plane data will be unprotected.

v. Vulnerabilities in implementation of NRF Security Functionalities:

If NF discovery authorization feature for specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices. This can result in reduced assurance level of slice data isolation, making the system vulnerable as well as wasting resource.

vi. Vulnerabilities in implementation of NEF Security Functionalities:

If the authentication of the Application Function is not supported, the application function without legal certificates, or pre-shared key could be able to establish a TLS connection with the NEF due to which the data stored in the NEF may be exposed to an unauthorized entity.

vii. Vulnerabilities in authentication and authorization of 5G Core components:

a. Usage of function without successful authentication on basis of user ID and authentication attribute (e.g. password, digital certificate) can be exploited in the system to introduce Vulnerabilities.
b. Level of authentication varies according to level of sensitivity of information. Improper implementation of strong security policy creates the possibility of accessing the resources by unauthorized entities.

c. In order to ensure session protection of 5G core components, the system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. A permanent exposed session increases the vulnerability of the system as an entry point for unauthorized person. Hence OAM user interactive session shall be terminated automatically after a specified period of inactivity.

viii. General Vulnerabilities of Network devices, Web Servers and Configuration etc. of 5G Core components:

The Security threats pertaining to Devices and Servers are also applicable in case of Network device and Web servers are as follows:

a. Lack of adequate mechanisms to filter incoming IP packets on any IP interface according to pre-defined rules make the network device vulnerable to denial-of-service attacks, degradation of services.
b. In the absence of effective GTP-C filtering mechanisms, the network device is vulnerable to Border gateway bandwidth saturation or GTP flood along with exposure to malformed GTP packets and denial of Service attacks.
c. The reachability of services should be restricted on the network product so that they can only be reached on interfaces where their usage is required. The absence of appropriate mechanisms exposes the services to risk of exploitation of known or unknown vulnerabilities by malicious entities.
d. Unused software components or parts of software which are not needed for operation or functionality of the network product may create an unnecessary attack surface and have a high susceptibility of falling outside patching and vulnerability management processes and therefore are increasingly exposed to malicious attacks and technical faults.
e. Unrestricted remote login for privileged users expose the network element to increased risk of unauthorized access and manipulation.
f. Kernel based Network functions which are not needed for the operation of the Network element may generate an attack surface. Some of the vulnerable services are IP Packet Forwarding between different interfaces of the same equipment, Proxy ARP (resource exhaustion attacks and man-in-the-middle attacks), Directed broadcast (Smurf, Denial of Service attack), IPv4 Multicast handling (smurf and fraggle attacks), gratuitous ARP messages (ARP Cache Poisoning attack).
g. Web servers can be configured to list the contents automatically of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analyzing and attacking those resources. It also increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps.
h. Unused File type or script-mappings of the web servers can be used in attacks based on delivery of malicious payloads, such as code-injection attacks.
i. Improper restriction of execute rights may lead to Remote Command Execution by unauthorized delivery of malicious payload through various vectors.
j. Improper restriction of access rights in servers may lead to remote Command execution by unauthorized delivery of malicious payload through various vectors.
k. Unused http methods in the servers provide an unnecessary attack surface that can lead to security compromise of the system.
l. Inadequate setting of access rights for web server configuration files may lead to unauthorized disclosure or modification of configuration information.

4 5G Threats Taxonomy:

The Security is defined on the basis of three principles which are defined as Confidentiality, Integrity and Availability. The brief of attacks/threats w.r.t affecting the security principles are as follows:

i. Loss of Availability:

The example of scenarios effecting confidentiality are as follows:

a. The availability of system may be compromised by attackers flooding the interface and network assets (AMF, AUSF) resulting in DDoS condition on the signaling plane. (e.g., multiple authentication failure on N1, N2 interface).
b. It may also be done by attacker crashing a Network element (e.g., AMF) by sending malformed packets.

ii. Loss of Confidentiality:

The scenarios effecting confidentiality are as follows:

a. Attackers eavesdrop on sensitive data on control and bearer plane to retrieve user location and device details and sensitive user data.
b. Data leakage due to unauthorized access to sensitive data (e.g., user profile) stored in UDR, UDSF.

iii. Loss of Integrity:

Integrity of system may be compromised in the following attack scenarios:

a. Attackers modify traffic information during transit in user plane interface N3 (SIP header modification, RTP spoofing)
b. Attackers modify data on network element (e.g., change the gNodeB configurations through admin interface)

iv. Loss of Control:

a. Attackers control the network via protocol or implementation flaw
b. Attacker's compromise of network element via management interface

v. Insider threats:

a. Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.

5 Security Controls in 5G:

As per 3GPP security architecture, the 5G architecture should have following Security controls:

i. AMF

a. The AMF shall verify that the UE's 5G security capabilities received from the target gNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as Generation of Alarm.
b. AMF shall support replay protection of NAS signalling messages between UE and AMF on N1 interface." as specified in TS 33.501.
c. To establish the NAS security context, the AMF shall choose one NAS ciphering algorithm and one NAS integrity protection algorithm. The AMF shall then initiate a NAS security mode command procedure and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE. The AMF shall select the NAS algorithm which has the highest priority according to the ordered list.
d. The Security Anchor Function should handle authentication failure message with synchronization failure (AUTS) from the UE, as to prevent possible exploitation from denial of service / resource exhaustion attacks / incidents. Complementary procedures have to be performed at USIM level.

ii. UPF:

a. Allocation and release of Network Tunnel Information is performed when a new PDU Session is established or released. This functionality is supported either by SMF or UPF, based on operator’s configuration on the SMF as specified in TS 23.501.

iii. SMF:

b. The SMF must provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure. In particular, The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target Gnb.

iv. NRF

a. NRF shall ensure that NF discovery request shall be authorized according to discovery configuration of the Network slice as specified in TS 33.501.

v. NEF

a. Integrity protection, replay protection, confidentiality protection should be implemented for communication between NEF and Application function.
b. Mutual authentication should be implemented between NEF and Application function.
c. The NEF should have the capability to determine whether the Application function is authorized to have the interaction with the Network functions.

vi. 5G Core components, web server, Network devices and Operating Systems

a. Cryptographically protected network protocols are used. The data transmission should be done using protocols with sufficient security measures.
b. The system shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.
c. The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented.
d. The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. The various user and machine accounts on a system shall be protected from being misused.
e. Strong password policy along with protection against brute force and dictionary attacks should be implemented.
f. The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. The network product shall be able to continue to operate without interactive sessions. An OAM user interactive session shall be terminated automatically after a specified inactivity period.
g. There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allow a user to gain administrator/root privileges from another user account without re-authentication.
h. Access to the webserver shall be logged. The web server log shall contain the following information: Access timestamp / Source (IP address) / (Optional) Account (if known) / (Optional) Attempted login name (if the associated account does not exist) / relevant fields in http request.
i. All incoming packets, from other network element, that are manipulated or differing the norm shall be detected as invalid and be discarded in such a manner that performance of element should not be effected.
j. For each message of a GTP-C-based protocol, a mechanism to check whether the sender of this message is authorized to send a message pertaining to this protocol be implemented.
k. Unused software components or parts of software which are not needed for operation or functionality of the network product shall not be installed or shall be deleted after installation.

l. The system shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to perform the actions.

vii. Network Slicing:

a. Network slicing platform manager along with host platform support mutual authentication and should be configured to perform the access authentication and authorisation in addition to primary authentication.
b. Appropriate logging and auditing mechanisms should be implemented throughout the slice life cycle. Real-time analysis of security events to immediately detect any attempted attack. Slice life-cycle includes the Preparation phase, Installation, Configuration and Activation phase, Run-time phase and Decommissioning phase.
c. Slices are end-to-end logical networks, so end-to-end security should be considered. All resources and network functions consumed by a slice should be monitored.
d. Proper isolation between distinct slices in the slice manager and restriction to perform changes on parameters shared among slices belonging to different tenants. Strong authentication and access control procedures must be in place. If a 5G customer device is allowed to simultaneously attach to multiple slices, isolation of data should be possible at the customer device end.
e. Isolation between Network slices is a key requirement and multi-layer isolation can be used to reduce the attack surface and lessen the impact. Examples of multi-layer isolation are NFVI boundary isolation, isolation of MANO system, security domain isolation, service instance isolation, VNF isolation.
f. Slices having different characteristics such as functionality level, sensitivity level should not be hosted on same hardware platforms to prevent side channel attacks.

viii. Network Function Vulnerabilities

a. Data transfer over internal interface of MANO should be done using an encrypted Network Protocols.
b. The confidentiality and data integrity of all messages shall be ensured by using TLS on each interface. The client and authorisation server along with resource server shall also mutual authenticate each other.
c. The 5G control plane should be configured in such a way that Network function can only communicate with the NF which they are intended to communicate with.
d. All control plane data in transit between hosts should be sent over an encrypted and authenticated channel using non-proprietary protocols.
e. The VNF shall synchronise with trusted time servers only.
f. The host system shall implement a strong key management system including key generation, key storage, key deletion and cryptographic processing.
g. The usage of a system function without proper authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented.

h. Strong Password policy should be implemented including the protection against brute force and dictionary attacks.
i. The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorisations to a system shall be restricted to a level and access be controlled to a specific user.
j. Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred.

ix. Software defined Networks (SDN):

a. Network providers should consider deploying encryption and authentication techniques to all SDN APIs.
b. Adequate security Mechanism should be implemented for integrity protection of configuration data stored in the SDN controller and configuration interfaces.
c. SDN control layer should have the functionality in the SDN control layer to authenticate the SDN Switch.
d. It is recommended to provide functionality in the SDN control layer to support hardware management to discover hardware failure automatically and recover from such a failure.

x. Multi-Access Edge Computing (MEC):

a. The confidentiality and data integrity of all messages shall be ensured by using TLS on each interface. The client and authorisation servers shall mutually authenticate. The client shall authenticate the resource server.
b. The mobile edge system shall allow the collection of charging-related information, log it in a secure way and make it available for further processing.
c. Security testing should be conducted to provide assurance that application vulnerabilities are identified and mitigated in a timely manner.
d. The mobile edge system shall provide a secure environment for running services for the following actors: the user, the network operator, the third-party application provider, the application developer, the content provider, and the platform vendor.
e. Strong Password policy should be implemented including the protection against brute force and dictionary attacks.
f. Access control mechanism should be implemented.

6 Conclusion:

Security Assurance is a continuous and evolving process. Also 5G will play pivotal role as critical infrastructure due to its varying use cases and therefore security assurance carries much more importance. Every new technology possesses security risks which are discovered and addressed in course of time.5G involves the usage of relatively new technologies in comparison with previous Generation Networks such as Network Slicing, Virtualisation which in addition of offering security advantage may create new platform of risks due to several use cases.

The gaps in security architecture developed by 3GPP may be covered in further releases to be freezed by 3GPP. Although 3GPP has developed security architecture for 5G but operators must need to regularly examine and implement 3GPP recommendations for ensuring the security in their Network.

Additionally, 5G is not only about the right security architecture. It requires building the secure workflows, procedures and collaboration across several stakeholders. A multi-stakeholder approach involving operators, vendors, regulators, policy makers and representatives of 5G users is fundamental to the security baseline of trustworthy, cost-efficient and manageable 5G networks. Due to level of complexity introduced by 5G, predefined security measures configured by 5G needs to be supplemented with dynamic security measures and behaviour-based checks should also be implemented at check points. Defences can be made more effective by properly segmenting the Network by operators so that operator can contain the threat if whole Network is compromised.

7 Glossary:

i. **AKA:** Authentication and Key Agreement Protocol
ii. **AMF:** Access and Mobility Function
iii. **API:** Application Programming Interface
iv. **APN:** Access Point Name
v. **ARP:** Address Resolution Protocol
vi. **AUSF:** Authentication Server Function
vii. **CPS:** Cyber Physical System
viii. **CUPS:** Control and User Plane Separation
ix. **DoS attacks:** Denial of Service attacks
x. **EAPAKA:** Extensible Authentication Protocol and Key Agreement
xi. **E2E:** End to End Network
xii. **EPS:** Evolved Packet System
xiii. **3GPP:** 3rd Generation Partnership Project
xiv. **GSM:** Global System for Mobile Communications
xv. **GTP:** GPRS Tunnelling Protocol
xvi. **GUI:** Graphical User Interface
xvii. **GUTI:** Globally Unique Temporary Identifier
xviii. **HSS:** Home Subscriber Server
xix. **IMSI:** International Mobile Subscriber Identity
xx. **IoT:** Internet of Things
xxi. **LTE:** Long Term Evaluation
xxii. **M2M:** Machine-to-Machine communication
xxiii. **MCC:** Mobile Country Code
xxiv. **MEC:** Multi-Access Edge Computing
xxv. **MNC:** Mobile Network Code
xxvi. **MVNO:** Mobile Virtual Network Operator
xxvii. **NAI:** Network Access Identifier
xxviii. **NAS:** Non-Access Stratus
xxix. **NEF:** Network Exposure Function
xxx. **NF:** Network Function
xxxi. **NFV:** Network Function Virtualization
xxxii. **NFV MANO:** Network Functions Virtualization Management and Orchestration

xxxiii. **NRF:** Network Repository Function

xxxiv. **OAM:** Oracle Access Management

xxxv. **PDU:** Protocol Data Unit

xxxvi. **PLMN:** Public Land Mobile Network

xxxvii. **QoS:** Quality of Service

xxxviii. **RBS:** Rogue Base Station

xxxix. **RRC:** Radio Resource Control

xl. **SA:** Service and System Aspects

xli. **SCA**-Side Channel Attacks

xlii. **SDN:** Software Defined Networking

xliii. **SEAF:** Security Anchor Function

xliv. **SEPP:** Security Edge Protection Proxy

xlv. **SIDF:** Subscriber Identifier De-Concealing Function

xlvi. **SUCI:** Socialist Unity Centre of India

xlvii. **SUPI:** Subscriber Permanent Identifier

xlviii. **SMF:** Session Management Function

xlix. **TLS:** Transport Layer Security

l. **TMSI:** Temporary Mobile Subscriber Identity

li. **UAV:** Unmanned Aerial Vehicles

lii. **UDM:** Unified Data Management

liii. **UDR:** User Data Repository

liv. **UDSF:** Unstructured Data Storage Function

lv. **UE:** User Equipment

lvi. **UMTS:** Universal Mobile Telecommunications System

lvii. VM-Virtual Machines

lviii. **VNF:** Virtualized Network Functions

8 References:

i. ETSI TS 133 501 V15.4.0: 5G; Security architecture and procedures for 5G System
ii. 5G PPP Phase1 Security Landscape by European Commission
iii. The Evolution of Security in 5G:5G Americas White Paper
iv. 5G Threat Landscape-ENISA
v. Security for 5G and Beyond- IEEE Communications Surveys & Tutorials by Finland
vi. 5G Security Issues by GSMA
vii. 5G security - enabling a trustworthy 5G system by Ericsson
viii. 5G Security Strategy Considerations by Juniper Networks
ix. 5G security - scenarios and solutions by Ericsson
x. An overview of the 3GPP 5G security standard by Ericsson