September 16, 2020

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

REPORT ON RISKS INTRODUCED BY 3GPP RELEASES 15 AND 16 5G STANDARDS

Working Group 3: Managing Security Risk in Emerging 5G Implementations

Table of Contents

Table of Figures

Table of Tables

1 Results in Brief

1.1 Executive Summary

5G is the fifth-generation mobile network that delivers higher multi-Gbps peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries (often referred to as "verticals"); Examples of which include connected vehicles, smart cities, industrial automation, eHealth, Internet of Things (IoT), and many others.

The FCC tasked CSRIC VII to evaluate the 3rd Generation Partnership Project (3GPP) Releases 15 and 16 standards, identify areas of risk, and develop risk mitigation strategies to minimize risk in core 5G network elements and architectures.

In developing 5G specifications the 3GPP group has addressed many of the security and privacy threats found in 4G LTE. This Report examines the new security enhancements of 5G New Radio (NR) and the new 5G Core network (5GC), with a primary focus on what is commonly referred to as the Standalone (SA) architecture.

The Report begins with a detailed background and related security activities in 3GPP, previous CSRIC groups, and other organizations. Next, an analysis of key features of 5G is performed to identify any potential areas of risk. Finally, the report concludes with several Recommendations on how to mitigate potential 5G security threats, as well as proposed future work. Additional work on optional 5G features related to security and privacy will be the focus of our second report.

2 Introduction

5G wireless and network technology is enabling a new wave of innovation that will impact many aspects of people's lives from connected vehicles to healthcare and internet of things. To meet this need, not only is it critical that 5G networks are highly capable and reliable, it is essential that they are highly secure, ensuring the confidentiality and integrity of their intended use.

5G New Radio (NR) is the global standard for a unified, more capable 5G wireless air interface. It will deliver significantly faster and more responsive mobile broadband experiences and extend mobile technology to connect and redefine a multitude of new industries.

In addition to a more advanced air interface a new 5G Core network (5GC) has been defined that allows many different functions to be built, configured, connected, and deployed at the required scale in a programable and flexible manner, to meet the need at any given time. 5GC also brings the ability to develop new functions easily, reduce time-to-market for new services, incorporate off-the-shelf technology, leverage IT-Industry virtualization capabilities to drive changes in the network functions themselves. The result is a migration away from telecom-style protocol interfaces towards web-based APIs and services. This so called "Service-Based Architecture" (SBA), is centered around services that can register themselves and subscribe to other services. This enables a more flexible development of new services, as it becomes possible to connect to other components without introducing specific new interfaces.

The initial capabilities were developed by 3GPP in Release 15 of their specifications, and has been further enhanced in Release 16 finalized in the June 2020 timeframe.

While security and privacy are an important aspect of the specifications produced by 3GPP there are always potential risks when introducing new core and radio technology and 5G is no different. This report aims to highlight some of the new network elements, features, functions, and capabilities introduced by 5G, and where possible identify what appropriate mitigation can be undertaken.

2.1 CSRIC VII Structure

CSRIC VII was established at the direction of the Chairman of the FCC in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairman of the FCC.

Communications Security, Reliability, and Interoperability Council (CSRIC) VII					
CSRIC VII Working Groups					
Working Group 1: Alert Originator Standard Operating Procedures	Working Group 2: Managing Security Risk in the Transition to 5G	Working Group 3: Managing Security Risk in Emerging 5G Implementations	Working Group 4: 911 Security Vulnerabilities during the IP Transition	Working Group 5: Improving Broadcast Resiliency	Working Group 6: SIP Security Vulnerabilities
Chair: Craig Fugate, America's Public Television Stations	Chair: Kathy Whitbeck, Nsight	Chair: Farrokh Khatibi, Qualcomm	Chair: Mary Boyd, West Safety Services	Chair: Pat Roberts, Florida Association of Broadcasters	Chair: Danny McPherson, Verisign
FCC Liaison: James Wiley	FCC Liaison: Kurian Jacob	FCC Liaison: Steven Carpenter	FCC Liaison: Rasoul Safavian	FCC Liaison: Robert "Beau" Finley	FCC Liaison: Ahmed Lahjouji

Table 1 - Working Group Structure

2.2 Working Group 3 Team Members

Working Group 3 consists of the members listed below.

Name	Company
Farrokh Khatibi* - Chair	Qualcomm Technologies, Inc.
Billy Bob Brown, Jr	CISA DHS
Brian K. Daly*	AT&T Services Inc.
Christopher Joul	T-Mobile
Mohammad Khaled	Nokia Bell Labs

Michael Liljenstam	Ericsson
John Marinho	CTIA
Danny McPherson*	Verisign
Susan M. Miller*	ATIS
Travis Russell*	Oracle Communications
Greg Schumacher	T-Mobile
D.J. Shyy	MITRE
Lee Thibaudeau*	Nsight
Brian Trosper*	Verizon
Steve Watkins*	Cox Communications
Jeffrey Wirtzfeld	CenturyLink
Fei Yang	Comtech
Steven Carpenter	FCC

Table 2 - List of Working Group Members

* CSRIC Members

The Working Group members had an option to nominate an alternate to participate in the discussions when they were unavailable. Although these alternates are not a member of the Working Group and may not vote, they provided valuable input towards the completion of this report that should be acknowledged. Working Group 3 alternate members are listed in Table 3.

Name	Company
Steve Barclay	Alliance for Telecom Industry Solutions (ATIS)
Vinod Choyi	Verizon
Martin Dolly	AT&T Services Inc.
Yong Kim	Verisign
Kathleen Whitbeck	Nsight

Table 3 - List of Working Group Alternate Members

The Working Group members had several subject matter experts presenting material relevant to the group's scope and charter. The subject matter experts are listed in Table 4.

Name	Company	Topic
Alper Kerman	NIST	Zero Trust Architecture
Peter Schneider	Nokia Bell Labs	Network Slicing Security
Peter Thermos John Kimmins	Palindrome Technologies	5G Mobile Security Technology & Services – Cybersecurity Perspective
Syed Rafiul Hussain	Purdue University	LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE
James Scuse	GSMA	GSMA's CVD Programme: 4G & 5G submissions

Table 4 - List of Subject Matter Experts

3 References

[Ref 1] 3GPP TS 23.501, "System architecture for the 5G System (5GS)".[1]

[Ref 2] 3GPP TS 23.502, "Procedures for the 5G System (5GS); Stage 2".[1]

[Ref 3] 3GPP TS 33.501, "Security architecture and procedures for 5G system".[1]

[Ref 4] 3GPP TS 38.300, "NR; Overall description; Stage-2".[1]

[Ref 5] 3GPP TS 38.331, "NR; Radio Resource Control (RRC); Protocol specification".[1]

[Ref 6] 3GPP TS 33.210, "Network Domain Security (NDS); IP network layer security"[1]

[Ref 7] CSRIC VI , "Final Report – Recommendations to Mitigate Security Risks for Diameter Networks" version 1.1, March 14th, 2018[2]

[Ref 8] IETF News, "5G and Internet Technology", Jari Arkko (IAB Member) and Jeff Tantsura (IAB Member), 16 Jun 2017.

[Ref 9] Syed Rafiul Hussain, Mitzi Echeverria, Omar Chowdhury, Ninghui Li, Elisa Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," Proceedings of Network and Distributed System Security Symposium (NDSS) 2019, San Diego, 2019.[3]

[Ref 10] Singla, Ankush & Hussain, Syed & Chowdhury, Omar & Bertino, Elisa & Li, Ninghui, (2020). Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks. Proceedings on Privacy Enhancing Technologies. 2020. 126-142. 10.2478/popets-2020-0008.[4]

[Ref 11] Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft).[5]

[Ref 12] M. Lokshin, S. Azari, D. Newsom, "Quality of Open Source Software: how many eyes are enough?", Jan. 2019[6]

[Ref 13] ETSI GS NFV 002 V1.2.1, "Network Functions Virtualisation (NFV); Architectural Framework"[7]

[Ref 14] ETSI GS NFV-EVE 005 V1.1.1, "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework"

[1] This document is available from the Third Generation Partnership Project (3GPP) at: http://www.3gpp.org/specs/specs.htm.
[2] https://www.fcc.gov/files/csric6wg3finalreport32018pdf
[3] https://www.ndss-symposium.org/wp-content/uploads/ndss2019_05B-5_Hussain_slides.pdf
[4] This paper is available at: https://www.researchgate.net/publication/338475577_Protecting_the_4G_and_5G_Cellular_Paging_Protocols_against_Security_and_Privacy_Attacks/fulltext/5e169cf24585159aa4bffd8c/Protecting-the-4G-and-5G-Cellular-Paging-Protocols-against-Security-and-Privacy-Attacks.pdf
[5] https://csrc.nist.gov/publications/detail/nistir/8259/draft
[6] https://blogs.worldbank.org/opendata/quality-open-source-software-how-many-eyes-are-enough
[7] https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

4 Objective, Scope, and Methodology

4.1 Objective

The FCC directed CSRIC VII to review risks to 5G wireless technologies that can lead to the loss of confidentiality, integrity, and availability of wireless network devices. CSRIC VII will recommend best practices to mitigate the risks for each vulnerability it identifies and address recently proposed solutions by security researchers.

Additionally, the FCC directed CSRIC VII to recommend any updates, if appropriate, to the 3GPP SA3 (security working group) standards, including digital certificates and pre-provisioned Certificate Authorities, to mitigate these risks and then place the vulnerabilities on a scale that accounts for both risk level and remediation expense.

Finally, the FCC directs CSRIC VII to identify optional features in 3GPP standards that can impact the effectiveness of 5G security, and recommendations to address these gaps.

The objective of this Report is to provide the following deliverables with the focus on the 5G Standalone architecture:

- Review lessons learned from the previous generation of wireless technology (4G)
- Gather input from researchers, technologists and thought-leaders, Standard Organizations
- Perform an assessment of implementation best practices and evaluate specific options
- Identify updates needed to the existing body of knowledge
- Identify barriers to implementation
- Advise & recommend accordingly

4.2 Scope

The scope of this report is to address a risk assessment for 5G wireless technology as defined in 3GPP specifications. Additionally, the report provides recommendations to mitigate the identified risks, corresponding best practices as well as possible areas for future consideration. The analysis and assessment are based upon industry best practices and standards including the National Institute of Standards and Technology (NIST) and (International Organization for Standardization) ISO Standards.

Although CSRIC VII reviewed the security of all options identified in 3GPP specifications, the primary focus of CSRIC VII is the options with 5GC, especially option 2 (see Figure 1). CSRIC VII also considered transitional security threats from the 5GC perspective.

Furthermore, when a carrier has a combination of EPC and 5GC core networks, CSRIC VII conducted a security assessment with respect to interworking between the two core networks. CSRIC VII, WG2's focus has been on the enhancements needed in EPC to support a secure interworking, while CSRIC VII WG3's has been primarily focused on the security requirements

in 5GC in this scenario.

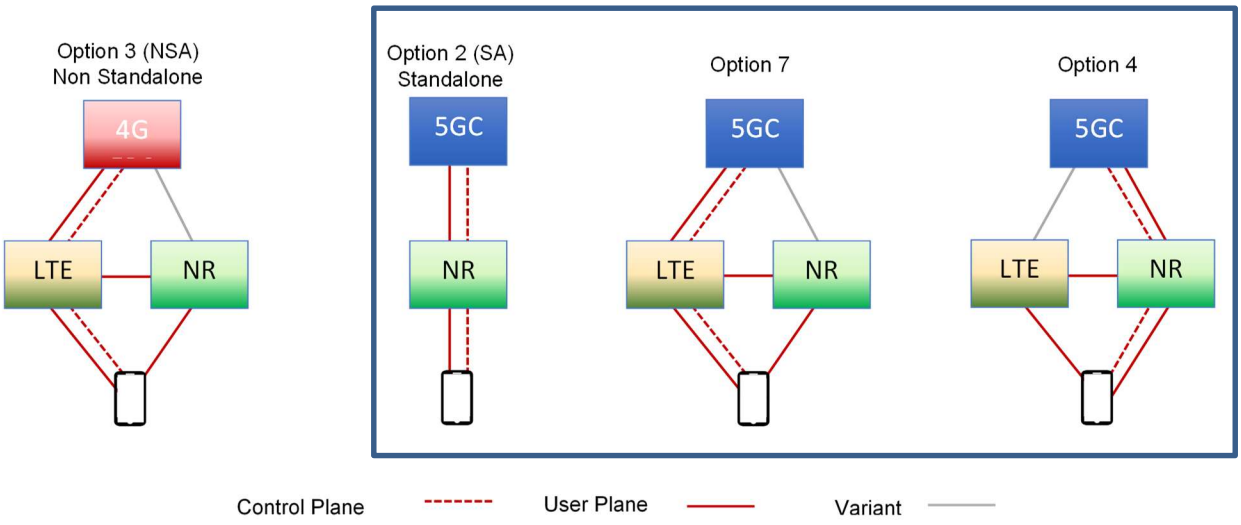


Figure 1 - Scope of CSRIC VII, WG3

4.3 Methodology

CSRIC VII, WG3 was asked to examine the security risks associated with 5G that result from both infrastructure and device capabilities that may introduce incremental security risk. The 3GPP, as well as several other standards organizations, continues work on 5G standards. A full 5G core will not be likely until after 2020, and even then, on a limited basis. Wide scale deployment of the 5G core will take time, as we have seen with other technologies (including 4G). As a result, the body of work on threats, risks and best practices to mitigate risk to 5G networks is still maturing. To address this limitation, we relied upon several sources to compile the data to identify and evaluate the emerging security risks anticipated in the transition to 5G, including:

- Industry SME presentations
- Standards bodies and industry associations (GSMA, CTIA, ETSI, 3GPP, NIST, ISO)
- Individual contributor research gathered by Working Group members
- Academic papers

Some of the specific topics under consideration by CSRIC VII arise because of the migration away from traditional, engineered systems designed to support specific network functions to a more distributed, Service Based Architecture (SBA) including virtualization technologies. This new architecture exposes telecom networks to new attack vectors stemming from the adoption of IT technologies. As a result, the research into 5G technologies, IoT, NFV/SDN, etc. are influenced by body of work addressing risk mitigation in the IT domain where these capabilities have existed for a number of years.

The methodology used in this Report is based on NIST SP 800-39[8] as shown in Figure 2. In order to frame the 5G security risks, risk context must be framed, the corresponding risks must

[8] https://csrc.nist.gov/publications/detail/sp/800-39/final

be assessed, risk response recommendations must be identified, and ongoing monitoring must be performed.

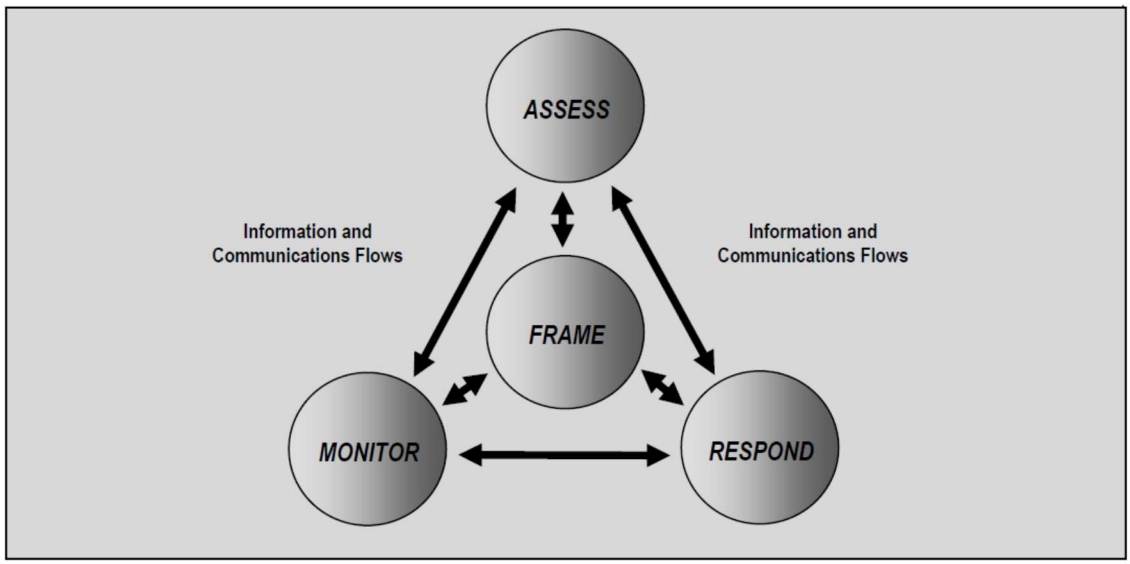


Figure 2 - NIST SP 800-39 Managing Information Security Risk, Risk Management Process

5 Background and Related Security Activities

In this section we provide some background and related security activities.

5.1 3GPP

5.1.1 General Architecture

The 5G Core Network (5GC) evolution from the 4G Core architecture is shown in Figure 3. The evolution shows the migration from the traditional 4G point-to-point configuration to an architecture that is based on functional interconnections through a "common bus" approach that permits functional elements to communicate based on service definition. The architecture is called a Service Based Architecture (SBA), where key differentiators include:

- Service Based Architecture (SBA)
  - Direct and Indirect communication and delegated discovery through Service Communication Proxy
  - Introduction of NF Set and NF Service sets – For 5GC the control plane functionality and common data repositories of a 5G network are delivered by way of a set of interconnected Network Functions (NFs), each with authorization to access each other's services or sets of services.
  - Selection and reselection within NF Set – The 5GC employs a centralized discovery selection framework that leverages a NF Repository Function (NRF). The NRF maintains a record of available NF instances and their supported

services. It allows other NF instances to subscribe and be notified of registrations from NF instances of a given type. The NRF supports service discovery, by receipt of Discovery Requests from NF instances and details which NF instances support specific services.

  - Convert IMS interfaces to utilize SBA – The 5GC provides the mechanism to convert today's IP Multi-Media Sub-system (IMS) to use of a Services Based Architecture (SBA) that provides flexibility and scale in service delivery as well as support for new capabilities such as Network Slicing.

- Network Slicing - Network slicing is a fundamental new capability of 5GC that provides flexibility when deploying diverse network services and applications. A logical end-to-end network slice has pre-determined service capabilities, traffic characteristics and service level agreements and includes the virtualized resources required to service the needs of a group of subscribers, including a dedicated User Plane Function (UPF), Session Management Function (SMF) and Policy Control Function (PCF). Key capabilities include:
  - Slice specific authentication and authorization
  - Improvements in slice interworking with EPC

  Additional details available in Clause 6.1.4.
- Control Plane/User Plane (CP/UP) Split- 5G standards require the separation of the Control and User Planes (traffic paths within the 5G architecture) within the network. The separation is driven by the notion that user-plane and control plane functionalities are quite different given the performance characteristics of exchanging signaling messages between network control functions and the needs of a transport network that carries user/application traffic.
- Integration of cloud/edge computing – The integration of cloud and edge computing is another new fundamental capability in 5G. The capability no longer relies on centralized, cloud-based computing, and instead utilizes cloud capabilities at the edge of the network to deliver real-time performance and reduced latency.
- Flow based QoS – Quality of Service (QoS) in 5G is flow based, rather than bearer based as in 4G. Packets are classified and marked using QFI (QoS Flow Identifier). The 5G QoS flows are mapped in the RAN to DRBs (Data Radio Bearers) unlike 4G LTE where mapping is one to one between EPC and radio bearers.

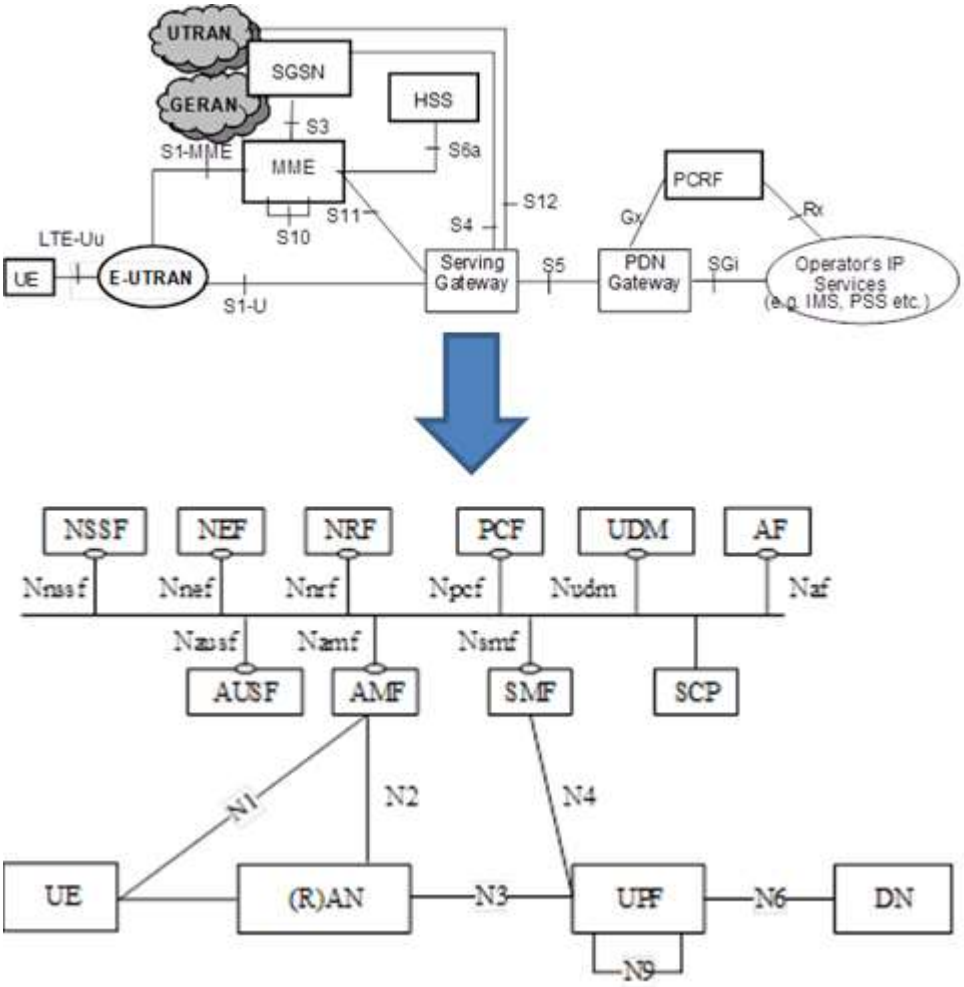


Figure 3 - 5G Core Network Evolution

Figure 4 illustrates a few of the options considered in 3GPP.

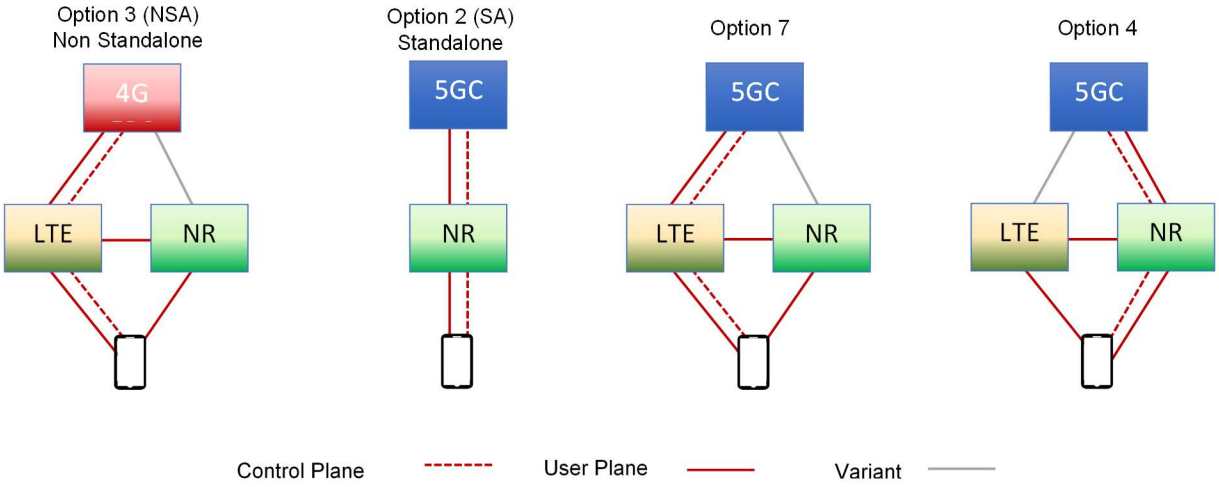


Figure 4 – A Few of the Core Network Options Considered in 3GPP

As described in Figure 4, in previous networks, network appliances connect to one another using point-to-point interfaces. In voice services, there are specific network functions that are used for every voice call. Likewise, in data sessions there are specific network appliances that support every data session. As an example, this proves problematic for Internet of Things (IoT), where support of billions of devices trying to send simple data sets to an application do not need all of the functionality provided in traditional networks. This is one of the drivers to moving to SBA.

SBA has been around for some time, where Web applications use SBA to deliver services through Web applications. This concept has been adopted by the 3GPP and used in 5G where network functions are delivered as services, as needed.

To accomplish this, traditional signaling such as SS7 or Diameter is almost eliminated (see section 5.17 for some legacy signaling impacts). There is no need for complex signaling protocols with specific message sets defined for each function. In place, each network function is able to advertise the services it can provide to the network and when a specific function is needed to support a session, the device is able to connect to the function through a common RESTful API using HTTP commands.

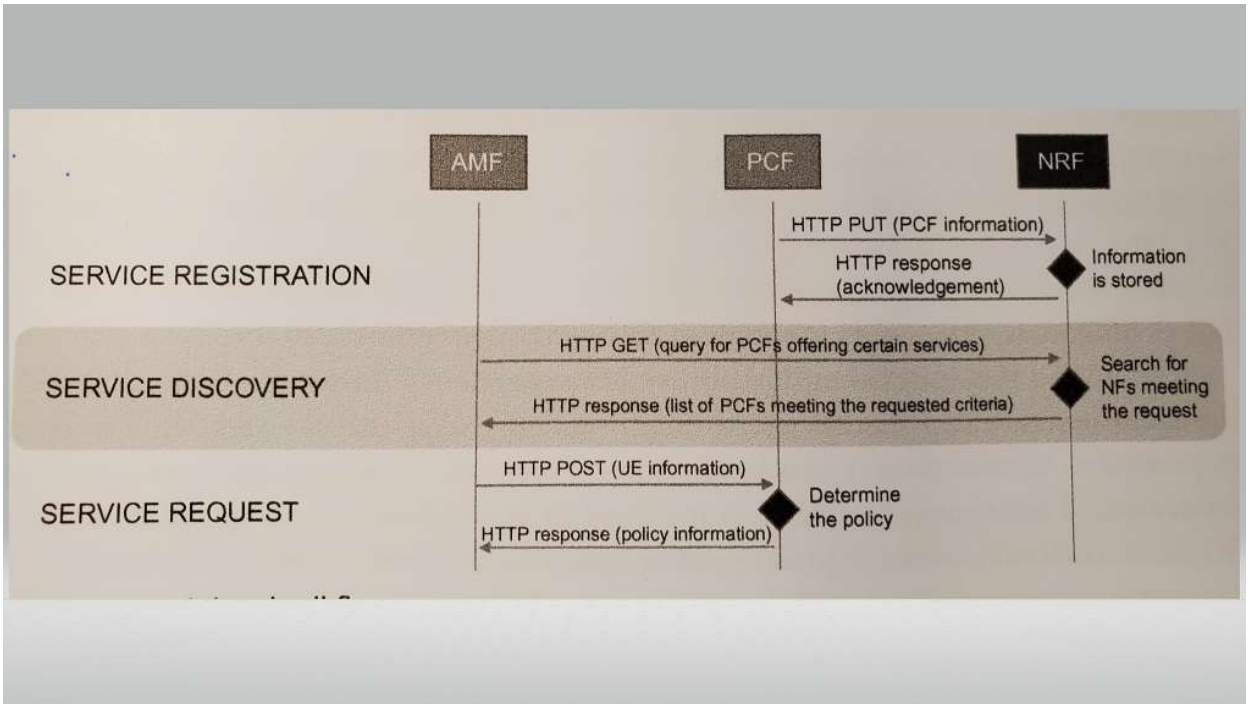


Figure 5 - Consolidated SBA Call Flow[9]

As shown in Figure above, there are three basic steps in a service; service registration by each of the Network Functions (NF), service discovery by NF, and service request by NF.

Service registration is the process used by each NF to register with the network and provide its capabilities, as well as services offered by the NF. This is stored in the NRF and used by devices requesting network services. Service discovery is used by devices that are requesting services from the network. Depending on the type of session, the request will ask for specific types of network services, such as policy or network slice selection. A service request is sent by the device to request services from the network such as connection request.

In a "pure" 5GC, all of the signaling in the network core is done through HTTP over RESTful APIs. The latest version of HTTP is currently being ratified for use in 5G networks as part of the R16 specifications. HTTP/3 uses QUIC rather than TCP services. QUIC emulates the connection-oriented services of TCP over a UDP connection, eliminating the added latency found in TCP.

5.1.2 5G Core Enhancements versus 4G EPC

- Introduction of Security Edge Protection Proxy at PLMN border
  - Application layer security for information exchanged between Network Functions in different PLMNs
- Subscriber Identifier Privacy
  - Use of the home network public key to encrypt the MSIN part of the subscriber

[9] 5G Core Networks: Powering Digitalization, S. Rommer, P. Hedman, M. Olsson, L. Frid, S. Sultana, C. Mulligan, London, UK, Elsevier, Academic Press, 2020

identifier, IMSI, so that it is protected over the air

- Anti-Bidding Between Architectures (ABBA)
- Introduction of Security Anchor Function (SEAF) or anchor key concept
    - Allows for re-authentication of the UE when it moves between different access networks or even serving networks without having to run the full authentication (e.g., AKA authentication). This reduces the signaling load on the home network (HSS/UDR) during various mobility scenarios
- Unified Authentication Framework
    - Access-agnostic authentication. Use of the same authentication methods for both 3GPP and non-3GPP access networks
    - Native support of EAP (allows for ability to plug-in new authentication methods in future without impacting the serving networks)
- Increased home network control for authentication
    - Ability for the home network to verify that the UE is actually present and requesting service from the serving network. This may be useful in certain roaming scenarios (e.g., a roaming operator claims that the UE is roaming into their network when in fact it is not)
- Authentication and Authorization between NFs over SBI
    - Mutual Authentication between NFs shall be based on client-side and server-side certificates by means of either TLS 1.2 or TLS 1.3 when transport layer protection is used. In indirect communication scenarios, where an SCP is used as intermediate proxy, the NF Service Consumer (NF-C) and NF Service Producer (NF-P) shall use implicit authentication by relying on authentication between NF-C and SCP, and between SCP and NF-P. In case, additional authentication of the NF-C is required based on operator policy, a client credential assertion (CCA) may be used which is generated by the NF-C using its private key for access token request to the NRF. Additionally, the NF-P may authenticate the NF-C at the application layer using the CCA.
    - If the PLMN uses token-based authorization, then the authorization framework relies on the OAuth 2.0 framework as specified in RFC 6749. The grants provided shall be of the type "client credential grant, as described in clause 4.4 of RFC 6749 and the access tokens shall be JSON Web Tokens (JWT) as described in RFC 7519. The JWT shall be secured with digital signatures or message authenticate codes based on JSON Web Signature (JWS) as described in RFC 7515. If token-based authorization is used, then the network shall use protection at the transport layer by means of TLS.
- Secondary Authentication
    - As an implementation option the 5GC provides capabilities to perform secondary authentication (i.e., a second authentication level occurring after successful primary mutual authentication of the UE and network), to support enhanced security and verification when user devices access services provided by external networks.
    - Secondary authentication is based on EAP protocols using a method that is determined and controlled by the external network, where an external DN-AAA acts as the authentication server; The credentials used for secondary authentication

are different from the ones used for primary authentication and are controlled by the external network.

- Release 15 of the 3GPP specifications describe how secondary authentication is performed on a per PDU session basis for a specific DNN; Release 16 of the 3GPP specifications expands on the capabilities to allow for slice-specific authentication.

5.1.3 5G RAN

Interference mitigation is listed as one of the key issues in 3GPP TR33.809 (Study on 5G NR Security Enhancement Against False Base stations). A few 5G new radio (NR) techniques are mentioned as potential mitigation techniques including beamforming and RAN slicing. The vulnerabilities of 4G LTE to interference are well documented.[10] The 4G LTE vulnerabilities on physical channels and signals include:

- Synchronization signals (primary and secondary) are at the fixed locations of the 2-dimensional orthogonal frequency division multiplexing (OFDM) resource grid.
- Master Information Block (MIB) inside Physical Broadcast CHannel (PBCH) is at a fixed location.
- Cell-specific Reference Signal (CRS) is at fixed locations although the specific locations are a function of the Physical Cell ID (PCI).
- The downlink Physical Control Format Indicator Channel (PCFICH) is at a fixed location.

In general, 4G LTE design in the frame structure is rigid and transmissions of broadcast messages and signals are repetitive. However, 5G NR design is highly flexible and transmissions of broadcast messages and signals are mostly on-demand such that various use cases (e.g., eMBB, URLLC and massive IOT) can be supported.

The following presents some improvements of 5G NR over 4G LTE. These improvements can be leveraged to provide interference mitigation. For each improvement, the operation in 4G LTE is described to establish the baseline.

In 4G LTE, the Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and PBCH are always located in the center of the downlink channel bandwidth. PSS and SSS are used to assist the UE to acquire time and frequency synchronization with a cell and detect its Physical Cell ID (PCI). After the UE detects the PCI, the UE completes the cell search. The PBCH is adjacent to the PSS and MIB is carried inside the PBCH. In each 10 ms frame, there are two occurrences of PSS/SSS where PBCH is associated with just one PSS/SSS. The pattern for transmissions of PSS/SSS and PBCH (i.e., the locations of the signals and channels within a frame) is always fixed. After UE acquires MIB, it decodes system information blocks (SIBs) on the downlink to understand the cell configurations and prepare for establishing radio resource control (RRC) connections.

For 5G NR, its MIB is part of synchronization signal block (SSB) which consists of all three:

[10] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," IEEE Communications Magazine, vol. 54, no. 4, 2016.

PSS/SSS/PBCH. The numerology (μ) and cell operating frequency determine the transmission pattern of SSB. SSB is not always in the center of the channel bandwidth. 5G NR has a new concept called the synchronization raster that indicates the candidate frequency locations of SSBs when explicit signaling of the SSB position is not present. Numerology (μ) defines the OFDM configurations: 0 – 4 where 0 is the same as LTE. When μ becomes larger, wider subcarrier spacing, shorter symbol duration, and more slots per frame.

The 4G LTE Cell-specific Reference Signals (CRSs) are sent continuously on the downlink. They are transmitted on equally spaced subcarriers at the first and third from last symbol of each slot. RSs are sent on every sixth subcarrier. The starting position of RSs on the frequency domain is a function of PCI. In 5G NR, the CS-RSs are eliminated. 5G NR introduces new types of RSs and RSs are sent on-demand.

In 4G LTE, the PCFICH (downlink channel) indicates the amount of resource in the time domain for control channels to use, i.e., it indicates the size of control region. PCFICH is always at the beginning of a downlink subframe. In 5G NR, this channel is eliminated.
In 4G LTE, the PHICH (downlink channel) transmits Hybrid-ARQ (H-ARQ) acknowledgements responding to uplink shared channel transmissions. Its symbol location is always at the beginning of a downlink subframe. In 5G NR, the HARQ is asynchronous so there is no need for a dedicated channel to handle acknowledgements. As a result, the PHICH is removed.

In 5G NR, a Bandwidth Part (BWP) is a set of contiguous physical resource blocks (PRBSs) within a given frequency carrier using a given numerology for a UE to receive and send user applications, where the BWP is ≤ operating carrier bandwidth. Instead of using the whole channel bandwidth of the operating carrier for UEs to communicate with the 5G NR base station (gNB), a UE uses a BWP. Flexibility in BWP allows vendors to build different categories of UEs (e.g., supporting different sizes of BWP) and those UEs will still work in any 5G NR cell whose channel bandwidth may be much larger than the BWP. In addition, BWPs allow for asymmetric allocation of channel sizes for UL/DL of a 5G NR connection which is not possible in LTE.

5G NR also supports antenna beamforming capability whose beam directivity can be used to mitigate interference.

A comparison of the differences in channels and signals between 4G LTE and 5G NR is summarized in Table 5.

Table 5 - Differences in Channels and Signals Between 4G LTE and 5G NR

	5G NR	4G LTE
PCFICH, PHICH and cell-specific reference signal (CRS)	Eliminated	At fixed location of two-dimensional resource grid
Synchronization Signals and Master information block (MIB)	The location is a function of numerology or configured by higher layer	Fixed in center of channel bandwidth
Channel Bandwidth	Variable via the use Bandwidth Part (BWP) Asymmetric for uplink / downlink	Fixed Symmetric for uplink / downlink
Beam	Multiple Beams	Does not exist

5.1.4 3GPP SA3 (Security) Standards

The 3GPP standards process is an ongoing effort that will continue to release updates for adoption. This specification defines the security architecture (i.e., the security features and the security mechanisms for the 5G system and the 5G core) and the security procedures performed within the 5G system including the 5G core and the 5G NR. Here are the main features defined in TS 33.501 [Ref 3].

5.1.4.1 Increased Home Control

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

This was added in answer to the vulnerabilities found in 3G and 4G networks where networks could be spoofed and send false signaling messages to the home network in an effort to request the IMSI and location of a device. This information could then be used to intercept voice calls and text messages.

5.1.4.2 Unified Authentication Framework

In 5G networks, authentication will be access agnostic. The same authentication methods are used for both 3GPP and non-3GPP access networks (5G radio access and Wi-Fi access, for example).

Native support of EAP is key. This allows for new plug-in authentication methods to be added in the future without impacting the serving networks.

5.1.4.3 Security Anchor Function (SEAF) and Authentication Framework

5G introduces the concept of an anchor key, with the new function of the SEAF. The SEAF is co-located with the AMF in release 15 of the 5G network specifications. The SEAF allows for

the re-authentication of the device when it moves between different access networks, or even serving networks without having to run the full authentication method (e.g., Authentication and Key Agreement (AKA) authentication). This reduces the signaling load on the home network HSS during various mobility services.

The purpose of the primary AKA procedures is to enable mutual authentication between the user equipment and the network that provides keying material reuse between the user equipment and the serving network in subsequent security procedures. The keying material generated by the primary AKA procedure results in an anchor key called the K_{SEAF} provided by the Authentication Server Function (AUSF) of the home network to the SEAF of the serving network.

Keys for more than one security context can be derived from the anchor key without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the user equipment and a non-3GPP inter-working function used in untrusted non-3GPP access.

The user equipment and the serving network support both EAP-AKA' and 5G AKA authentication. This is an improvement from previous generations of wireless where different encryption schemes were used depending on the access. In 5G, these two methods are used regardless of the access type, and are the only methods supported.

As a result of a successful primary authentication of a UE, an intermediate key, K_{AUSF} is generated irrespective of whether 5G-AKA or EAP-AKA' authentication method is used and may be stored securely at the AUSF and at the UE until a new primary authentication is performed. An anchor key, K_{SEAF}, which is bound to the serving network is generated by the AUSF from the K_{AUSF} and provided to the serving network.

The SEAF generates a K_{AMF}, which is then used to generate NAS protection keys (NASint, NASenc) similar to what occurs in 4G and access network keys: K_{gNB}, K_{N3IWF}, which are then provided to the appropriate gNB and N3IWF functions respectively. A feature of the 5G key hierarchy, as shown in Figure 6, is the ability to protect the integrity of user plane traffic by using K_{UPint}. Another feature is the ability to use, the K_{N3IWF} for generation of keys used to protect connection over non-3gpp access.

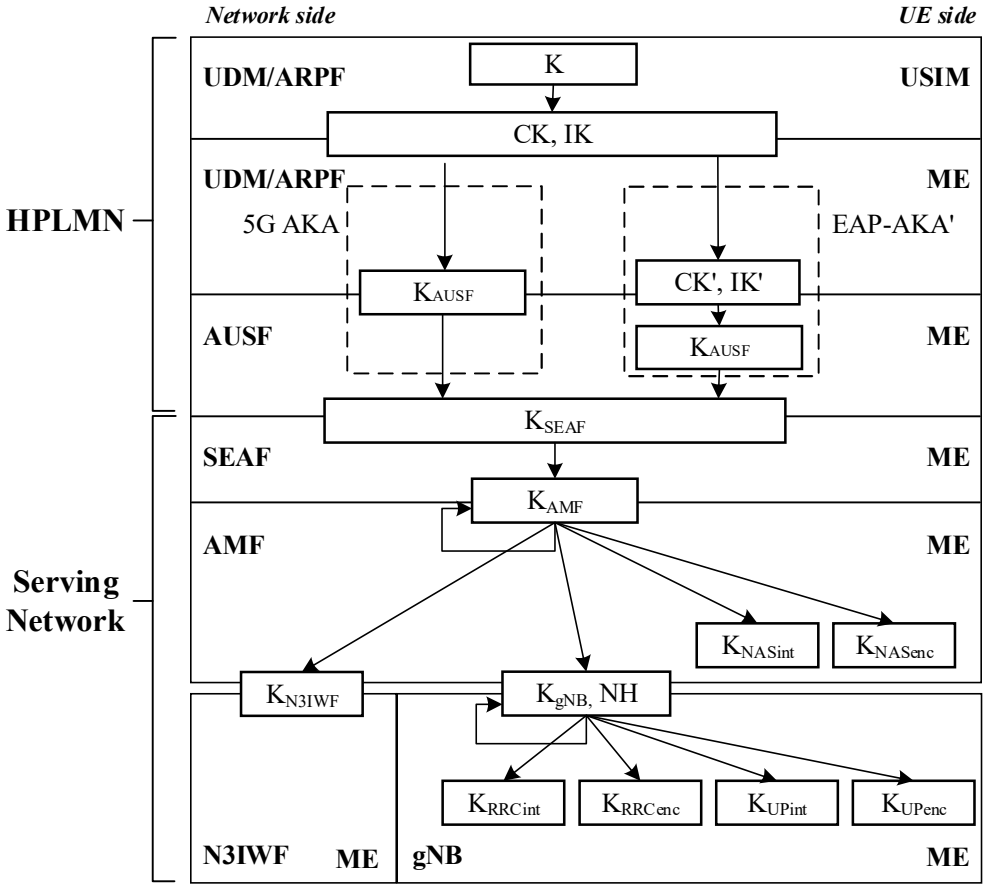


Figure 6 - Key Hierarchy

5.1.4.4 Serving Network Authentication

Binding authentication keys to a serving network prevents network spoofing. The serving network thereby authenticates itself to the user equipment. The serving network authentication is used for access technologies (i.e., 5G networks and Wi-Fi access).

5.1.4.5 Mitigation of Bidding Down Attacks

5G includes requirements that prevent an attacker from attempting a bidding down attack that makes the user equipment and the network entities respectively believe that the other side does not support a security feature, even when both sides in fact support that security feature.
This prevents fake base stations from forcing devices with earlier access (e.g., 2G, 3G) to avoid more advanced security features developed in later releases.

5.1.4.6 Subscriber Identifier Privacy

Each subscriber in the 5G system is assigned a globally unique Subscriber Permanent Identifier (SUPI). The SUPI is provisioned in the UDM/UDR and is only used within the 5G network. The SUPI incorporates the IMSI as part of its value, allowing the IMSI to be extracted and used when interworking with 3G/4G networks. The SUPI also incorporates the MCC/MNC for identifying the home network when used in 5G.

The SUPI replaces the IMSI used in previous networks, but the SUPI is never disclosed over the

air in the clear when a mobile device is establishing a connection.

To avoid disclosing the SUPI, a Subscription Concealed Identifier (SUCI) is used until the device (and network) is authenticated. Only then is the SUPI disclosed by the home network to the serving network but never sent "in the clear" over the air. The MCC/MNC portion of the SUPI is not protected, allowing other networks to quickly determine the home network for the SUPI.

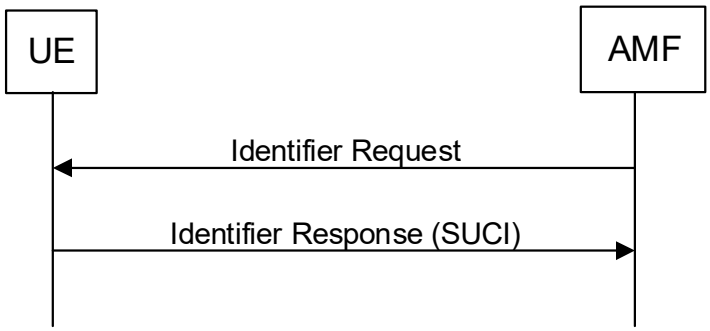


Figure 7 - The user equipment sends a SUCI when the AMF returns an identifier request message in response to a registration or re-registration

The user equipment generates the SUCI when it sends a registration request to the network (if it does not already have a 5G globally unique temporary identifier [GUTI] assigned). The SUCI can also be sent if the network responds to a registration (or re-registration) request with an identity request message.

This procedure has been defined to prevent IMSI catchers (also known as False Base Stations, or Stingrays) from being able to retrieve the subscriber identity by simply attaching to a device. In addition to the SUPI and SUCI, a Permanent Equipment Identifier (PEI) is assigned to the user equipment. This is analogous to the International Mobile Equipment Identifier (IMEI) used in previous generations of wireless networks.

The Subscription Identifier De-concealing Function (SIDF) is responsible for de-concealing the SUPI from the SUCI. 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 ensure that only a network element of the home network can send a request to the SIDF.

When roaming, the AMF is responsible for issuing a temporary identifier to roamers. The GUTI is allocated to the user equipment on both 5G access and non-3GPP access (i.e., Wi-Fi). The AMF is responsible for managing the assignment of the GUTI and can re-assign the GUTI on new transactions.

5.1.4.7 Overview of Security Architecture

The security architecture defined in TS 33.501 defines security as shown in Figure 8.

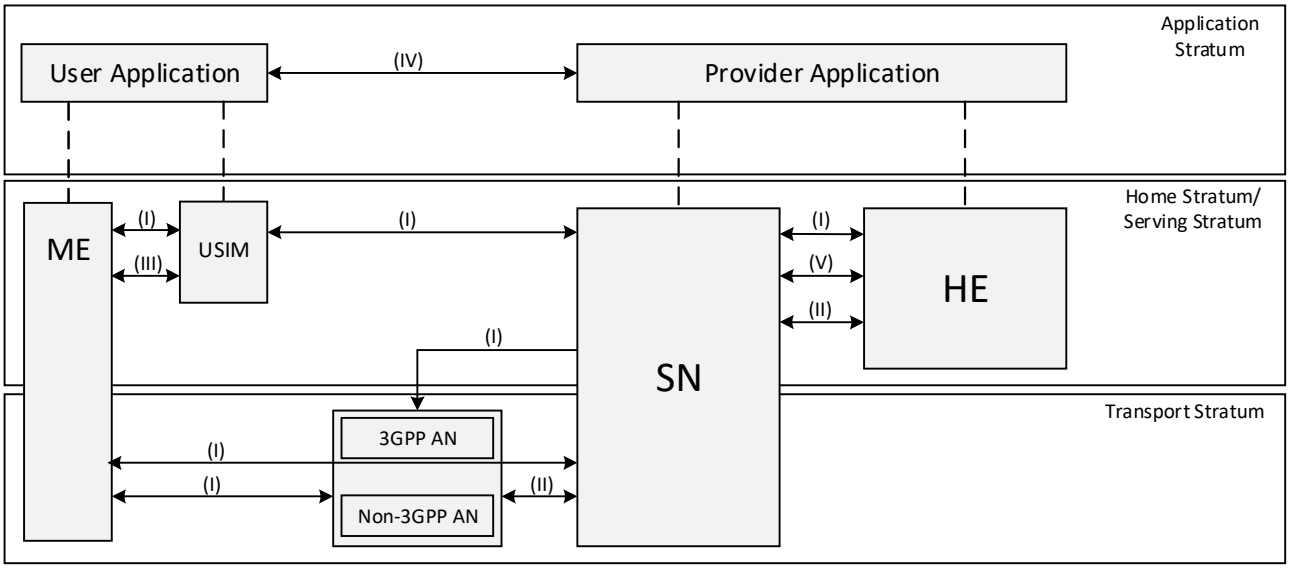


Figure 8 - The 3GPP 5G Security Architecture SOURCE: 3GPP

ME: Mobile Equipment
SN: Serving Network
HE: Home Environment

Network access security (I): the set of security features that enable a user equipment to authenticate and access services via the network securely, including the 3GPP access and non-3GPP access, and in particular, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from the serving network to user equipment for the access security.

Network domain security (II): the set of security features that enable network nodes to securely exchange signaling data and user plane data.

User domain security (III): the set of security features that secure the user access to mobile equipment.

Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.

SBA domain security (V): the set of security features about the SBA[11] security including the network element registration, discovery, and authorization security aspects, and also the

[11] 3GPP uses the term, Service Based Middleware (SBA) for the specific instantiation of Service Oriented Architecture in 5G specifications. Service Oriented Architecture (SOA) is the general purpose and more broadly used nomenclature. CSRIC VII uses SOA in this report as the acronym of choice.

protection for the service-based interfaces.

Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

5.1.4.8 Security Edge Protection Proxy (SEPP)

To protect messages that are sent over the N32 interface (between two 5G networks), the SEPP is defined as the entity sitting at the perimeter of the 5G network. The SEPP:

- Receives all service layer messages from the network function and protects them before sending them out of the network on the N32 interface and
- Receives all messages on the N32 interface and forwards them to the appropriate network function after verifying security, where present.

The SEPP implements application layer security for all the information exchanged between two network functions across two different PLMNs.

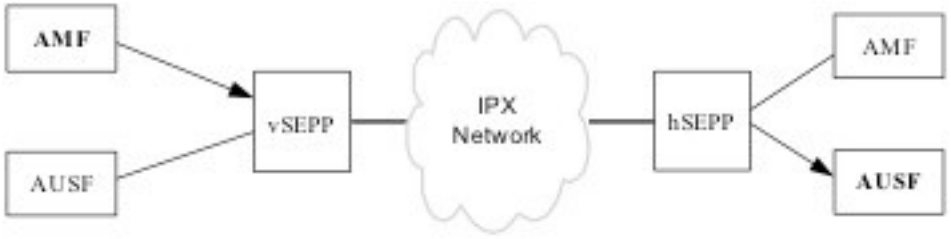


Figure 9 - The role of the SEPP in the security architecture. SOURCE: 3GPP

Protection for the HTTP message payload, sensitive information contained in the HTTP message header, and the Request URI is provided by the SEPP. However, not all information in the payload gets the same level of protection. Some information may require end-to-end encryption, while other information may only require integrity protection end-to-end, while still allowing modification of the message by intermediary Internetwork Packet Exchange (IPX) providers. The SEPP provides confidentiality of sensitive information as it is passed between two networks. This prevents intermediary networks (such as IPX) from being able to see this sensitive information (such as authentication vectors).

If there are parameters in the data that need modification by the IPX (such as parameters modified by mediation for interoperability), both networks must agree on what changes can be made and those changes must be integrity protected. When modifications are made by an IPX, the receiving network verifies the changes. The SEPP can detect any unauthorized message modifications received by an IPX.

The SEPP also provides traditional gateway functions, such as topology hiding, protection from malformed packets, protection against signaling storms, and validation of the message source.

In Release 16 the principle of Inter-PLMN Security for User Plane traffic in roaming scenarios has begun to be addressed by 3GPP – The role of the UPF is expanded to include protection for the N9 traffic between two roaming PLMNs. As is already defined in 5G architecture, the UPF can be segmented according to function, role, or deployment scenarios – thus this new

functionality can be implemented either in a combined node with other UPF functionality, or in a dedicated inter-PLMN UPF at the edge of the network.

5.1.4.9 New Security Requirements on the User Equipment

User equipment changes have been defined for 5G as well. The subscribers' credentials are protected using a tamper resistant hardware component, to prevent changing the identity of the device or accessing sensitive credentials.

Another capability in 5G for the user equipment is the ability to manage the radio technology used on the user equipment.

The user equipment allows the subscriber to disable and re-enable one or more of the radio technologies supported by the device, regardless of the network. These could be 4G/LTE, GSM/EDGE, WCDMA, or 5G NR.

The home network also can disable and re-enable radio technologies on the device, such as restricting the use of GSM/EDGE when 5G NR is available. This must be done using a secure connection between the user equipment and the network. These settings are remembered even when a user equipment powers down or is rebooted. If a prioritized service (such as emergency services, MPS, or mission critical services) is needed, and the user equipment is unable to connect to a network using the radio technologies that have been allowed, the prioritized service can override the user and network and select the radio technology supported an accessible network.

5.2 Device Ecosystem Evolution

5G will deliver high throughput speeds with low latency and network slicing to enable real-time and mission critical use cases, while improving consumer quality of experience. Enterprises will no longer tied down to a wired infrastructure and a less secure Wi-Fi network.

4G allowed us to experience the joy of mobile streaming but 5G will support the continued growth of networked systems, supporting Internet-of-Things (IoT)-enabled devices and constantly moving targets like self-driving cars. Issues with bandwidth, latency, and speed will all be exacerbated.

With the 5G evolution the device ecosystem has potential to add millions of connected devices.

Today consumers are depending on their devices more than ever and this dependency is increasing at an exponential rate. With the technology evolution and integration of technology in our day to day life dependency on connectivity will go to whole another level. For example, today smart devices along with IoT are actively used to measure and monitor heart rate; one of the leading device OEM has constantly evolved their product towards recognizing patterns in the heart rate using smart device sensors and flagging anomalies almost real time.

This increasing connectivity needs also results in a growing loss of privacy, as these smart devices collect and share data with the manufacturer and others. It's a goldmine of data about

how they're being used — and increasingly who is using them. And that tradeoff is not always apparent or clearly understood by the consumers using the device.

There is an opportunity for the consumers to know standards of testing being put in place to understand the security risks associated with technology and applications.

Today it is incumbent upon consumers to recognize risks associated with various sensors they are bringing into their homes — whether it's microphones, video cameras or just devices that are capturing all sorts of data.

There is an opportunity to define standards for Smart devices in terms of gathering certain types of data to work properly and improve their performance. In the absence of these standards, device OEMs/Carriers are collecting every possible information and exposing consumers to unknown risks.

5.2.1 Device Software vs. Hardware

Today's Smart device complexity is not just contributed from the technology (4g vs. 5g) but also from the evolving software applications. As an example, the most popular connected applications fall in six categories: smart home, entertainment, toys and games, wearables, health and exercise and pet products.

It is recommended to define and publish basic standards for every software application that is preloaded on consumer device such as:

- Is there a privacy policy and how accessible is it?
- Does the product require strong passwords?
- Does it collect biometric data?
- Are there automatic security updates?

5.2.2 Connected Devices

Connected devices are the most vulnerable when it comes to security due to their applications by consumers. There is a strong need for a security framework to evaluate various connected devices. This framework should be used for analyzing the devices' security components and report should be published. This is very critical for objectively assessing the risks of IoT equipment, in terms of how the devices communicate with cloud servers, the applications running on the devices, and the cloud-based endpoints. Today there is a wide variation in security depending on the manufacturer. In some cases, equipment made by small and lesser-known companies performed better than devices made by larger companies.

5G devices have a potential to be deployed from consumer-based use cases to mission critical uses that support health care, factory automation, infrastructure monitoring. With all the use cases being discussed for 5G there is a potential to add millions of devices to 5G networks. With such a large number of devices, device management on 5G networks becomes a critical aspect of deployment.

Following are key mobile equipment security areas driven by 5G architecture that need guidelines for testing and operational best practices during deployment:

- Risks due to compatibility with previous generation of telecom networks:

  For a while, 5G networks will be used side by side with 4G, and even 3G and 2G networks. There are known vulnerabilities in 4G networks such as denial of service (DDoS), possibility of incorrect protocol implementation by device manufacturers leading to control plane vulnerabilities. Because of 4G's role during the transition period, these threats will remain even after 5G reaches the public. In order to build adequate protection for 5G networks, standards for securing previous-generation networks should be published with structured test plans.

- Security risks due to use of internet technologies:

  The 5G network core is built on well-known Internet protocols such as HTTP and TLS. These internet technologies have been around and well known to attackers: there are a lot of techniques to search for vulnerabilities in them, and there are many tools available for easy exploitation. There is a need to standardize software development platforms for 5G devices to ensure that known high risks vulnerabilities of web technology are well documented similar to Metasploit penetration test platforms used for IT networks vulnerability testing and risks assessment (https://www.metasploit.com/).

- Network slicing:

  Network slicing splits a network into isolated slices. Each slice is allocated its own resources (bandwidth, service quality, and so on) and has unique security policies. This has significant security implications. As the configuration burden and number of parameters increase, so does the probability of a security slipup. This may be especially true when 5G network infrastructure is built jointly by several operators or when a single 5G network is shared by several virtual mobile operators. Security standards and guidelines for 5G in the form of default settings should be implemented across the board. Configuration flaws have been found to be a key vulnerability in 70% of the attacks either on corporate IT networks or cloud networks.

- Security Patching

  Security patching requires well defined standards as this exposes the devices to highest risks when it comes to connected devices. The consumer shouldn’t have to be aware that their refrigerator needs updates that must be downloaded to the device. There is a need for establishing policy and standards for security patching. While the notion of hacking a slow cooker might seem amusing, the devices have heating elements that could cause a fire if a malicious actor turned up the temperature.

5.3 Network Slicing Security

In 3GPP, Network Slicing is being defined in TS 23.501 [Ref 1]. A Network Slice is defined within a Public Land Mobile Network (PLMN) and includes the Core Network Control Plane and User Plane Network Functions as well as the 5G Access Network (AN). The 5G Access Network may be:

- A Next Generation (NG) Radio Access Network described in 3GPP TS 38.300 [Ref 4], or
- A non-3GPP Access Network where the terminal may use any non-3GPP access to reach the 5G core network via a secured IPSec/IKE tunnel terminated on a Non-3GPP InterWorking Function (N3IWF).

TS 23.501 further defines Network Function, Slice, and Slice Instance as follows:

- Network Function: A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behavior and 3GPP defined interfaces. (Note: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform, e.g., on a cloud infrastructure.)
- Network Slice: A logical network that provides specific network capabilities and network characteristics.
- Network Slice instance: A set of Network Function instances and the required resources (e.g., compute, storage and networking resources) which form a deployed Network Slice.
- NSI ID: an identifier for a Network Slice Instance.

5G mobile networks are expected to support network slices, as an example a network slice can be implemented in a virtual network running on a common infrastructure with different flavors like Core Network slices, RAN slices, end-to-end slices. A network slice may be created to support a specific communication service type, such as massive machine-type communication, or even a specific application, for example one single Internet of Things (IoT) application. Slices can use a common infrastructure (NFV infrastructure, Cloud Native, SDN-based transport) and may use common functions (e.g., a common radio scheduler may assign radio resources in a cell to different slices).

A common misconception is that slicing and Quality of Service (QoS) are directly linked by the 3GPP specifications – this is not the case as QoS is defined using separate functionality to slicing, and all QOS values can be used in any slice. However, since the computing infrastructure and packet routing network upon which a slice is implemented will have a direct impact on the performance of a slice, there is an implied relationship between a slice identifier and the QOS that the services using a particular slice experience.

Operator specific slices will typically require the same security considerations that standardized slice types require; however, some implementations of operator specific slices may require additional levels of security (e.g., physical separation, additional authentication, etc.) to accommodate the requirements of the specific service, or customer type.

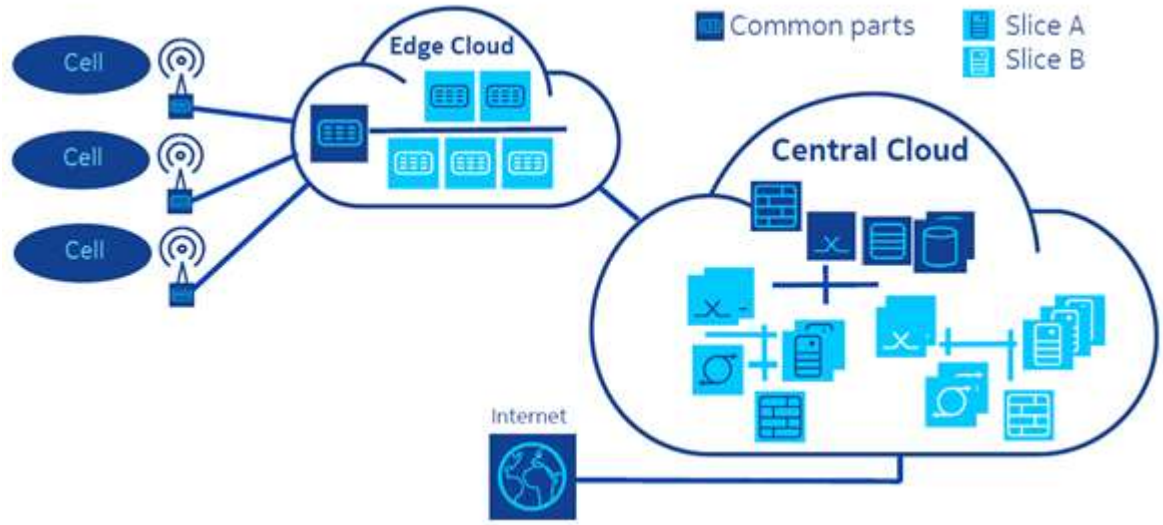


Figure 10 - A Mobile Network with Multiple Slices

5.4 5G Private Networks

Initial support for 5G Private Networks (called Non-Public Networks in 3GPP specifications) was added to 3GPP Release 16 and is being extended in release 17. 5G Private Networks essentially extend 5G technologies for deployment and use in private (enterprise) environments. 5G Private Network development is being driven mainly by two use cases:

- Industrial settings employing advanced automation (variously referred to as *The 4th Industrial Revolution, Industry 4.0 or IIOT – Industrial Internet of Things).*
  For these scenarios, the 5G Private Network is likely to serve a single or cluster of industrial facilities such as factory, warehouse, logistics center, or port in a flexible and lower cost manner. Examples of what Industry 4.0 elements the 5G Private Network will be used to support include: IIOT factory automation; inventory management and tracking; asset management and tracking; and process control.

- Campus settings providing enterprise voice and data services
  5G Private Network will be used for combined enterprise level voice and data services providing mobility within and beyond the campus setting as well as rapid setup and maintenance. 5G Private Networking will provide additional flexibility and cost effectiveness over the current use of Wi-Fi and softswitch PBXs with their attendant wiring for the Wi-Fi access points.

3GPP TS 22.261 introduces Non-Public Networks (private) as follows:

> *Non-public networks are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilising both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN.*

5G Private Networks in 3GPP are further divided into stand-alone 5G Private Networks not relying on functions which are provided by a public or commercial 3GPP network – Stand Alone Non-Public Networks (SNPN) – and 5G Private Networks integrated into public or

commercial networks – Public Network integrated Non-Public Network (PNI-NPN). The PNI-NPN allows the 5G Private Network subscriber to access public network services where permitted.

5G Private Network devices can be setup to only access specific 5G Private Networks or access both public networks and specific 5G Private Networks. Some of these public/private network combination devices will be able to connect to both types of networks simultaneously.

Various public-private interconnection arrangements are currently supported in Release 16:

- Access to public network services via the standalone 5G Private Network through the non-trusted 3GPP access (also used for Wi-Fi)
- Access to standalone 5G Private Network services via the public network also through the non-trusted 3GPP access.

The 5G Private Network enhancements currently being studied for 3GPP Release 17 at the time of this report include:

- Private Network credentials owned by an entity external to the 5G Private Networks (and any integrated public network)
- Remote 5G Private Network device provisioning

5.5 Edge Computing

5G applications may benefit from additional processing in the edge. In an example, as shown in Figure 11, an edge platform may be offered by the 5G network operator to support applications served from the content provider or from the cloud.

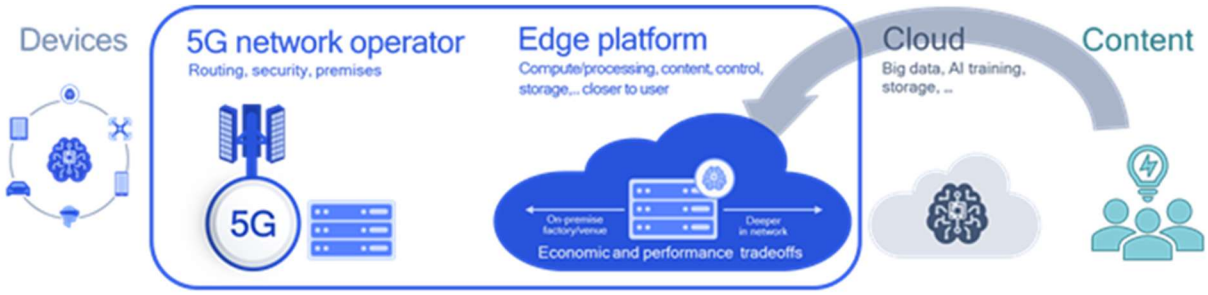


Figure 11 - Cloud and Edge Processing

Basic support for Edge Computing started in Release-15. 3GPP work is ongoing (in Release-17) in order to identify enhancements to the integration of edge processing in 5G systems. Specifically, this study is investigating mechanisms to discover connectivity to available Edge Computing resources (e.g., using DNS), mobility improvements for both UE consuming Edge Computing services and for Edge Application Servers, and for network capability exposure towards the Edge Application Server.

In addition, a new set of application layer interfaces for Edge Computing are identified that may potentially be useful for integration of Edge Computing. Specifically, the interfaces will enable application-layer discovery of Edge Application Servers, capability exposure towards the Edge

Application Server, and procedures for onboarding, registration, and lifecycle management of Edge applications.

The activities detailed in the present clause are intended to be application-neutral (i.e., to provide generic solutions for any use of Edge Computing platforms). The media aspects for using Edge Computing are not identified in these studies and information in the present Technical Report may be beneficially to contribute to Edge Computing for media processing. Integration of computational resources into the 5G System as part of Edge Computing functionalities are currently under study in 3GPP. Related to Edge computing, OpenFog Consortium defines Open Fog computing as system-level horizontal architecture that distributes computing, storage, and networking closer to users, and anywhere along the cloud-to-things continuum.

A number of academic papers have surveyed the security landscape for Edge & Fog computing:

- Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges; https://www.sciencedirect.com/science/article/pii/S0167739X16305635
- Fog computing and security issues: A review; https://ieeexplore.ieee.org/abstract/document/8390464
- Fog computing security: a review of current applications and security solutions; https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0090-3

5.6 5G Services

The development of 5G is guided and motivated by adding support for new services and enhancing existing services following four major categories:

- Ultra-Reliable Low Latency Communications (URLLC)
- Massive Internet of Things (MIoT)
- Enhanced Mobile Broadband (eMBB)

Additionally, Network Operations (NO) has been enhanced to support these services.

What follows are the high-level service elements in each of these areas along with example use cases motivating these elements. Specific vertical segments and industries are engaging with 3GPP to ensure that any unique vertical requirements are considered and incorporated in 5G standards. In future releases, 5G will be extended and enhanced to support more of these vertical segments and industries.

5.6.1 Ultra-Reliable Low Latency Communication (URLLC)

URLLC communication is targeted for applications dependent on critical communications. Critical communication typically requires various combinations of low latency, high reliability and high availability.

5G is designed to support applications with a wide range of reliability and latency needs, ranging from Ultra Reliability and Very Low Latency to High Reliability and Low Latency.

The following use cases are illustrative of different required combinations of very low latency, lower latency, ultra-high reliability, and higher reliability.

5.6.1.1 Ultra-reliability

Services requiring ultra-reliable communications, a minimum level of reliability and latency is required to guarantee the user experience or enable the service initially. This is especially important in areas like eHealth or for mission critical infrastructure communications.

5.6.1.2 Higher reliability and lower latency

These use cases are characterized by system requirements for higher reliability and lower latency. In most cases the data rates are moderate, and what matters most is that the messages are transmitted quickly and reliably.

One typical application where this type of communication is needed is in a power plant. The network coverage may be limited to a confined area, either indoor or outdoor, and often only authorized users and devices can attach to it.

Another typical application is for industrial factory or process automation requiring communications for closed-loop control applications. Examples for such applications are robotic manufacturing, round-table production, machine tools, packaging and printing machines.

5.6.1.3 Very Low Latency

Very Low Latency use cases typically are distinguished by very tight feedback constraints where input from the mobile device requires a very quick response or action. Examples of these Very Low Latency use cases includes Virtual Reality and Augmented Reality where image and scenery display on the user's device is based on real—time device sensor input such as movement and location.

Another use case is where tactile input is used to control some activity in real time such as tele-surgery where a surgeon is remotely controlling a surgical robot. Immediate tactile feedback of what the robot is encountering with the patient must be provided quickly back to the surgeon's controls for proper surgery progress feedback and assessment.

5.6.1.4 Higher reliability, higher availability, and lower latency

These use cases are characterized by high system requirements for reliability, availability, and latency. In most cases the data rates are moderate, and what matters most is that the messages are transmitted quickly and reliably, and that the network and its services are consistently available, with minimal downtime.

One example use case of this is UAV control. Drones must be controlled quickly and reliably everywhere they go. The latency does not, however, need to be ultra-low because when a human operator is involved, the human reaction speed sets the expected level of delay and requiring a much lower latency from the communications network makes little sense. The data rates to

transmit the control and measurement data are not very high but if the operation of the vehicle relies on a video feed, then the required data rates are higher. The pilot of the vehicle needs to be aware of the location of the vehicle. For most purposes the geographic location is needed to provide a rough position, and local positioning, e.g., radar, is used for collision avoidance. Another typical area is support of advanced telemedicine techniques, and cloud-based services can be used to provide anytime and anywhere access to patient medical records, which makes security related issues more important. Additionally, the computing resources available through the cloud are expected to support advanced diagnostics and facilitate remote examinations of patients in high mobility scenarios.

Since the ambulance may be dispatched to a remote location that does not have the same coverage and available RATs as in an urban environment (location of the hospital), fast and seamless handover between different technologies is crucial. Furthermore, if the ambulance moves from one operator's network to another then the m-Health service must seamlessly switch/handover from one network to another.

5.6.2 Massive Internet of Things (MIoT)

5G MIoT expands on 4G's IoT support in the following dimensions:

- Support for several orders of magnitude larger numbers of IoT devices.
- Support new categories of consumer IoT devices continue to emerge such as smart wearables, personal sensors (such as exercise trackers, heart rate monitors), and Personal Area Networks with additional requirements such as power limitations.
- Support increased focus on IoT security
- Support of "lightweight" IoT devices where small infrequent messages are communicated, and also where low power and long battery life is critical.
- Expands IoT connectivity options from direct 5G radio interfaces to indirect radio interfaces, for example a smart watch connected to a mobile phone via Bluetooth.

5.6.3 Enhanced Mobile Broadband (eMBB)

5G's eMBB is enhancing user's broadband experience by building on increased radio bandwidths as well as increasingly flexible bandwidth usage and control.

5G eMBB provides for:

- Higher user data rates through advanced services and richer user experiences such as supporting high definition video (4K UHD)
- Supporting higher user densities such as in dense urban settings
- Providing higher mobility options such as eMBB on airplanes or high-speed trains
- Continue to improve femto/small cells for ease of installation and support for higher user data rates and user densities
- Accelerate convergence between fixed and mobile networks for seamless user experience and operational efficiencies

5.6.4 Network Operations (NO)

In order to support the previously described service improvements faster and efficient manner, 5G network design, deployment and operation is also being upgraded to be more flexible and efficient.

Increased 5G network flexibility is accomplished, for example, by:

- Supporting a wider range of network deployments for both existing network operators as well as for new smaller non-traditional networks such as for non-public networks in a scalable fashion
- Reducing the minimum service levels required to operate a network in specific cases such as for non-public networks.
- Network slicing to allow establishing dedicated and isolated logical networks with the physical networks. These can be used for instance to create private logical networks for specific users or user segments (e.g., IoT)
- Increase efficiency of user plane traffic to support more users per bandwidth
- Exposing certain network capabilities to selected 3rd parties. This could be, for example, exposing mobility events to a 3rd party's server for that party's IoT devices in a dedicated slice

Increasing access options by enhancing 5G support for:

- Increasing the access options available for use when multiple access networks are used simultaneously such as Wi-Fi and 5G NR.
- Use of satellite access as part of a 5G network

5.7 IoT Applications Security and Certification

As discussed in CSRIC VI and clause 5.6.2, IoT Service Enablement in 5G, focuses on the essential interconnectivity between the "Things" and the "Internet" that will be enabled as a result of the realization of a 5G network. Examples of IoT Applications include connected things that are industrial, medical, and consumer products; all that have one thing in common: they represent another attack vector that can be used against critical infrastructure if not managed and secured. Industrial processes, localized or geographically distributed, are increasingly automated to ensure quality, consistency, and cost-effective production of goods or services. Connectivity is required for these sensors and actuators both indoors and outdoors with high availability and reliability to ensure seamless production and the ability to adapt processes in real-time for maximum flexibility.

Autonomous cars use a combination of technologies to detect their surroundings including wireless communication technologies, laser and radar sensing, GPS, odometers, computer vision, and advanced control systems. 5G technologies are anticipated to enable these cooperative automatic driving use cases in an enhanced fashion where sensor information will be exchanged in real time between thousands of cars connected in the same area. Smart Grids will enable enhanced monitoring, better management, and greater control of energy generation and distribution networks leading to increased availability and resilience. Lastly, the media and entertainment industry seek to improve the user experience and enable access to an expanding universe of content anytime and anywhere. This vertical opportunity focuses on different types

of multi-media services that include regular live/linear media, on-demand content, user-generated content and gaming. Reference CSRIC6 for additional detail and information.

5.7.1 Industry Device Certification Initiatives

IoT devices often lack device cybersecurity capabilities. Manufacturers can help customers by improving how securable the IoT devices they make are, meaning the devices provide functionality that their customers need to secure them within their systems and environments, and manufacturers. Within the IoT industry are numerous certifications published, all working on an equal basis to find common ground on IoT device security for new designs. While individual industry segments work on security, broad efforts are taken to address the challenge in harmonizing the industry. These efforts are occurring in all parts of the globe, such as the European Union, Japan, U.K, and United States.

CTIA Cybersecurity Certification Working Group: CTIA manages a cybersecurity certification program for Internet of Things (IoT) devices, establishing an industry baseline for device security on wireless networks. The CTIA IoT Cybersecurity Certification Test Plan supports a variety of use cases and levels of device sophistication.

- CTIA's Certification Test Plan defines the cybersecurity tests that will be conducted in CTIA Authorized Test Labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. CTIA's Cybersecurity Certification is defined in three levels- the first level identifies core IoT device security features; the second and third levels identify security elements of increasing device complexity, sophistication and manageability.

CSDE's C2 "The Consensus Baseline IoT Device Security Capabilities": This is a common set of device security capabilities that can be applied to all new IoT devices that connect to the internet. The baseline is a set of best practice capabilities that are broadly applicable—vertically and horizontally—across markets. The baseline is a starting point for IoT device security that will need to evolve over time based on both changes in technology and changes to the threat landscape. This document informs further work on capabilities for IoT device cybersecurity that is more targeted to specific verticals, device types, use cases, etc.

UL IoT Security Rating: The UL IoT Security Rating Framework aligns with prominent industry standards, including ETSI, and can serve to demonstrate conformance to those standards. This effort is based on UL's IoT Security Top 20 Design Principles, which aims to serve two purposes-

- Help manufacturers and developers improve the security posture of their solutions by leveraging proven security best practices
- Rate the security posture of IoT solutions in order to make security more transparent and accessible to consumers

BITAG IoT Security and Privacy Recommendations: BITAG believes that following the guidelines in this report can dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs. This document was issued in November 2016.

ETSI: This work effort helps in ensuring that IoT devices are compliant with the General Data Protection Regulation (GDPR). This present document can also help organizations implement a future EU common cybersecurity certification framework as proposed in the Cybersecurity Act [i.13] and the proposed IoT Cybersecurity Improvement Act in the United States.

ioXt: The purpose of this Certification Program is to define a common method for the assessment and rating of a products (and organizations) fulfillment of the ioXt Security Pledge. With the engagement and support of their members companies, the certification program foundation has been created and Alliance staff is working with key members to review and fine tune the assessment process.

5.7.2 GSMA IoT-SAFE Model

IoT SAFE[12] (IoT **S**im **A**pplet **F**or Secure **E**nd-to-End Communication) is an ongoing initiative in GSMA to enable IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardized Root of Trust to protect IoT data communications. The latest version of the GSMA IoT security documents include references to the IoT SAFinitiative, leveraging the SIM for IoT security.

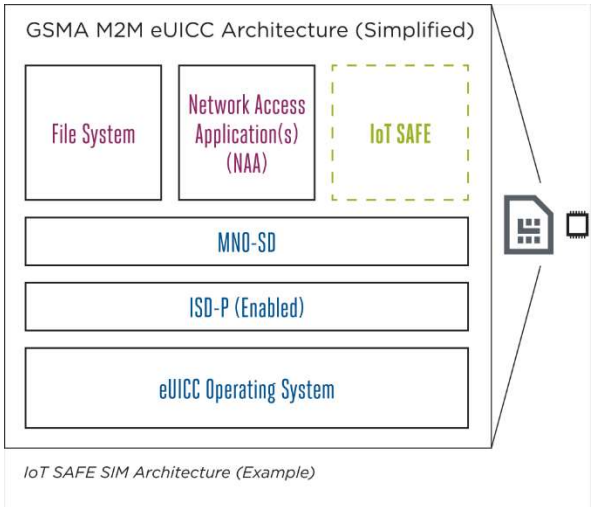


Figure 12 - IoT SAFE SIM Architecture. Source: GSMA

As shown in Figure 12, the SIM is used as a mini 'crypto-safe' inside the device to securely establish a (D)TLS session with a corresponding application cloud/server. This is compatible with all SIM form factor: SIM, eSIM, iSIM, etc. This provides a common API for the highly

[12] https://www.gsma.com/iot/iot-safe/#doc

secure SIM to be used as a hardware 'Root of Trust' by IoT devices. The IoT SAFE SIM architecture helps solve the challenge of provisioning millions of IoT devices.

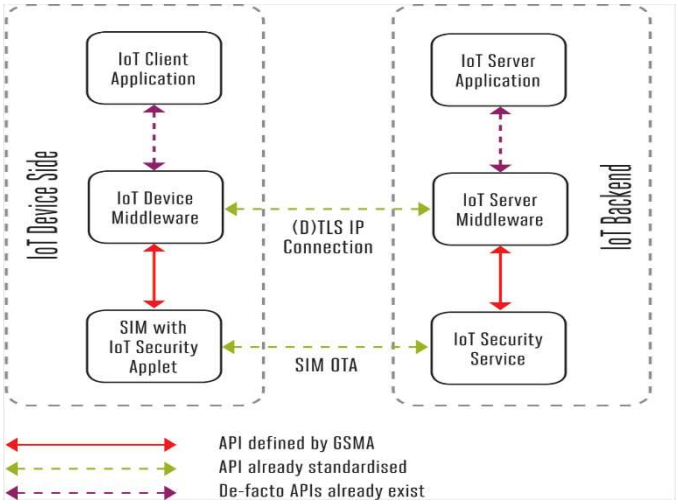


Figure 13 - Security Services. Source: GSMA

IoT SAFE provides security services that enable IoT devices to securely perform mutual (D)TLS authentication to a server using either asymmetric or symmetric security schemes. Additionally, IoT devices will compute shared secrets and keep long-term keys secret.

5.8 Wireline and 5G

Fiber optic networks plays a prominent role in enabling the 5G infrastructure because the many benefits that will be realized through the deployment of 5G. 5G architecture utilizes small cell technology employing high frequency transmissions. Such high frequencies allow extremely high-speed transmission of data from smart phones to small cells. Higher frequencies, however, are not well suited to penetrate urban structures of concrete, metal, or wood. In this environment, fiber is best used to transmit data between small cells and cell towers and, in turn, backhauled to switching offices at maximum speeds.

Additionally, once fiber is in place, it can scale easily to accommodate higher speeds and the expected growth of transmissions. Fiber will necessarily be deployed broadly throughout the emerging 5G networks to act as an essential partner in implementing 5G capabilities and capacities.

5.9 IETF

It is useful to understand how 5G affects Internet technology. IETF [Ref 4] work has been and will be affected by 5G, as the IETF works on many of the general facilities that modern networked systems such as 5G are based on.

These interactions typically fall in one of the following categories:

- New dependencies on existing IETF technology. For instance, the flexible authentication framework mentioned above is EAP (RFC 3748, RFC 5448). This is likely to be merely

a reference to existing RFCs, or if additions are needed, they are small.

- Dependencies to ongoing work at the IETF. This includes various general facilities as noted above, but also other things. For instance, the IETF DETNET working group defines mechanisms to guarantee deterministic delays for some flows across a network. As one of the 5G use cases is time-critical communication and low-latency applications, this is a component technology that is being looked at. Similarly, IETF routing-related work such as traffic engineering, service chaining and source routing are likely tools in managing traffic flows in 5G networks.

5.10 ETSI NVF and SDN

ETSI NFV is a sub working group within ETSI focused on developing virtualization technology and the application of such technology to telecommunication networks and services. Since the work began in 2012 many documents have been produced, grouped into various releases (currently release 1, 2 and 3 are available and release 4 is under development). The early releases focused on the framework, and the protocols that are required for NFV, more recently the group has focused on implementation, operation, and testing guidelines of the technology; this includes several documents focused on security related aspects.

5.10.1 NFV Reference Architecture Framework

ETSI has defined a Reference Architecture for NFV in document ETSI GS NFV 002 V1.2.1 [Ref 13] as shown in Figure 14.

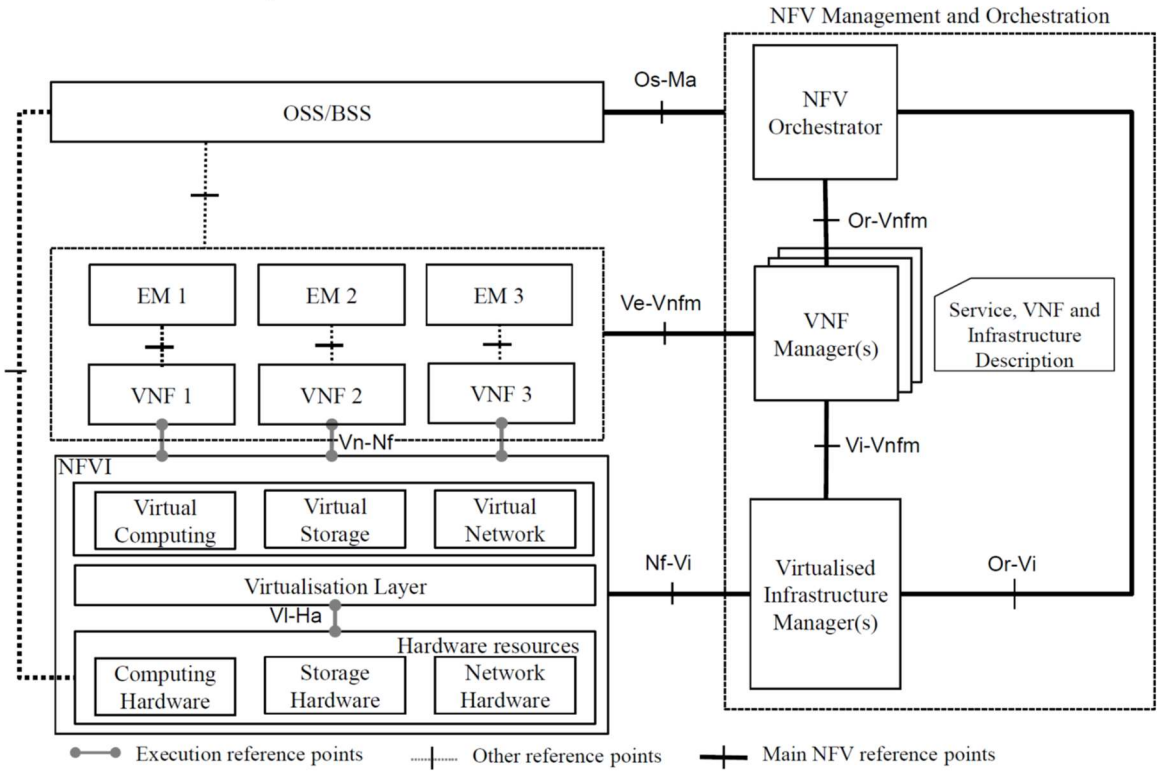


Figure 14 - ETSI NFV Reference Architecture Framework

Details on each of the above elements, sub-elements and interfaces are described further in the same document. While not directly defined, it is implied that the Network Hardware may be supplied by a SDN, the subsequent document ETSI GS NFV-EVE 005 V1.1.1 [Ref 14] details many of the benefits and impacts of combining NFV and SDN in a network.

5.10.2 ETSI NFV Work on VNF and SDN Security

The following papers have been produced by ETSI NFV to consider different security aspects of NFV, and impacts to NFV systems:

- ETSI GR NFV-SEC 009 V1.2.1 (2017-01) Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration
- ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components
- ETSI GS NFV-SEC 013 V3.1.1 (2017-02) Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification
- ETSI GR NFV-SEC 018 V1.1.1 (2019-11) Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture
- ETSI GS NFV-SEC 021 V2.6.1 (2019-06) Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification
- ETSI GS NFV-SEC 022 V2.7.1 (2020-01) Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access
- ETSI GS NFV-IFA 026 V3.2.1 (2019-07) Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification

5.10.3 Security Recommendations and Requirements for ETSI NFV

The documents listed above define many security related features and functions that a NFV operator should employ when deploying virtual functions and applications – A High-level summary of these security recommendations and requirements is provided here for reference:

- Different requirements for Single-Operator and Multi-Operator Trust Domains
- Security Hardening of Management and Monitoring Systems
- Passive/Active/Hybrid Security Monitoring
- Memory inspection & Secure logging
- Platform hardening (including OS-level access control, authentication controls, Read-only partitions and Write-only partitions)
- Data protection and confidentiality (secure storage and retrieval, self-encrypting storage)
- Communications Security (including message integrity & encryption)
- Bootup and bootstrap hardening (including Measured boot, secured boot, Secure Bootstrapping Protocol)

- Hardware-mediated execution enclaves (including Trusted Platform Module (TPM) and
- Hardware Security Modules (HSM))
- Software integrity protection and verification
- Attestation & Signing (Software, Operating system, Virtual Instance, Hypervisor, etc)

Since 5G infrastructure is anticipated to be virtualized (in most deployments), many of these capabilities are relevant to 5G networks.

5.11 Open Source Developments (ONAP, O-RAN)

5G is not about bolting some new radios to towers and calling it a day. 5G requires an entirely new approach to designing and building networks. Data traffic on our wireless network averages has increased, with one operator reporting an increase of more than 470,000% since 2007. Introduce 5G into that mix, and you have the recipe for a data explosion. Autonomous cars, robotic factories, seamless AR/VR and other new applications will be connected to 5G, on top of the video streaming, gaming and other apps we already use. Thus, the need to make the network not just faster, but a lot more efficient.

Open Source Software (OSS) is a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose[13]. Open source "products" typically evolve through community cooperation among individual programmers as well as large companies. An open source license permits anybody in the community to study, change and distribute the software for free and for any purpose.[14] Open source collaborations drive innovation, making it easier to deploy technology in the marketplace.

In a U.S. DoD CIO memorandum "Clarifying Guidance Regarding Open Source Software (OSS)"[15], open source software is defined as "software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of that software ". Open source software (OSS) is typically developed through a collaborative process. Most OSS projects have a "trusted repository" (web) location where people can get the "official" version of the program, as well as related information (documentation, bug report system, mailing lists, etc.). Trusted developers can modify the software in the trusted repository

One of the fundamental differences between open source software and proprietary software is that the source code of open source software must be made available with the software. This does not mean that the source code must be physically delivered with the software, just that it must be available at a freely accessible location.

Commercially available software, or proprietary software, doesn't give access to its source code because the software is considered the intellectual property of the developer. As a result, users often pay for licensing the intellectual property or software. In comparison, open source software is considered shared intellectual property among all contributors that have helped

[13] https://en.wikipedia.org/wiki/Open-source_software
[14] Oracle White Paper, September 2013, The Department of Defense (DoD) and Open Source Software
[15] https://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf

develop or alter it.

Software defined networking and virtualization promise substantial security enhancements. 5G's virtual and cloud-based network systems will allow for more adaptable security since they can be quickly adjusted, removed, or replaced using software, reducing the likelihood that an entire network would be impacted by a cyberattack.

Closed-loop automation based on ONAP and virtualization's inherent elasticity feature will be a significant 5G security advantage; for example, a network can be quickly scaled to mitigate DDoS attacks

Potential advantages of open source software:

- Reduces the cost and effort to produce common functionality.
- Larger numbers of developers producing and maintaining more popular functionality
- Platform design is being crowdsourced by global stakeholders
- Provides for faster distribution of bug fixes

Potential disadvantages of open source software:

- Usually not subjected to any formal review, validation or verification processes
- May provide a higher opportunity for malicious code injection.
- Open source software code equally available for study by developers and potential attackers.
- Widespread use of open source software creates a larger base of exploit targets (as opposed to potentially smaller bases of vendor proprietary software)

5.12 5GC Virtualization

Open and virtualized systems have great potential to transform the telecommunications industry as we progress into the 5G era, with more services moving to the edge, and a greater demand for elasticity and responsiveness. Virtualization has existed in networking for decades, but it will be baseline for 5G in more parts of the network with the greatest impact seen in the Core, Edge and, in some implementations, (Radio) Access.

Virtualized networks can provide improvements in dynamic services, the speed of rollout, network resiliency and cost/performance benefits in some situations as compared to pure hardware solutions. However, a virtualized infrastructure also can consist of a highly distributed supply chain, with multiple functional layers to deliver a service, creating potential complexity in operations and lifecycle management in Figure 15.

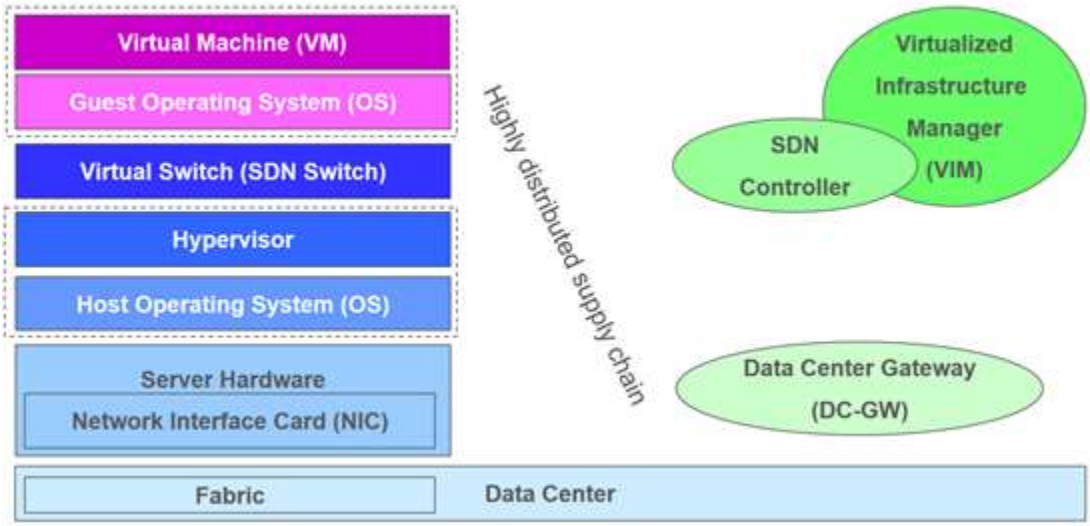


Figure 15 - Virtualization Environment

Virtualized networks can provide a similar level of security, as compared to coupled hardware/software, given that certain best practices and controls are followed, but the inherent complexity of an implementation can make this more arduous. Some examples of common best practices:

- hardening and patch maintenance should be done across all of the layers, where possible
  - note that even this can be challenging due to the inter-layer relationships required in a virtualized stack. Individual portions can't be upgraded or locked down independently; comprehensive testing is required
- segmentation and separation between tenants must be maintained and unauthorized VM's should be blocked
- ingress/egress filtering across virtual functions and interfaces should be enabled or protected through the use of virtual firewalls and/or ACL's
- where cryptographic functions are required, TRNG (true random number generation) should be available for tenants, due to the lack of native entropy
- role based and/or attribute-based access controls must be tightly maintained across multiple layers and access to the (sometimes separate) management systems should be governed as well
- Side channel attack protections should be considered, especially in high security environments or where cryptographic functions are required

In order to deliver services across a virtualized infrastructure, the terms SDN (Software Defined Networking) and NFV (Network Function Virtualization) are commonly used – while they are related in practice, they serve different purposes. SDN can mean different things in different environments, is not based on one "standard" and does not even require virtualization. Typically, it seeks to achieve separation of the control and data/forwarding planes, utilizes a centralized controller and central view of the network and allows for network programmability. This is illustrated in Figure 16.

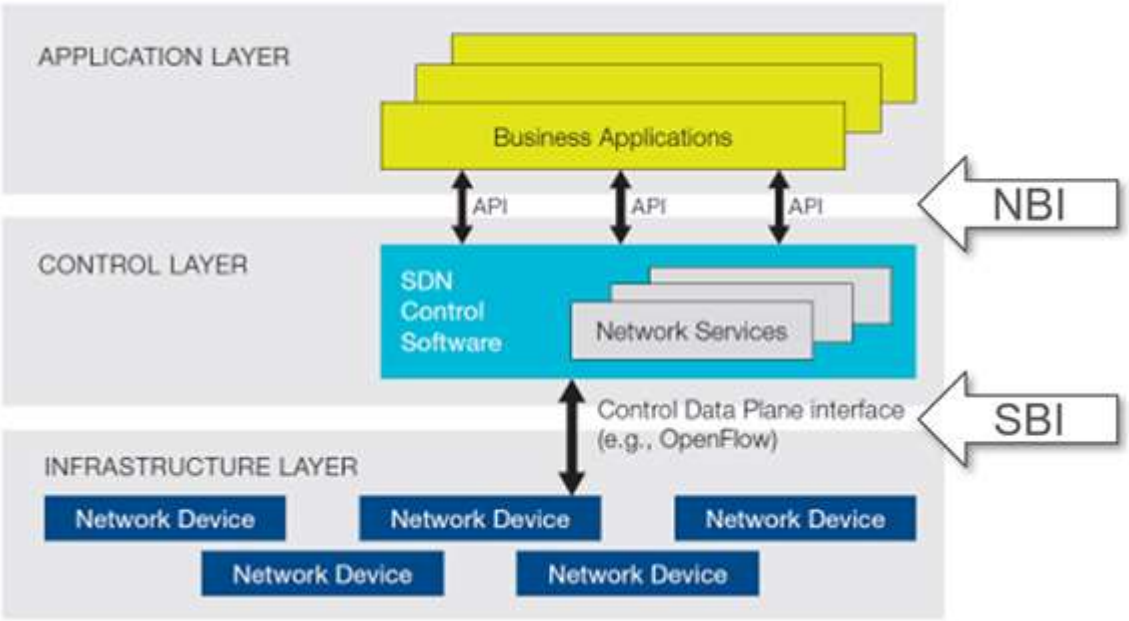


Figure 16 - Common SDN Implementation

Utilizing SDN as part of a virtualized, 4G/5G network will be common for many implementations, due to the needs for centralized orchestration and automation of services. The flow-based nature of SDN (separating the data channel into multiple flows and layers) compliments classic perimeter security model thinking and works well for virtualized security functions in service chaining. It also allows for dynamic and flexible security policy adjustments and resilience of network management if individual data planes are disrupted. However, the SDN controller is also a single point of compromise or failure and this must be considered in a widely distributed architecture especially North Bound Interfaces (NBI) must be monitored for malicious applications that are outside of the protected control layer and South Bound Interfaces (SBI) must have protected communication paths between the controller and switches.

5.12.1 O-RAN

While operators around the world believe that a modern 5G infrastructure will enable new vertical market revenue opportunities, there is unanimous agreement that traditional supply chain and procurement models must change. Status quo, proprietary product architectures and complicated, vendor specific Operations and Management (O&M) systems will not serve these operator's collective goals and must evolve to overcome the real capital, operational and technical challenges the industry is facing today. According to a Telecom Infra Project (TIP) report16 the RAN accounts for approximately 70% of network costs, making a reduction an attractive opportunity for operators. An open RAN is expected to lower the total cost of ownership (TCO) associated with the deployment and maintenance of networks. As a result, there are two major industry initiatives looking at evolving and opening up the radio access networks. The first is the O-RAN Alliance[17], and the second is the OpenRAN project group

[16] https://telecominfraproject.com/wp-content/uploads/OpenRAN-v11082019-vFinal.pdf
[17] https://www.o-ran.org/

under the Telecom Infra Project (TIP)[18].

The O-RAN Alliance was founded by operators to clearly define requirements and help build a supply chain eco-system to realize its objectives. To accomplish these objectives, the O-RAN Alliance's work will embody two core principles: openness and intelligence. The O-RAN Reference Architecture is designed to enable next generation RAN infrastructures. Empowered by principles of intelligence and openness, the O-RAN architecture is the foundation for building the virtualized RAN on open hardware, with embedded AI-powered radio control, that has been envisioned by operators around the globe. The architecture is based on well-defined, standardized interfaces to enable an open, interoperable supply chain ecosystem in full support of and complimentary to standards promoted by 3GPP and other industry standards organizations.

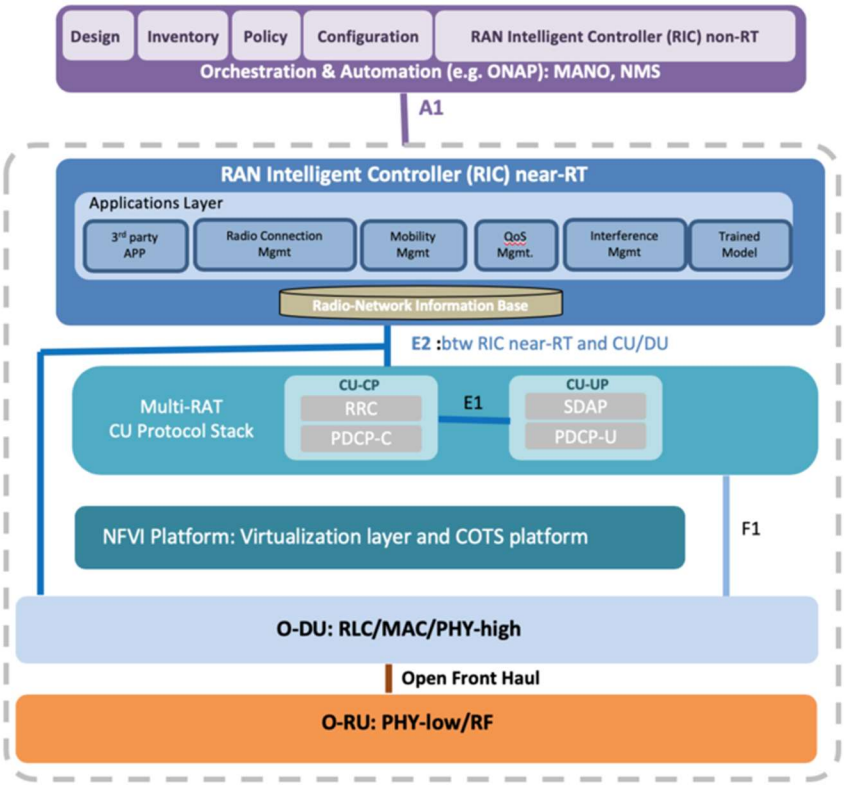


Figure 17 - O-RAN Architecture

The O-RAN Software Community (SC) is a collaboration between the O-RAN Alliance and Linux Foundation (LF) with the mission to support the creation of software for the Radio Access Network (RAN). The RAN is the next challenge for the open source community. The O-RAN SC plans to leverage other LF network projects, while addressing the challenges in performance, scale, and 3GPP alignment.

The OpenRAN Project Group under the Telecom Infra Project (TIP) is an initiative to define and build 2G, 3G, and 4G RAN solutions based on a general-purpose vendor-neutral hardware and

[18] https://telecominfraproject.com/openran/

software defined technology. This project group's main objective is the development of fully programmable RAN solutions based on General Purpose Processing Platforms (GPPP) and disaggregated software so they can benefit from the flexibility and faster pace of innovation capable with software-driven development.

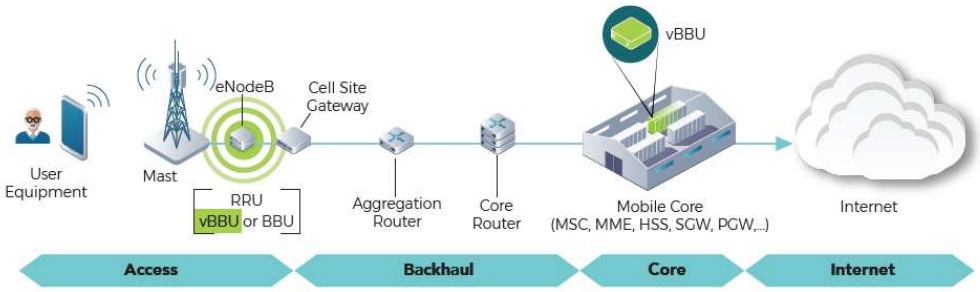


Figure 18 – OpenRAN

OpenRAN has also began looking at the 5G NR as shown in Figure 19.

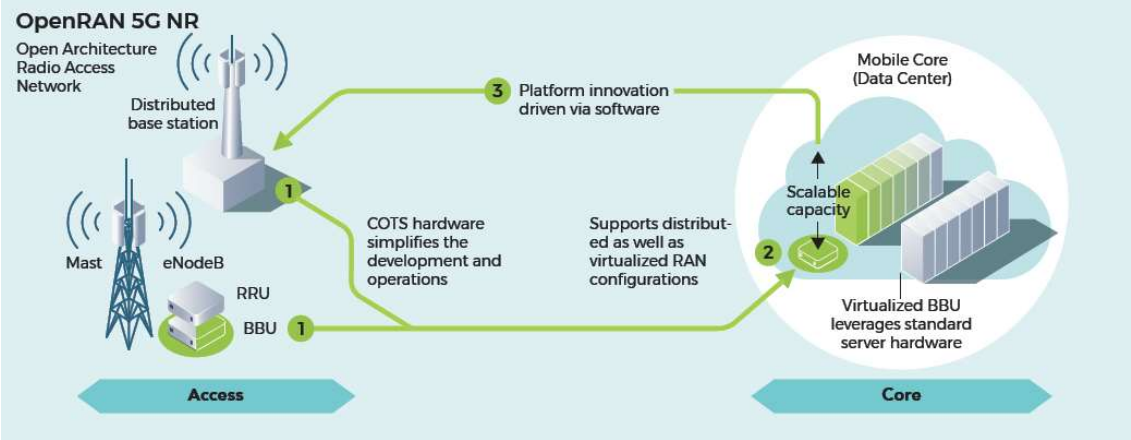


Figure 19 - 5G NR in OpenRAN

5.12.2 Network Management & Orchestration, Edge, Intelligence, and SDN

As the networks move toward cloud native implementations, open source platforms become increasingly important in the deployment of 5G networks, especially for network management and orchestration, software-defined networking, moving intelligence to the edge, and automating function throughout the network.

Open Network Automation Platform[19] (ONAP) provides a comprehensive platform for real-time, policy-driven orchestration and automation of physical and virtual network functions that will enable software, network, IT and cloud providers and developers to rapidly automate new services and support complete lifecycle management. The ONAP project addresses the rising need for a common automation platform for telecommunication, cable, and cloud service providers—and their solution providers—to deliver differentiated network services on demand, profitably and competitively, while leveraging existing investments. ONAP decouples the

[19] https://docs.onap.org/en/dublin/guides/onap-developer/architecture/onap-architecture.html#onap-architecture

details of specific services and supporting technologies from the common information models, core orchestration platform, and generic management engines (for discovery, provisioning, assurance etc.). Furthermore, it marries the speed and style of a DevOps/NetOps approach with the formal models and processes operators required to introduce new services and technologies. It leverages cloud-native technologies including Kubernetes to manage and rapidly deploy the ONAP platform and related components. This is in stark contrast to traditional OSS/Management software platform architectures, which hardcoded services and technologies, and required lengthy software development and integration cycles to incorporate changes. The following provides a high-level view of the ONAP architecture with its microservices-based platform components as shown in Figure 21.

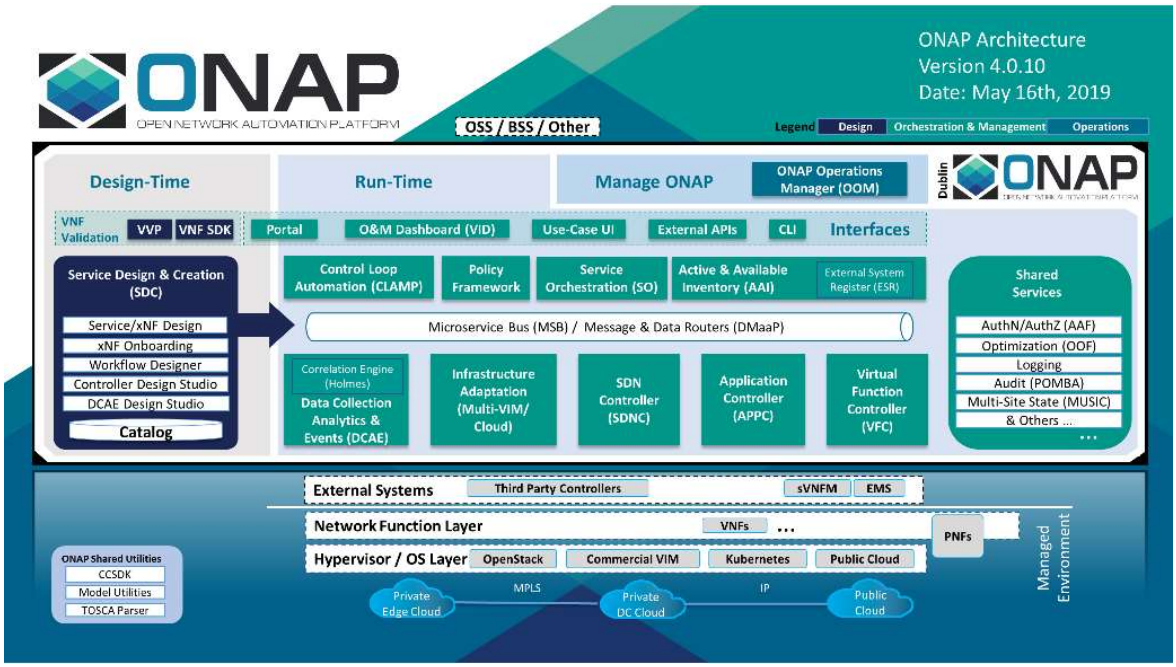


Figure 20 - ONAP Architecture

The evolution and rapid progression of new technologies like augmented reality, autonomous vehicles, drones, and smart cities are inevitable. The demand for real-time processing capabilities at the edge instead of centralized processing can be addressed with Edge Computing. Edge Computing enables processing and storage capabilities closer to the endpoint using familiar cloud technologies. This approach will reduce the total cost of ownership and enable faster processing to meet application latency requirements. The Edge Cloud solution will also comply with local and global data privacy requirements.

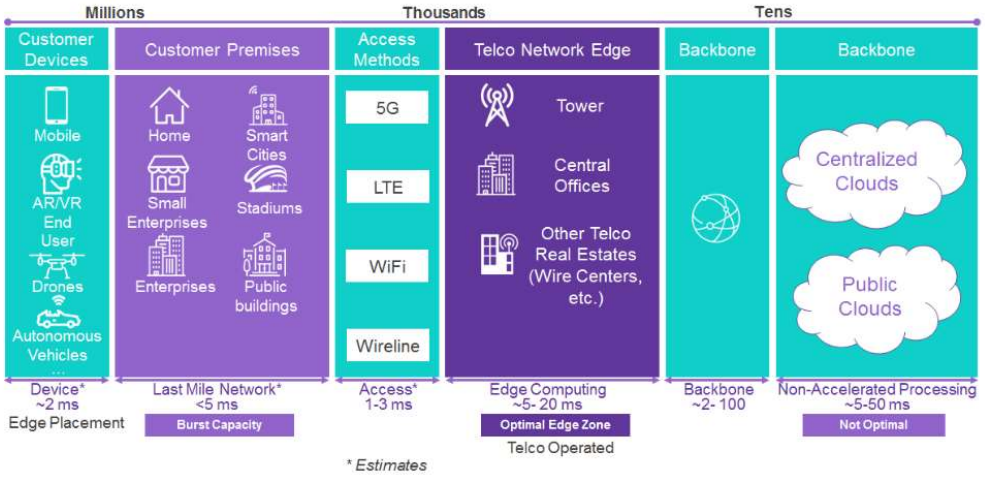


Figure 21 - Edge Cloud Solution

Akraino is a Linux Foundation (LF) open source project intended to create an open source software stack supporting high-availability cloud services optimized for edge computing systems and applications. LF Edge is an umbrella organization within the Linux Foundation that aims to establish an open, interoperable framework for edge computing independent of hardware, silicon, cloud, or operating system. Akrino will offer users new levels of flexibility to scale edge cloud services quickly, to maximize the applications or subscribers supported on each server and to help ensure the reliability of systems that must be up at all times. Akraino R1 delivered the first iteration towards new levels of flexibility to scale edge cloud services quickly, maximize efficiency, and deliver high availability for deployed services. It delivers a deployable and fully functional edge stack for edge use cases ranging from Industrial IoT, Telco 5G Core & vRAN, uCPE, SDWAN, edge media processing, and carrier edge media processing. Akraino Edge Stack also provides processing power closer to endpoint customer devices to meet application latency requirements of less than ~20 milliseconds. Akraino Edge Stack community is focused on Edge APIs, Middleware, Software Development Kits (SDKs) and will allow for cross-platform interoperability with 3rd party clouds. The Edge Stack will also enable the development of Edge applications and create an application w/ Virtual Network Function (VNF) ecosystem.

A typical service provider will have thousands of Edge sites. These Edge sites could be deployed at Cell tower, Central offices, and other service providers real estate such as wire centers. End-to-End Edge automation and Zero-Touch provisioning are required to minimize OPEX and meet the requirements for provisioning agility.

The Akraino Edge Stack is intended to support any type of access technologies such as Wireless (4G/LTE, 5G), Wireline, Wi-Fi, etc.

Acumos AI[20] is a platform and open source framework that makes it easy to build, share, and deploy AI apps. Acumos standardizes the infrastructure stack and components required to run an out-of-the-box general AI environment. Acumos is part of the LF AI Foundation, an umbrella

[20] https://www.acumos.org/

organization within The Linux Foundation that supports and sustains open source innovation in artificial intelligence, machine learning, and deep learning while striving to make these critical new technologies available to developers and data scientists everywhere.

Acumos empowers data scientists to publish adaptive AI models, while shielding them from the need to custom develop fully integrated solutions. AI models can be acquired from the marketplace, trained, graded on their ability to analyze datasets, and integrated, automatically, into completed solutions. They can access encapsulated AI models, without knowing the details of how they work, and connect them to a variety of data sources, using a range of data adaptation brokers, to build complex applications through a simple chaining process.

Acumos employs the open source collaboration model to achieve flexibility and create a highly adaptable industry-wide framework for building, training, integrating and deploying machine learning solutions. Acumos breaks the development flow into four distinct steps:

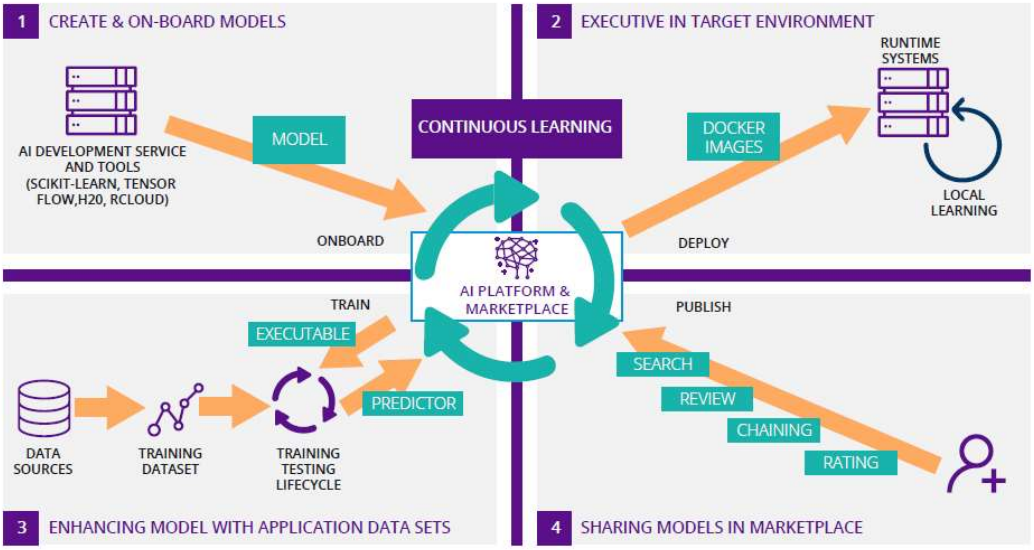


Figure 22 - Acumos Development Flow

Some applications of Acumos include:

- **Networking** - where network operators must contend with anomalies in the flow of traffic across systems and networks. These anomalies may occur during periods of peak demand or when demand shifts from one geographical area to another or when it shifts from one application to another. Machine Learning algorithms can be used to identify the normal flow of traffic through a network and identify whenever that normal pattern changes. By responding quickly to such changes, a network can adapt quickly, as necessary, so as to minimize the impact of a change on customer experience.
- **Failure Detection & Recovery** - failures in network links or sudden loss of servers occur due to either hardware or software failures, a traffic anomaly will follow. An automated response based upon the detection of such a networking anomaly can provide rapid replacement or rerouting of service to correct the failure.

- **Security** - Machine learning can be employed as an effective countermeasure to many such threats, including both known and unknown attacks. AI software can learn new patterns of attack, as they occur, by detecting sudden changes in data traffic and comparing them to earlier experiences in order to select and deploy countermeasures. Not only could such software adapt to entirely new threats, as they are launched, but the software can also become better at detecting security threats as it learns from each successive threat. Machine learning based analytic software could be installed once and continue to improve its responses over time based upon experience, so companies would not be required to continuously install updates and patches in order to keep ahead of the latest threats.
- **Software Scanning** - Machine learning can also be applied to the task of actively scanning software, systems and networks for vulnerabilities. Weaknesses in design of software and networks could be detected and repaired even before they are exploited. This scanning could include searching for insecure operating system versions or detecting packets from unsecured sources entering restricted areas of a network or probing for ports and addresses that should be blocked, but are not.
- **Customer Care** - Chatbots are already making use of flagged words to automate customer support interactions by taking customers through a scripted interaction based upon keyword matching. This technology can be extended to support topic models which classify natural language queries against a learned set of topic categories. By aggregating and scoring customer responses to an interaction with human agents, a machine learning algorithm can automatically "answer" a customer's question, classifying the customer request to a known topic and playing back a human's response, recorded earlier, to a similar question.

SDN separates the control plane from the data plane freeing software innovation cycles to become independent of hardware innovation cycles. SDN accelerates Internet and Cloud innovation while significantly reducing the costs of building and operating networks. ONOS[21] is the an SDN controller platform that supports the transition from legacy "brown field" networks to SDN "green field" networks. This enables exciting new capabilities, and disruptive deployment and operational cost points for network operators.

[21] https://onosproject.org/

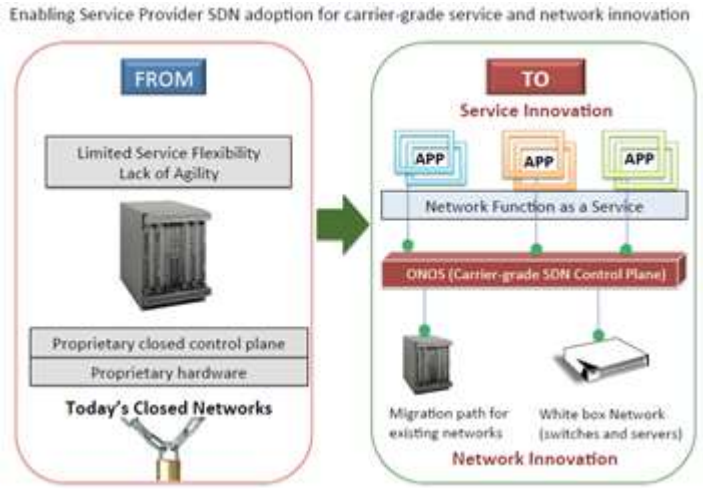


Figure 23 - ONOS Vision of Service Provider Network

ONOS has enabled the SDN revolution. Combining ONOS with white box switches and ONOS applications enables new forms of innovation never before possible with closed legacy networks. CORD™ (Central Office Re-architected as a Datacenter) is delivering edge cloud for operators, reinventing the edge of operator networks in cloud-native ways for efficiency and agility. By blending the best of Cloud, SDN and NFV, CORD provides complete integrated solutions for fixed access Passive Optical Network (PON), mobile and wireless 5G access, mobile core (EPC) and enterprise service delivery. CORD combines NFV, SDN, and the elasticity of commodity clouds to bring datacenter economics and cloud agility to the Telco Central Office. CORD lets the operator manage their Central Offices using declarative modeling languages for agile, real-time configuration of new customer services. ODTN (Open Disaggregated Transport Network) is disaggregating carrier core networks, and reassembling a solution using SDN principles and white box efficiencies to build high performance backbones with disruptive economics.

5.12.3 Service Mesh

Service mesh is an implementation technology often seen in virtualized networks outside telecommunication networks; however, it is considered here as the 3GPP Release 16 specifications identified how aspects of the 5G core may use a service mesh to implement the 5GC functions.

A service mesh provides the ability to effectively manage the complexity involved in micro-service deployment. Any interactions between those micro-services that may be part of the same network function and also interactions with external applications can be managed by the service mesh. Some of the key features of a service mesh include the ability to discover other micro-services, perform load balancing, collect metrics, monitoring and the ability to proxy mutual TLS authentication and authorization on behalf of micro-services.

An example of a service mesh is Istio, an open source effort that describes a control plane and data plane. The control plane consists of Citadel, Pilot and Gallery. Citadel is an in-built certificate authority (CA) that is used for life-cycle management of certificates used for mutual

TLS (mTLS) communications between the various micro-service pods. Citadel can be interfaced with an operator's PKI, to operate as an intermediate CA. Pilot is used for policy configuration, which may include authentication and authorization rules associated with each micro-service pod.

A special sidecar proxy also referred to as envoy side-car proxies, forming part of the data-pane may be injected into each micro-service pod. The envoy proxies are used to intercept of all network communication on behalf of the micro-service, and perform mTLS communications between envoy proxies in different micro-service pods.

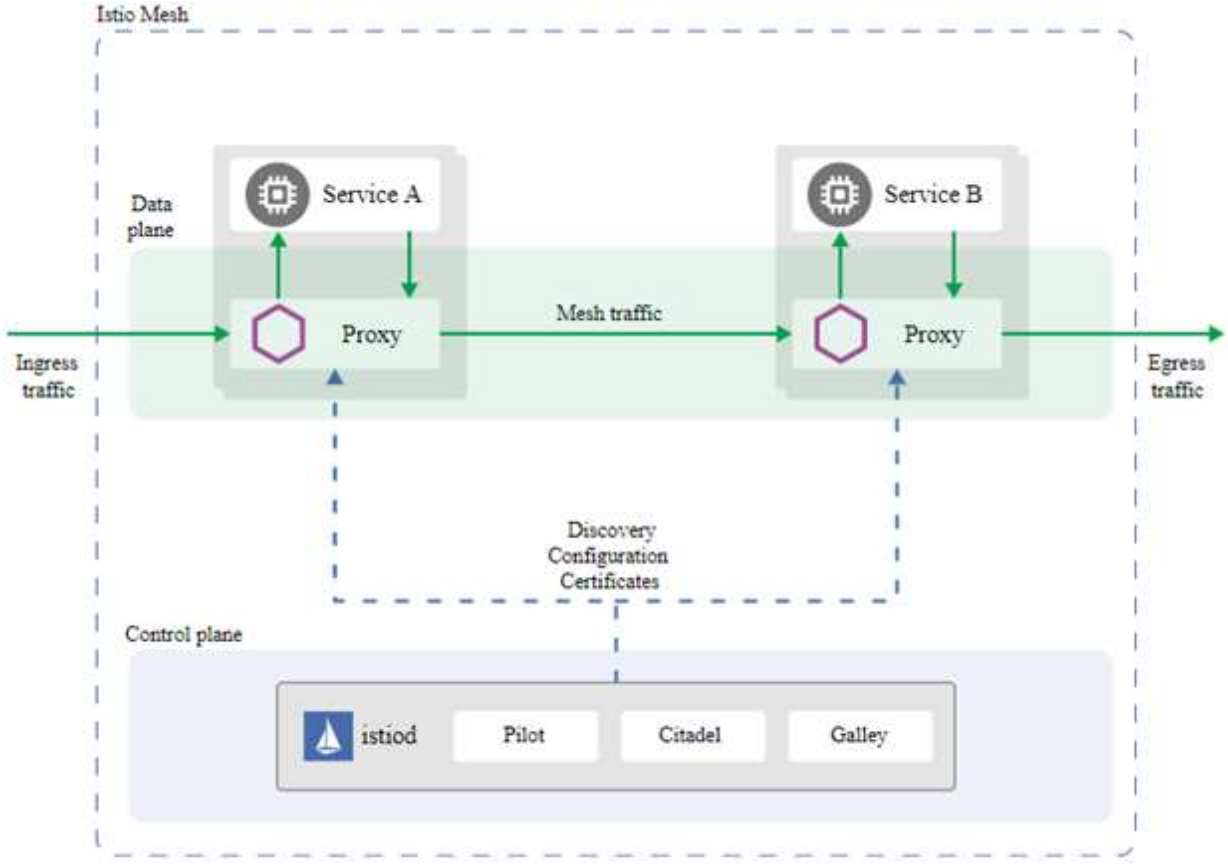


Figure 24 - Istio Architecture[22]

5.13 NIST and ISO 27001

Security standards development continues to be an area of focus by industry in collaboration with government entities. Leveraging the Cybersecurity Framework23 NIST is active in their efforts to address security risk management and 5G security, as well as the International Standards Organization (ISO). The items below highlights some of these efforts:

1. NIST, https://www.nccoe.nist.gov/events/workshop-5g-cybersecurity-preparing-secure-evolution-5g
2. ISO 27001, https://www.iso.org/isoiec-27001-information-security.html

[22] Source: https://istio.io/docs/concepts/what-is-istio/
[23] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

ISO/IEC 27001 is the best-known standard in the ISO family of standards providing requirements for an Information Security Management System (ISMS).

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process and is relevant to 5G.

Both ISO 27001, the NIST Cybersecurity Framework and related standards are complementary security risk management regimes that are relevant to 5G security as industry evolves and transitions from 4G to 5G.

5.14 NIST Standards and IoT

The NIST 8259 publication describes voluntary, recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. This standard describes six voluntary, but recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers.

- Four out of six activities primarily impact decisions and actions performed by the manufacturer before a device is sent out for sale. The remaining 2 activities impact decisions and actions performed by the manufacturer after device sale.
- Pre-market activities: identify expected customers and define expected use cases; research customer cyber goals; determine how to address customer goals; and plan for adequate support of customer goals.
- Post-market activities: identify expected customers; decide what to communicate and how to communicate it.

The 2nd draft [Ref 11] has made changes to Table 1 in 8259, but is still very similar to the first draft. Notable changes include:

- NIST has removed the “Rationale” column from the table, which previously explained why the device cybersecurity capability was included in the core baseline.
- NIST has updated its “Reference Examples” to include references to IoT device cybersecurity guidance documents from the Council to Secure the Digital Economy (CSDE), the Cloud Security Alliance (CSA), the International Electrotechnical Commission (IEC), the Internet Society/Online Trust Alliance (OTA), and the Platform Security Architecture Joint Stakeholder Agreement (PSA).
- The updated version of the table has moved the defined terms so they are included on the page where the defined term is used first, rather than at the end of the table

The NIST 8228 publication identifies three high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices.

- Many IoT devices interact with the physical world in ways conventional IT devices usually do not.
- Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
- The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices.

Cybersecurity and privacy risks for IoT devices can be in terms of three high-level risk mitigation goals, such as:

1. Protect device security. In other words, prevent a device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.
2. Protect data security. Protect the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device except those without any data that needs protection.
3. Protect individuals' privacy. Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection. This goal applies to all IoT devices that process PII or that directly or indirectly impact individuals.

5.15 Zero Trust Architecture (ZTA)

On February 2019, FCIO Council and NIST and volunteers from other agencies have launched a project to address Federal initiative for adoption of Zero Trust principles and approaches for securing USG. The draft out is NIST SP 800-207[24], "Zero Trust Architecture".

On September 2020, National Cybersecurity Center of Excellence (NCCoE) and the industry collaborated to implement an enhanced identity governance based ZTA solution at NCCoE. Also, a lab is provisioned to build a base network infrastructure for the NCCoE project, Testing and upgrading components, and integrate ZT Components and test capabilities.

The tenets of Zero Trust are:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-connection basis.
- Access to resources is determined by dynamic policy - including the observable state of client identity, application, and the requesting asset - and may include other behavioral attributes.
- The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of

[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

network infrastructure and communications and uses it to improve its security posture.

Figure 25 shows a traditional single perimeter defense with threats from Internet as well as insider attack.

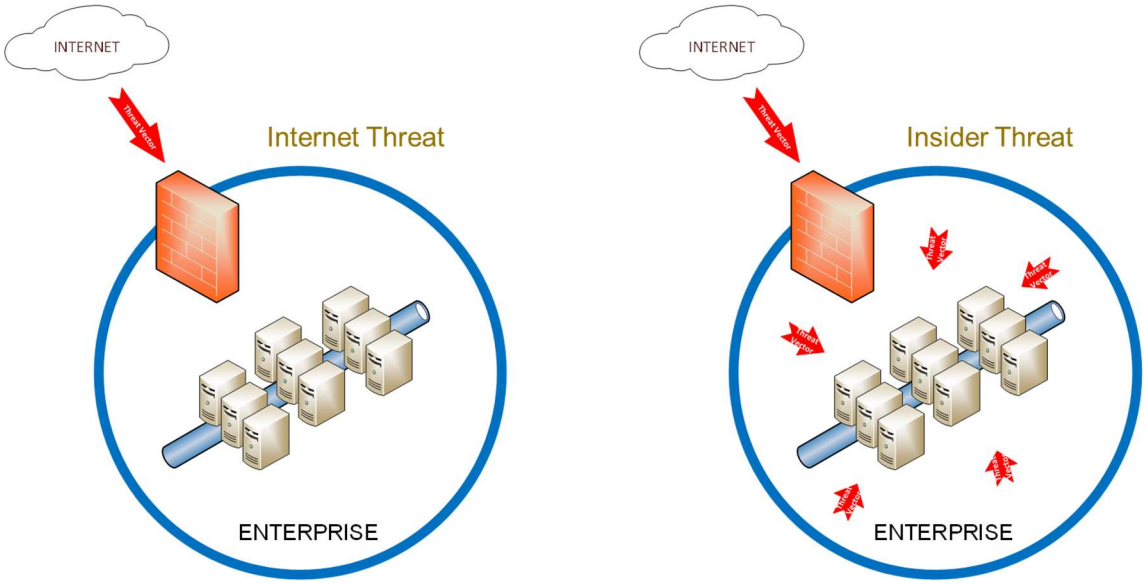


Figure 25 - Traditional Single Perimeter Defense

Figure 26 shows Zero Trust perimeter defense approach focuses on data protection, assuming no implicit trust in the perimeter.

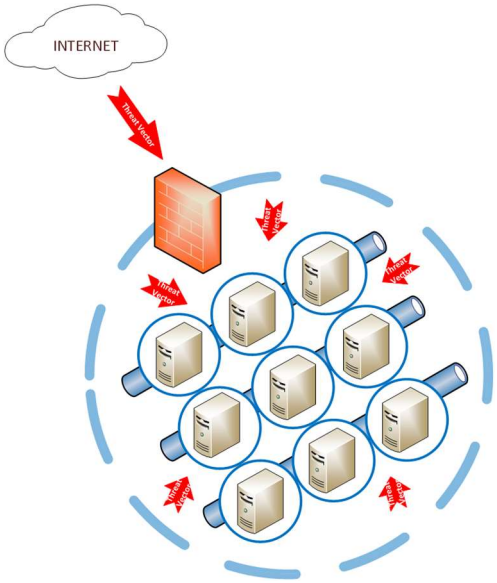


Figure 26 - Zero Trust Perimeter Defense Approach Focuses on Data Protection

While the specific features of ZTA has been developed for implementation within enterprise networks, there are several areas where this may overlap with the capabilities of 5G deployments. For the operator of the 5G network, many aspects of the management systems (e.g., billing, subscriber management, network management, etc.) are typically implemented on

enterprise platforms using commercial systems; for these the principles of ZTA are directly applicable and relatable. Additionally, the introduction of functionality to support private networks in Releases 16 and 17 may result in some 5G functions implemented inside ZTA networks.

A casual review, however, of 5G specifications however show that the concepts of ZTA have influenced development of those 5G specifications and affected the architecture and security systems – for example previous generations implicitly trusted roaming partners, placing the perimeter of defense around the outside of the PLMN operator's "club", in 5G architecture the SEPP places the perimeter of defense around a single PLMN (effectively the ZTA concept at a macro system level). Additionally, within an individual PLMN, some tenets of the ZTA can be realized with the introduction of 5G capabilities (e.g., network slicing to ensure functional separation, per NF authentication, and encryption of NF to NF traffic flows), but 5G architecture does not yet address all of the capabilities required to be described as ZTA.

Further analysis is needed to see what degree (if any) of ZTA should be required for 5G networks, and what changes to the 5G specifications would be necessary to support those ZTA concepts in typical network deployments, and future deployments in 3GPP Non-Public Networks.

5.16 CSRIC VI

CSRIC VI released a report on 5G Security.[25] This report was published in two March of 2018, with an addendum submitted in December 2018.

The FCC asked CSRIC VI to look at four areas and identify vulnerabilities and risks in each of those 4 areas:

- Network Function Virtualization (NFV)
- Open Source Software
- Internet of Things (IoT)
- Supply Chain

The supply chain section was submitted in December 2018.

CSRIC VI was only able to consider R15 for this report, as work on R16 had not begun. There are architectural additions and changes made in R16, and therefore it was the recommendation from CSRIC VI that the FCC continue researching 5G risks and vulnerabilities in the next CSRIC charter.

The recommendations that were made for each of these four areas can be found in the full report.

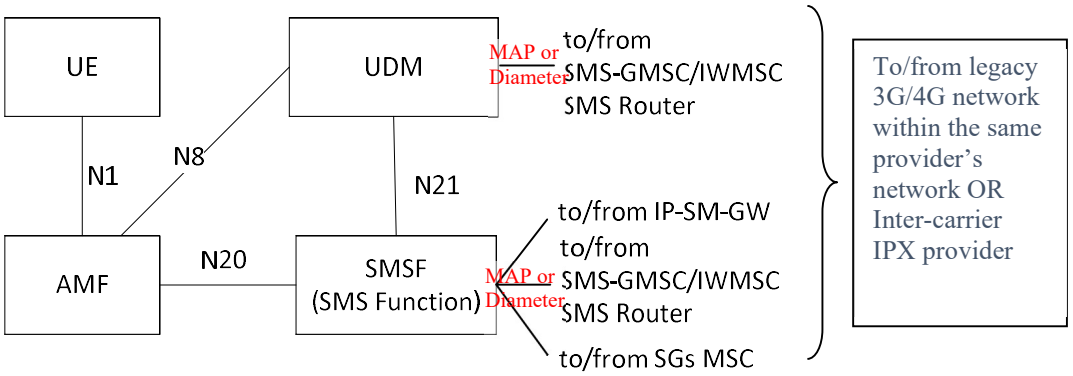
5.17 Use of Legacy Protocols in 5G for SMS

In 5G networks, the SMS Function (SMSF) supports the transfer of SMS over the Non-Access Stratum (NAS). In this capacity, the SMSF will conduct subscription checking and perform a relay function between the device and the SMSC (Short Message Service Centre), through

[25] https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

interaction with the AMF (Core Access and Mobility Management Function). The SMSF (SMS Function node) is like the MSC/VLR in 3G/4G. It relays Mobile Originated and Mobile Terminated SMS messages between a 5G subscriber and legacy 3G/4G networks. The SMSF to SMSC/SMSGW interface is based on the MAP (Mobile Application Part) protocol specified in 3GPP TS 29.002. It optionally may be based on the Diameter reference point SGd per 3GPP TS 29.338.

Other interfaces based on legacy protocols such as Gy / Ro Diameter interfaces between OCS and CHF, PFCP on N4 interface and GTP on S5 interfaces may be used in non-standalone architectures.



N8: Reference point for SMS function address retrieval and SMS over NAS service authorization between AMF and UDM
N20: Reference point for SMS transfer between AMF and SMS Function
N21: Reference point for SMS subscription retrieval between SMS Function and UDM

Figure 27 - SMS 4G/5G Interoperability

AMF (Access and Mobility Management function node) is like the MME in 3G/4G network. The AMF provides the path for Mobile Originated or Mobile Terminated SMS for a 5G subscriber over the encrypted NAS protocol.

5.18 Security Work Done in Research/Academia

The focus of a paper on "Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks" [Ref 10] is on analyzing the security and privacy of the cellular paging protocol with respect to the quality-of-service and battery consumption of a device. The paper claims that attacks against this protocol can have severe repercussions, for instance, allowing attacker to infer a victim's location, leak a victim's IMSI, and inject fabricated emergency alerts. It analyses the underlying design threats and propose approaches to address them.

The paper analyses the Attach procedure as shown in Figure 28. When a UE is switched on with a valid SIM card, it first scans the network and selects the base-station that satisfies its selection criteria. To establish a connection with the core network, the UE then sends an attach_request message to the MME, containing its IMSI/TMSI and the supported cipher suites. The UE and the core network authenticate each other using a challenge-response protocol (using a pre-

installed symmetric master key in the SIM card) and then negotiate the cipher suite to be used for encryption and message authentication based on their individual capabilities. Finally, the MME completes the attach procedure by sending an encrypted and integrity protected attach_accept message containing the UE's TMSI.

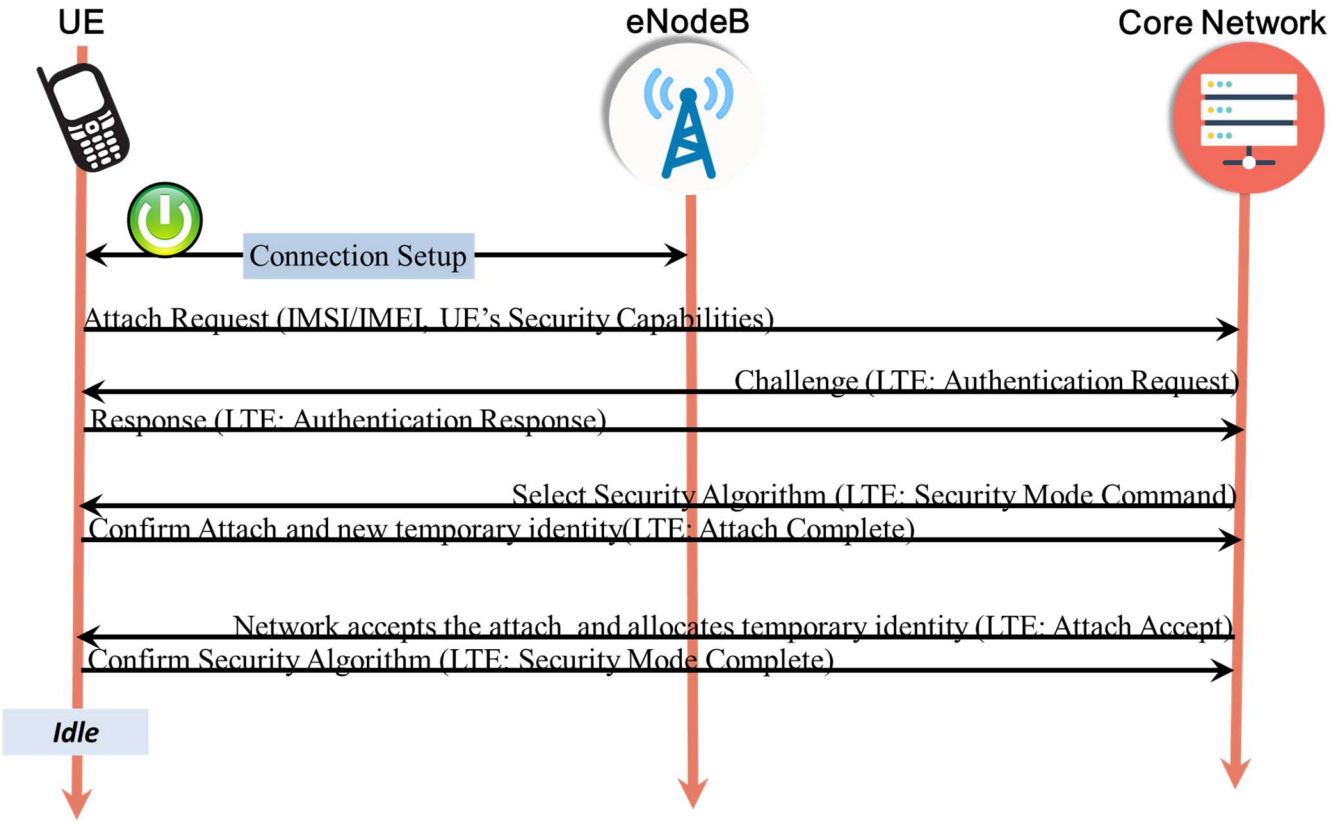


Figure 28 - Attach Procedure

The paper then analyses the paging and detach procedures, as shown in Figure 29, that allows a UE to enter a low power-consumption mode only when there are no uplink or downlink messages for a pre-defined amount of time. The paper also describes paging cycle as when in idle mode, the UE periodically wakes up to check if there is any notification for pending service(s). Finally, it describes paging frame as the radio frame at which the UE wakes up in every paging cycle to check for a paging message. The specific subframe of the paging frame at which the UE wakes up is also computed. The paging frame and the sub-frame together form a UE's paging occasion.

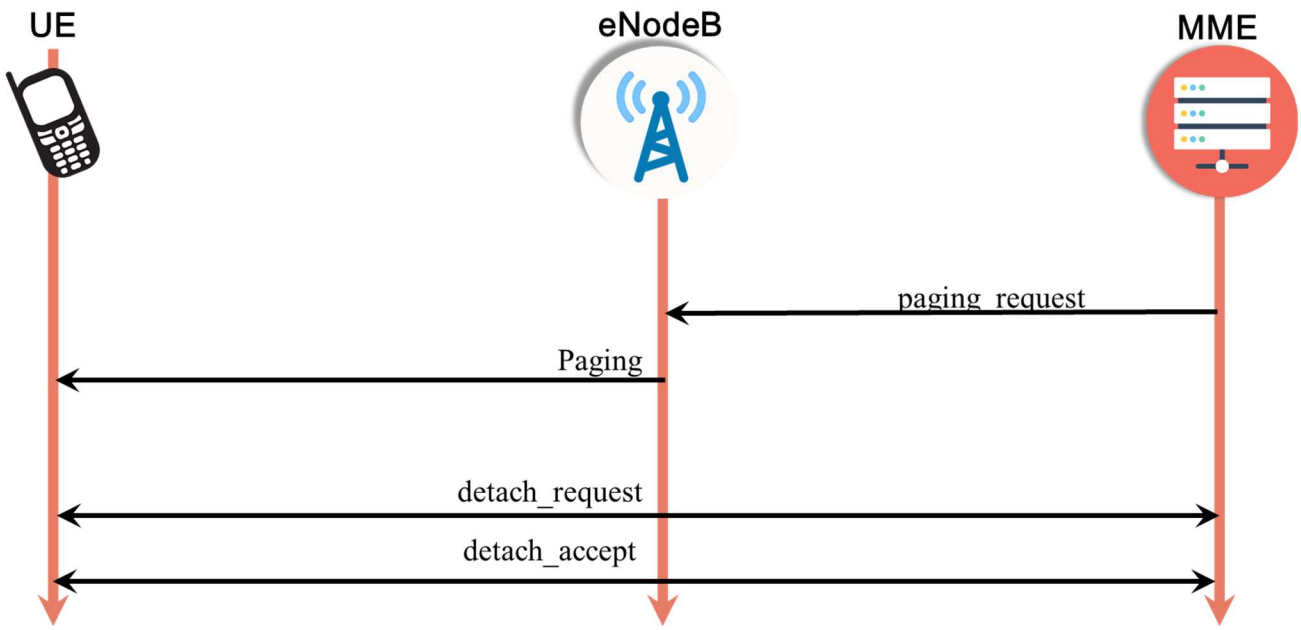


Figure 29 - Paging and Detach Procedures

The paper then concludes that fundamental weakness in 4G paging protocol. For a particular device in a specific cell, the time intervals when the device wakes up from the low-power state to check for paging messages (i.e., the paging occasions) are fixed. This is because the paging occasion is computed from the device's persistent IMSI. This essentially exposes side-channel information which is shown to be exploitable by the ToRPEDO (TRacking via Paging mEssage DistributiOn) attack. So, the paper concludes that 4G is vulnerable because paging contains IMSI as device identifier. Also, the infrequent update of TMSI could expose the location of the UE.

While in 4G, it is optional to refresh the temporary identifier - the S-TMSI - after paging, in 5G networks it becomes compulsory to refresh the 5G-S-TMSI. Furthermore, it is also compulsory to allocate new 5G-S-TMSI at initial registration and mobility registration update procedures. But, the paper authors claim that since the configuration update procedure requires additional interactions between the device and the core network, the upcoming 5G deployments may similarly try to get away without introducing such additional interactions and run into similar issues as 4G operational networks – thus becoming susceptible to location tracking attacks.

The authors have developed a tool called LTEInspector for "A Systematic Approach for Adversarial Testing of 4G LTE" as shown in Figure 30.

Based on the analysis, the paper does not introduce new attacks. The previously identified vulnerabilities continue under industry review and assessment. The network-side attacks were validated using a core network built with open source software and Software Defined Radio (SDR). For UE side attack validation, a real 4G networks was used to which the UE was initially connected and, using a fake eNodeB, malicious packets were injected to that target UE.

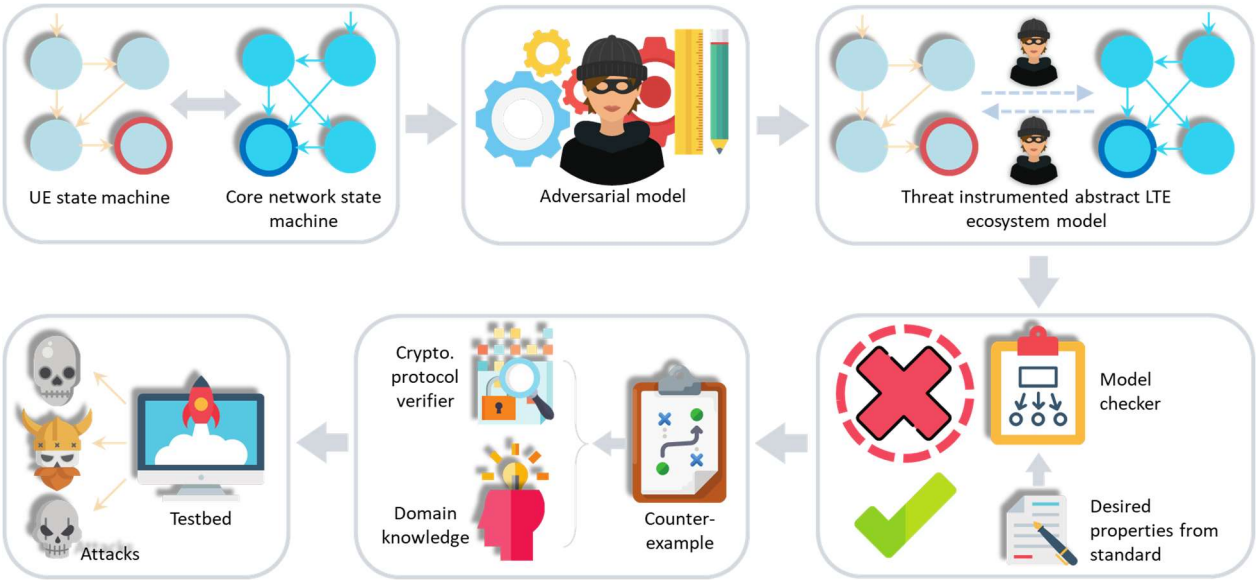


Figure 30 - LTEInspector: "A Systematic Approach for Adversarial Testing of 4G LTE"

5.19 Supply Chain Security Management

In October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) launched the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. Chartered under the National Infrastructure Protection Plan Framework and the associated Critical Infrastructure Partnership Advisory Council (CIPAC), the Task Force's efforts are directed by a collaborative leadership team with representatives from CISA and the Communications and Information Technology Sectors. The Task Force's constituent Working Groups are comprised of sector members, subject matter experts from those sectors, and representatives from across the government.

The Task Force's combination of industry and governmental expertise has yielded strong results in its first year. These results were captured in an interim report published in September of 2019[26] highlighting impacts of the Task Force's overall mission on supply chain risk management. This report details the Task Force's methodologies, areas of discussion, and, where appropriate, key findings, recommendations, and potential areas for further study identified by each of the Task Force's Working Groups (WG). Working Groups continue to address areas of significant policy concerns related to SCRM challenges, including:

- The timely sharing of actionable information about supply chain risks across the community;
- The understanding and evaluation of supply chain threats;
- The identification of criteria, processes and structures for establishing Qualified Bidder Lists (QBL) and Qualified Manufacturer Lists (QML);

[26] INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT, Status Update on Activities and Objectives of the Task Force, September 2019

- Policy recommendations for incentivizing the purchase of ICT from original equipment manufacturers and authorized resellers; And
- The development of templates vendors can use to self-attest to supply chain practices.

The findings and recommendations of the Working Groups from this past year will be foundational to the Task Force's second year of activity. In its next phase, the Task Force and the Working Groups will continue to support efforts by the Federal Government and industry to manage ICT supply chain risk.

5.19.1 Summary of other Government 5G Efforts

5.19.1.1 Federal Acquisition Security Council (FASC)

The Federal Acquisition Security Council looks to collect data on supply chain threats and help agencies counter such threats through guidance. The FASC will prioritize the development of guidance in 2020 to help agencies address threats to the supply chain. The Federal Acquisition Supply Chain Security Council is authorized to issue "Exclusion and Removal Orders" prohibiting or removing certain suppliers. Title II of the SECURE Technology Act, the Federal Acquisition Supply Chain Security Act of 2018, creates the FASC. The FASC is led by the Office of Management and Budget (OMB) and interim guidance is expected in 2020.

5.19.1.2 Department of Commerce

The Bureau of Industry and Security (BIS) establishes the Entities List, where BIS evaluates license applications to any listed entity, regulates the export of sensitive goods, enforces export controls, including anti-boycott and public safety laws. This program has the authority to prohibit commercial transactions, trade, and has critical effects to the global supply chain. The Department of Commerce issued a NPRM to implement a new authority "on a case-by-case basis." Public comments were filed in January 2020. Possible rules and prohibitive actions will follow. BIS added Huawei and 68 non-USA Huawei affiliates to the BIS Entity List, effective May 2019. BIS issued a Temporary General License through February 2020, and again for another 45 days through April 1st, 2020, partially restoring the previous licensing requirements and polices for export, re-export, and transfer of items subject to the Export Administration Regulation (EAR) to Huawei and the 68 affiliates.

5.19.1.3 NIST- Supply Chain Risk Management

NIST developed SP 800-161, Supply Chain Risk Management (SCRM) Practices for Federal Information Systems and Organizations. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT SCRM into federal agency risk management activities by applying a multi-tiered, SCRM – specific approach, including guidance on supply chain risk assessment and mitigation activities.

5.19.1.4 Executive Order (EO) 13873 Securing the Information and Communications Technology and Services Supply Chain

Executive Order (EO) 13873, in May 2019 declared a national emergency on exploitation and vulnerabilities in ICT technology via foreign adversaries. The EO prohibits any "...acquisition, importation, transfer, installation, dealing in, or use of any ICT technology or service

(transaction) subject to jurisdiction within the USA". The EO prohibits transactions with "foreign adversaries".

5.19.1.5 Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) issued a Supply Chain Notice of Proposed Rulemaking (NPRM) where it proposed prohibiting use of Universal Service Fund (USF) support on equipment and/or services from companies that pose "national security threats". The FNPRM proposes a replacement program and asks a number of additional questions about the prohibition. In October 2018 the FCC unanimously adopted NPRM prohibiting USF money to purchase equipment or services from certain providers (widely understood to be Huawei and ZTE). In November 2019 the FCC adopted an Order prohibiting USF money specifically naming Huawei and ZTE and USF and required USF recipient certification to that effect

5.19.1.6 Department of Defense (DoD)

DoD Cybersecurity Maturity Model Cybersecurity (CMMC) sets cybersecurity standards for DoD contractors. While focused on vendors' cybersecurity generally, rather than supply chain security specifically, CMMC will influence federal procurement requirements outside DoD and regulatory requirements for supply chain assurance and attestation. The CMMC Version 1.0 was released January 2020 and the CMMC Accreditation body has been established.

6 Analysis and Recommendations

6.1 Analysis

6.1.1 Device Management in 5G Networks

5G devices have a potential to be deployed from consumer-based use cases to mission critical scenarios supporting healthcare, factory automation, infrastructure monitoring. With all the use cases being discussed for 5G there is a potential to add millions of devices to 5G networks. With such a large number of devices, device management on 5G networks becomes a critical aspect of deployment.

Following are key mobile equipment security areas that need standardization:

- Guaranteeing a device's integrity, privacy, and confidentiality.
- Ensuring controlled access to data.
- Preventing the connected device from being stolen or compromised, and the data from then being compromised or used as a tool for aggression.
- Authentication and authorization on the interface between the network and the operator.

There is a critical need to create a comprehensive device security management system for 5G heterogeneous networks. Following areas should be considered for developing standards

- A policy-based security management system,
- Leverage Artificial Intelligence (AI) to detect malicious or anomalous device behavior, and
- Leverage device management capabilities to act as a policy feedback loop.

6.1.2 Subscription Identifier Privacy

Already at the outset of defining what new capabilities 5G networks would bring, it was known that devices sometimes called "IMSI catchers" or cell site simulators could interfere with cellular wireless connections and gather information about the location of subscribers or, in some cases, intercept communications. For instance, IMSI catchers are so called because they catch the long-term identifier IMSI (International Mobile Subscriber Identifier) which may be used to detect the presence of a subscriber in the vicinity. In this section we will focus on the location privacy aspects and only mention that other measures, starting with mutual authentication between UE and network (introduced already in 3G) and strengthening of interconnect security, address interception of communications. Tracking of subscribers by passively monitoring air interface has long been mitigated by the use of temporary subscription identifiers, that can be changed, making tracking difficult. However, some issues had remained. One issue has been long lasting temporary subscription identifiers, which end up effectively becoming yet another long-term subscription identifier. A more difficult challenge has been the need for the UE to report its long-term subscription identifier initially, and its use in some other situations. IMSI catchers could detect the presence of a particular subscriber, if the long-term subscription identifier is known, by monitoring the uplink, either through passively listening or through actively interacting with the UE. More recently, academic work has also described

potential methods for inferring the presence of subscribers from downlink paging messages [Ref 9]. All these cases have been addressed in 5G specifications.

To address the first issue, 5G specifications are stricter about refreshing temporary identifiers. For instance, 5G specifications make it mandatory to refresh the temporary subscription identifier (called 5G-GUTI) at certain events, thus, ensuring that it becomes practically unattractive to attackers.

5G specifications also addressed the issue with long-term subscription identifiers. In previous systems, the long-term subscription identifier is the IMSI, consisting of a Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Identification Number (MSIN). In 5G, the long-term subscription identifier is generalized as the Subscription Permanent Identifier (SUPI). The type of SUPI is either the IMSI or a network-specific identifier (in Network Access Identifier format consisting of user name and realm) [Ref 1]. In 5G, from the outset, new techniques based on asymmetric crypto were introduced so that the SUPI is concealed on the uplink, even when the UE initially establishes connection with the network using registration procedure [Ref 3][27]. These new techniques work as follows.

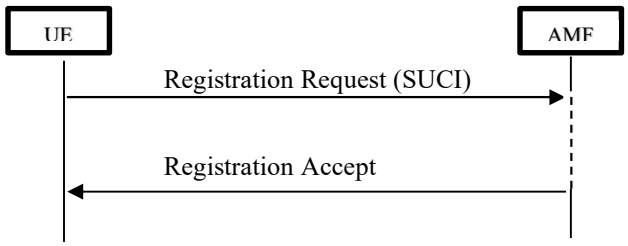


Figure 31 - Use of SUCI instead of SUPI in uplink registration request message in 5G. Simplified procedure illustration [Ref 2]

Each UE is provisioned with its SUPI and its home network public key. To keep the explanation simple here, we assume the case where SUPI is of type IMSI. Instead of sending the SUPI, a (partially) concealed identifier known as the Subscription Concealed Identifier (SUCI) is sent, where the MCC and MNC are kept in the clear, so that the home network can be located, but the MSIN is concealed. To construct the SUCI, the UE generates an ephemeral public/private key pair. The ephemeral private key and the home network public key are used to derive an ephemeral symmetric key which is used to encrypt the MSIN for inclusion in the SUCI [Ref 3]. In the SUCI, the ephemeral public key is transmitted together with the encrypted MSIN and a MAC tag to enable detection of modifications, and the use of the ephemeral private key ensures that the encrypted MSIN (i.e., SUCI ciphertext) is different each time for the same MSIN.

If the UE is not already authenticated, the AMF can request the AUSF to authenticate it, and the AUSF will request a translation of the SUCI to the corresponding SUPI from the UDM and once the UE has been authenticated return the SUPI to the AMF [Ref 2]. Having the SUPI, the AMF can then assign a temporary identifier for the UE, the 5G-GUTI (Globally Unique Temporary Identifier), which will be used in further communications (in conjunction with other temporary identifiers).

[27] Also, in Blog: https://www.ericsson.com/en/blog/2017/6/protecting-5g-against-imsi-catchers

5G also improved another procedure called subscription identification procedure which is used by the network when the UE cannot be identified with temporary subscription identifier. Upon receiving a NAS Identifier Request message asking the UE for its subscription identifier Figure 32, the UE constructs the SUCI as described above and sends the constructed SUCI in the response.

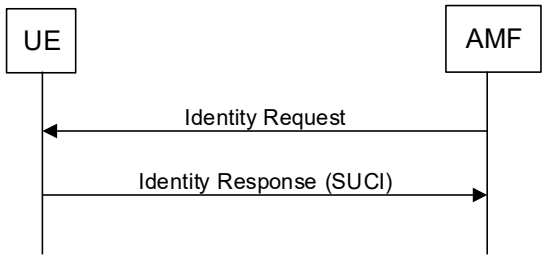


Figure 32 - Subscription identification procedure [Ref 3]

The new protection afforded by the SUCI is optional to use by the network, as the encryption scheme to use is under network control and it can choose to use a null scheme [Ref 3]. In order to use SUCI protection, the home network also needs to provision its Home Network Public key in the USIM.

Finally, the previously mentioned potential to infer the presence of certain subscribers by monitoring downlink paging messages is also avoided by making use of temporary subscription identifiers instead of a long-term subscription identifier. One important step was to move away from using either a temporary (S-TMSI) or a long-term subscription identifier (IMSI) as paging identifier, transmitted in paging messages. In 5G, only temporary subscription identifiers, either 5G-S-TMSI or I-RNTI (Interactive Radio Network Temporary Identifier), are used [Ref 5]. Moreover, the previously mentioned inference method was based on observing which paging timings were being used in a cell and exploiting the fact that long-term subscription identifiers were used to derive which timings to transmit on (and that the UE should listen on). These derivations have been changed to only use temporary subscription identifiers, i.e., the 5G-S-TMSI [Ref 1][28]. By changing the paging timing calculations to base them on the temporary subscription identifier, augmented by stricter requirements on when those need to be refreshed, the possibility of inferring a link to the permanent subscription identifier is avoided.

Besides privacy enhancement on subscription identifiers, it is also worth mentioning that 5G, by design, reduces as much information transferred in clear-text as possible that may lead to identification/tracking of subscriber. An example of which is that in the initial message from UE to the network, only a minimum set of information is sent in clear-text and the rest is either sent concealed or sent later when security has been established.

[28] Also, in Blog: https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy

6.1.3 Risks of Open Source in 5G

Open source software is incorporated into applications in many ways, and often an operator will not know where open source is used. When open source is used as the foundation for a vendors' product, any vulnerabilities could threaten the integrity of the vendors' solution. Open source software provides attackers with a target-rich environment because of its widespread use. This means vendors must ensure they have mechanisms in place to monitor Common Vulnerabilities and Exposures (CVEs) against any open source software components that they may use in their own products. Vendors must test and perform security assurance assessments on all open source software and bug fixes. Vulnerabilities such as Heartbleed were exploits that targeted open source software vulnerabilities, threatening systems using the open source code. According to the BlackDuck report, 67% of vulnerabilities discovered in open source code were known for more than four years. 52.6% of vulnerabilities were considered as high-severity by NIST. Open source vulnerabilities are published on sites such as the National Vulnerability Database (NVD) and are public documents. Network operators should be monitoring this as well and should understand where their vendors are using open source.

Use of open source will continue to increase as operators and vendors rely on open source software to speed delivery of new solutions and reduce TCO. Open source software can be viewed as being analogous to corporations outsourcing functions not related to their core competencies. This introduces a new set of security challenges in terms of keeping a consistent and coherent assurance of security-by-design, and prevention of resulting security flaws. To compound this issue, asking vendors to disclose the open source components used in their products may disclose more vulnerabilities and add to the risk. Note that many times while there may be a vulnerability in a specific software component, that vulnerability may only exist as a stand-alone component, and may be nullified when incorporated into the vendors' solution (through middleware where the open source component is isolated, for example). Care must be given in how open source components are disclosed to prevent exposure.

It is important to note that 3GPP has defined a Suite of Security ASsurance (SCAS) tests for 3GPP defined virtualized NFs to verify and certify the integrity of these nodes.

6.1.3.1 Threat Assessment for Open Source in 5G

While the use of open source offers benefits to enterprises and development teams in terms of time to market, cost and reliability, it also can be the source of vulnerabilities that pose significant risk to application security. Many development teams rely on open source software to accelerate delivery of digital innovation. Both traditional and agile development processes frequently incorporate the use of prebuilt reusable open source software components. As a result, some organizations may not have accurate inventories of open source software dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open source.

Open source allows for platform design that is crowdsourced by global stakeholders. Merely hiding source code does not counter attacks; "people who break software don't actually need to look at the source code". Even when the original source is necessary for in-depth analysis,

making source code available to the public significantly aids defenders and not just attackers. Continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized by the core development team. Use of any commercially-available software, be it proprietary or OSS, creates the risk of executing malicious code embedded in the software. OSS projects have a "trusted repository" that only certain developers (the "trusted developers") can directly modify. Since the source code is publicly released, anyone can review it, including for the possibility of malicious code.

As touched upon already, SW can be attacked without access to the source code. But the point about openness to review deserves some further consideration. While open source development brings both real and potential security benefits, it should be recognized that there is mounting evidence that some of the promoted benefits may not pan out in practice and need to be balanced against some very real drawbacks.

- A real or perceived advantage in cost and innovation speed from using OSS components leads many development organizations to make use of the same OSS components. (Generally speaking, reuse can bring development cost down and innovation/development speed can benefit from not having to reinvent/reimplement common functionality. One may also note that OSS is not the only way to achieve reuse, and other approaches may have some of the same advantages and disadvantages attached.) However, many organizations using the same code base for components results in increasing tendencies towards SW monocultures – at least in parts of systems. The security risks associated with mass exploitation of identified vulnerabilities in SW monocultures are well known and have been demonstrated historically many times over.

- While it is clearly beneficial to allow for more people to participate in security reviewing code, the question is how much deep review actually gets performed of the majority of open source code [Ref 12]. The discoveries of high impact vulnerabilities that have existed in widely used open source code for many years suggests that open source code is possibly neither more or less secure than other code[29].

- Due to high complexity and low tolerance for errors impacting services, typically all changes to telecom components require extensive system level testing to verify there are no unexpected side effects. Naturally, this also applies to changes to address uncovered security vulnerabilities, meaning developing and rolling out patches is not a quick process as it might be for some other types of SW.

- The discoveries of vulnerabilities have a tendency to occur in (possibly diffuse) waves following the discovery of a class of vulnerability. For instance, once the principles behind stack buffer overflow vulnerabilities and how they may be exploited became more widely known, followed a flood of discoveries of instances in various code. Based on the discovery of stack buffer overflow attacks, also followed discoveries of variants of vulnerabilities involving heap rather than stack memory, as well as other unsafe coding practices, and so on. With each discovery of a class of vulnerabilities follows

[29] See https://dodcio.defense.gov/Open-Source-Software-FAQ/

high activity to find instances of such vulnerabilities. For good and bad, this process is vastly simplified if the source code is available. Thus, while on the positive side, an open source community can – at least in principle – collaborate to find and remedy such new vulnerabilities, an adversary can then also do this much more quickly and easily than if the source code is unavailable. Thus, any time advantage a code maintainer might have from access to source code is lost.

6.1.3.2 Threat Mitigation for Open Source in 5G

For larger enterprises with multiple and vast repositories of code, identification of all of the applications where open source vulnerabilities may exist can be difficult. In order to address the identification and mitigation challenge requires an intentional effort that includes activities such as code inspection, dynamic security scanning and vulnerability testing. These are the same techniques that should be applied to all software code repositories, whether open source or not. There are also enterprise specific products that offer a complete end-to-end solution for third party components and supply chain management with features such as licensing, security, inventory, and policy enforcement. These products are offered by vendors such as Black Duck Software, Sonatype Nexus, and Protecode, to name a few.

Most organizations search the CVE and NIST Vulnerability Database for vulnerability information, but these sources provide little information on open source vulnerabilities. Information on open source vulnerabilities is distributed among so many different sources that it is hard to track it. To address the risk of open source vulnerabilities in the software supply chain, groups such as PCI and Open Web Application Security Project (OWASP) have specific controls and policy in place to govern the use of open source components. Other security repositories exist including the Node Security Project for JavaScript/Node.js specific vulnerabilities and Rubysec for Ruby specific vulnerabilities. However, there are still many open source projects and ecosystems that are not well covered.

An entire market of open source and commercial tools has emerged over the years to tackle this problem as a result. These tools vary in approach and capabilities, and some are open source themselves. Most of these tools use the NIST NVD as a starting point for sourcing open source software vulnerabilities. Each tool is then enhanced with usability features and/or additional data sourcing for improved functionality. A sample of these tools was included in the CSRIC VI report.

In general, an open source security analysis should:

- **Check for public vulnerabilities**—ensure the open source components do not contain publicly-known vulnerabilities, reported with vulnerabilities described in other public resources.
- **Use commercial security intelligence**—use additional vulnerability data sources (such as from data vendors) to augment the public vulnerability data.
- **Perform static analysis**—use static analysis tools to validate that the open source components do not contain unreported security vulnerabilities.

- **Perform comprehensive security reviews**—perform a comprehensive security review of the open source component

6.1.3.3 Improvements in Open Source as a Result of 5G

As the core network leverages more instances of the traditional Information Technology platforms to enable all services, the use of open source software by mobile network operators will inevitably increase. While this will not drive specific changes in best practices related to the use of open source software, the community as a whole will benefit from the expanded use that will result from the addition of companies in the 5G ecosystem. As a result, it is likely that the increased visibility into open source software will result in improvements in vulnerability detection, reporting, and patching.

The next phase of wireless connectivity represents the convergence of multiple advancements that will enable massive connectivity and innovative security as shown in Figure 33.

Figure 33 - Convergence of Multiple Advancements

6.1.4 Network Slicing Security

Security and trust aspects are a major concern when using shared network infrastructure. Since network slices are a new concept and not yet deployed widely, we have not seen attacks on network slices in the wild. However, there are some potential attacks against network slices like:

- DoS attacks on "small" slices.
- Attacks on interfaces to common network parts (vertical mobile network operator)
- Attacks on management interfaces provided for verticals to manage their slices
- Attacks via inter-slice interfaces
- Attacks on slicing-specific procedures: Slice selection, slicing-specific authentication and authorization, slice management
- Malicious message routing between different slices via a UE connected to different slices simultaneously.

Most of the above attacks can be mitigated by state-of-the-art security measures. A prerequisite for running a highly sensitive service in a network slice, is full isolation of the slice against all other users of the common network infrastructure. To achieve a full isolation, both resource isolation and security isolation need to be considered. Resource isolation means making sure

that Resources dedicated to one slice is not consumed by another slice. Security isolation means that data/traffic cannot be intercepted/faked by entities of another slice.

This brings the need for authenticating and authorizing the UE for the accessing the specific network slice. For 5G networks, 3GPP has specified an authentication and authorization framework to achieve the required level resource isolation as well as service isolation. In Rel-15 of 3GPP, network slice authentication and authorization is part of the primary authentication of the UE. When the UE is authenticated by the network, during its initial access, a set of allowed NSSAI (Network Slice Specific Access Identifiers) are returned to the UE. The serving network also gets copy of the allowed NSSAIs (where the UE is entitled to access). The UE can request to access any one of the allowed network slices (by including the corresponding NSSAI in the service request), but any request to access a network slice not belonging to the allowed list is not allowed by the network. Hence Rel-15 supports network slices as part of the UEs subscription information and authentication and authorization for slice access is built into the primary authentication. It is also possible that the network slice specific access identifier (NSSAI) is concealed and is not exposed at the radio layer, by provisioning, if is considered sensitive.
In Rel-16 of 3GPP, in addition to the primary authentication for network slice access, a slice specific authentication procedure using EAP authentication method is also supported. When the UE is authenticated for network access, the serving network and the UE gets a list of allowed network slices indicated by allowed NSSAIs. The allowed NSSAIs may further require slice specific authentication by a slice specific AAA. This additional slice specific authentication is indicated by the subscription information. If slice specific authentication and authorization is indicated, the AMF in the serving network triggers the EAP authentication procedure to authenticate the UE for slice specific access. This gives much more control for the slice access to the slice tenant without depending only on the PLMN operator.

In 5G networks, the 5G core network nodes may be implemented as Virtualized Network Functions (VNF) or Container Network Functions (CNF), also referred to as cloud-native network functions on a shared cloud infrastructure. Such sharing of cloud infrastructure brings the risk of potential breaches of resource, data and signaling, due to vulnerabilities and misconfigurations in the cloud software. It is of paramount importance to make sure that the cloud infrastructure with its different layers, provide adequate protection and isolation at the platform level, hypervisor level, at individual virtual machine (VM), or pod/container levels with proper configuration and monitoring tools. Inter VM communication channels need to be realized in a secure manner such that inter VM communication is not exposed as plain data to any other VMs in the cloud.

Isolation between different network slices running on a virtual shared infrastructure requires preventing virtual machines in one slice from impacting those in other slices. It is also required to prevent information from leaking between slices on side channels (e.g., via shared physical memory sequentially used by different slices).

It is important to note that 3GPP has also defined a Suite of Security Assurance (SCAS) tests for 3GPP defined virtualized NFs to verify and certify the integrity of these nodes.

6.1.5 Analysis of "Imp4GT: ImPersonation Attacks in 4G NeTworks"

6.1.5.1 Overall description

This attack allows **impersonation of the UE**, including hijacking of TCP connections by which the UE communicates with servers. In particular, in what the paper calls "Uplink Impersonation", the UE may be impersonated towards services provided by the MNO itself, like a customer portal where the subscriber may manage its subscription, and where authentication and security relies on the mobile network security only. (In contrast, a UE cannot be impersonated towards a server that uses its own security protocol, such as TLS, and authenticates the UE based on username/password or a client certificate.)

In "Downlink Impersonation", the attacker is able to address the UE directly, circumventing any firewall that may be in place between the mobile network and the Internet. For this communication, the attacker can spoof an arbitrary IP source address.
The attack requires the usage of a false base station (fBTS) acting as relay between the UE and the network and therefore suffers from the limitations of fBTS attacks – in particular it has only local impact, against single UEs, and only as long as they remain in the proximity of the fBTS. This is not a theoretical attack but has been implemented and tested successfully in a commercial network, with an only slightly modified commercial UE.

This attack is highly significant, as it breaks confidentiality and integrity of the LTE user plane, i.e., one of the most important security features provided by the 3GPP security architecture. The attack affects standard compliant equipment of any vendor. It cannot be prevented by proprietary changes of vendor equipment as this would kill interoperability between UEs and networks.

6.1.5.2 Details on how the attack works

The attack exploits the fact that LTE encryption is done using stream ciphers (in contrast to block ciphers) and that no integrity protection is applied in the user plane. In addition, it exploits a feature of the IP stack specified by the IETF: In case the IP stack receives an IP packet with unknown "protocol type" ("protocol" refers here to the next layer protocol transported in the IP packet, such as TCP or UDP), the stack replies with an ICMP error message that contains the received packet. This procedure is called "reflection" in the paper.

The attack builds on the "aLTEr" attack previously published by the same author(s), where DNS requests of a UE can be manipulated in a way that the UE uses a malicious DNS server instead of the legal one. However, the present attack goes far beyond "aLTEr".

In a first phase, the attacker performs an aLTEr attack with a fBTS to hijack a TCP connection that the UE initiates. For example, Android smartphones typically connect to a known server to check Internet connectivity after connecting to the mobile network. The attacker is then able to send TCP packets to the UE from the attacker's malicious TCP proxy in the Internet. The attacker sees the encrypted downlink packet at the fBTS and changes the protocol type "TCP" to an undefined value. Consequently, the protocol stack of the UE reflects the packet. As this reflected uplink packet may not be able to traverse the firewall of the mobile network towards the Internet, the fBTS changes the protocol type to an allowed value and receives the packet, decrypted by the network, at the attacker's server in the Internet. By this, the attacker learns the

complete cleartext of the downlink packet, as it is contained in the uplink packet due to the reflection mechanism. By this, the attacker learns, how the IP header of a packet from the Internet to the UE is changed by NAT and by routers decrementing the TTL field in the IP header.

So, when the attacker sends another packet to the UE in the hijacked TCP connection, and again changes via the fBTS the protocol type in the downlink packet, the fBTS can calculate the complete cleartext of the reflected uplink packet and can therefore extract the complete keystream. This allows the fBTS to craft an arbitrary packet (as long as it is not longer than the captured keystream), encrypt it and send it to the Internet. At this point, the fBTS crafts a UDP packet to a server of the attacker, and by this a UDP session is established, which allows the attacker to send a UDP packet to the UE at any time (which would otherwise not be possible due to the firewall of the mobile network towards the Internet). This concludes the preparation phase.

In uplink impersonation, when the attacker wants to send an uplink packet, the attacker sends a UDP packet from the Internet to the UE, changes the protocol type with the fBTS, captures the reflected packet at the fBTS, extracts the keystream, encrypts its own faked packet with the keystream and passes it to the network. For successful uplink impersonation, the attacker must be able to understand the respective downlink traffic, i.e., decrypt it. For this, again the attacker lets the UE reflect the downlink packet and modifies the uplink packet in a way it will be routed to the attacker's server in the Internet, decrypted by the network.

In downlink impersonation, when the attacker wants to send a downlink packet, the attacker sends a UDP packet from the Internet to the UE, and when the packet passes the fBTS, the fBTS changes the packet as needed, e.g., sets the IP source address to that of the impersonated communication peer and the protocol id to the desired value. For successful downlink impersonation, the attacker must be able to receive the respective uplink traffic. For this, the fBTS modifies the uplink packet in a way that it will be routed to the attacker's server in the Internet, decrypted by the network.

6.1.5.3 Limitations

- Limited to local attacks against UEs in the range of a fBTS.
- Meaningful impersonation only for sessions that do not use security mechanisms such as TLS, which is very common e.g., for smartphone applications. (The attack gives the attacker the same possibilities as someone controlling a router in the path between the UE and its communication peer, and most Internet communication today uses protection against such potential attacks.)
- No decryption of arbitrary traffic: For uplink/downlink traffic of the UE, the attacker needs to know the destination/source IP address, respectively, in order to be able to redirect the packet to the attacker's server and get the decrypted packet.
- Not applicable for certain UE operating systems that do not implement the reflection in all cases (in deviation of IETF specs).

- The packet rate for impersonation attacks is limited by the rate at which the IP stacks generates (reflected) ICMP packets. This rate may be set per default to a relatively low value, as high rate ICMP traffic is not required in normal operation and could be a sign of some abuse (as it is the case in this attack).
- Reflected packets are limited in size, so the original downlink packet may get truncated. Thus, downlink packets cannot be decrypted in arbitrary size, and keystreams cannot be generated in arbitrary size.
- The attack works, if no user plane integrity protection is used on the radio interface; this is always the case in LTE and in 5G non-stand-alone operation. In 5G stand-alone, user plane integrity protection is mandatory to support up to a bandwidth of only 64 kbit/s. If it is used, the attack does not work. However, it may not be used in many cases, as the support is not guaranteed for higher bandwidths.

6.1.5.4 Countermeasures

- Use of security mechanisms on the IP layer or above, such as TLS (does not affect the mobile network, is up to the applications); in particular, for access of a UE to an application of the MNO (e.g., a portal for subscribers to book services or manage their subscriptions otherwise), the MNO-application must not authenticate a UE simply by its IP source address, but must use proper authentication and integrity protection e.g., by TLS. This requires either the use of GBA, or the UEs must have additional credentials (such as username and password) to authenticate to the application server.
- More restrictions on the use of ICMP (may be enforced by the firewall of the mobile network)
- Use of user plane integrity protection (not specified for LTE, only in 5G stand-alone)
- Specifying other forms of user plane encryption on the radio interface: Block ciphers instead of stream ciphers. This would be a rather significant change and is therefore rather unlikely.

6.1.6 5GC Support of Different Access Technologies

Fiber transmission is highly secure, since fiber's signal can only be intercepted through a physical device that taps into the cable. As discussed in Clause 5.6, fiber will enable the secure transmission and backhaul of enormous quantities of transmissions as consumers, business including IoT, and manufacturing become more fully connected.

In the end, the power of fiber enhances the reach and security of 5G, and this partnership allows 5G in turn to become more exciting, more widespread, and more powerful.

6.1.7 Security Concerns of Using Legacy Protocols

The UDM may be prone to known HLR/HSS specific attacks that exist on legacy 3G/4G inter-carrier SS7 or Diameter roaming links.

The SMSF may be prone to known MSC/VLR specific SS7 or Diameter attacks that exist on the inter-carrier SS7 or Diameter roaming links.

The CHF may be prone to attacks that exploit vulnerabilities that exist in base Diameter protocol implementation without transport layer protection.

The SMF and UPF may be prone to attacks that may exploit GTP and PFCP protocols that are generally deployed without any message authentication, integrity and confidentiality protection.

6.1.8 Workforce Considerations

CSRIC V was tasked to examine and develop recommendations to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. The final report demonstrated the applicability of the National Cybersecurity Workforce Framework to the Communication Sector specific cybersecurity skills requirements. The applications, templates, and other tools documented by CSRIC V will benefit the Communications Sector as operators incorporate 5G-based technologies.

As the information and communications technology ("ICT") ecosystem evolves, the communications sector should be cognizant of cultural differences that may act as an inherent threat to the operator's ability to maintain carrier grade services. Operators must consider the potential intended and unintended threats to cybersecurity, reliability and interoperability that derive within the workforce.

Carrier-grade network reliability is the result of disciplined operations, administration, maintenance, provisioning and troubleshooting (OAM&P) rooted in standards maintained by the TM Forum. This Business Process Framework (eTOM) is designed to deliver 99.9999% (six-nines) reliability. Analogous IT service management practices are outlined in ITIL (formerly an acronym for Information Technology Infrastructure Library). This set of detailed practices for IT service management focuses on aligning IT services with the needs of the business-often 99.9% (three-nine's) reliability.

To ensure the highest level of security and reliability, operators will need to be prepared to help employees bridge the gap between operational processes used to deliver consumer and enterprise-grade reliability to those processes used to achieve carrier-grade reliability. CSRIC's collection of Best Practices provides a solid foundation to support 5G SA. Security is everyone's responsibility.

6.1.9 5G Private Networks

In Section 5.4, 5G Private Network was described. Several constraints limited detailed investigation into private network security by CSRIC VII:

- Only the security of the public 5G network was considered – the security impacts of providing public network assistance to a private network. The security of the private network itself was not considered at this time.
- During the preparation this report, 5G Private Networking was just entering Proof-of-

Concept and demonstration stages[30]. Very little detail about the 5G services the commercial network provided to the demonstration 5G private network was available. Without a clear view of actual public/private network service and facilities separation, a security evaluation could not be undertaken.

6.2 Recommendations

6.2.1 Recommendations to the FCC

6.2.1.1 Previous CSRIC Recommendations

CSRIC VII commends the FCC's efforts to support CSRIC recommendations as shown by previous Public Notices (PNs).[31] [32] CSRUC VII recommends that the FCC encourage industry for continued implementation of CSRIC's prior recommendations[33] [34] [35] and continue to promote awareness.

6.2.1.2 Supply Chain Recommendations

CSRIC VI published an addendum to their final report[36] regarding supply chain recommendations. CSRIC VI reiterates the recommendation that the FCC continue to actively participate in the ICT SCRM Task Force, engage with NIST on the review of SP 800-161 rev 1 and continue as an active member of the ATIS 5G Supply Chain Working Group. These SCRM programs represent strong public and private partnerships that are working to develop the framework for trusted 5G networks.

6.2.1.3 Network Slicing

CSRIC VII recommends that the FCC consider further investigation the security implication of Network Slicing for a future CSRIC task.

6.2.1.4 5G Private Networks

5G Private Networks was briefly discussed in section 5.4, but with limited conclusion due to the pending activities in 3GPP. CSRIC VII recommends that the FCC consider further investigation

---

[30] A sampling of announcements and press releases on private network POCs:
https://www.nokia.com/about-us/news/releases/2020/04/07/nokia-deploys-worlds-first-450-mhz-private-wireless-lte-network-poc-for-power-grid-operators-in-poland/
https://www.webwire.com/ViewPressRel.asp?aId=250700
https://www.globenewswire.com/news-release/2020/02/27/1991601/0/en/Nokia-deploys-5G-private-wireless-network-for-Lufthansa-Technik-virtual-inspection-trial.html
https://citymesh.com/en/news/brussels-airport-innovates-with-private-5g-network

[31] See: https://www.fcc.gov/document/fcc-seeks-comment-implementation-diameter-best-practices
[32] See: https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0824/DA-17-799A1.pdf
[33] CSRIC VI Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0
[34] See: Legacy Systems Risk Reductions, Final Report https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
[35] See: Recommendations to Mitigate Security Risks for Diameter Networks Version 1.1, https://www.fcc.gov/file/13925/download
[36] ADDENDUM to Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks, September 2018.

of 5G Private Network security for a future CSRIC task.

6.2.1.5 5GC Support of Different Access Technologies

CSRIC VII recommends that FCC consider further investigation of other access technologies that enable 5G deployment and delivery for a future CSRIC task. Additional work should be accomplished toward wireline, satellite, as well as other wireless access technologies concerning security and capacity as well as specific potential vulnerabilities.

6.2.2 Recommendations to Industry

6.2.2.1 Previous CSRIC Recommendations

CSRIC VII recommends that industry rely upon CSRIC Recommendations to mitigate threats to the 5G SA system, specifically CSRIC VI, V, and IV Reports.

6.2.2.2 Protection of legacy protocols

The protection of legacy protocols (Diameter, GTP) and associated interfaces shall be supported according to NDS/IP as specified in [Ref 6]. In case of intermediaries (e.g., hop-by-hop), it does not ensure end-to-end message authenticity and confidentiality protection. Additionally, protection of Diameter interfaces shall use recommendations described in [Ref 7].

6.2.2.2.1 UDM Implementations

The UDM may be prone to attacks similar to what was seen in earlier generations on the HLR/HSS. Attacks via SS7/Diameter in 3G/4G networks could be repeated in a 5G network using the IWF, or through new attacks against the HTTP protocol (refer to sections 5.1.4.6 and 6.1.2).

CSRIC VII recommends that remediation against known SS7/Diameter attacks be implemented at the IWF, and that safeguards for the UDM be implemented (refer to sections 5.1.4.6 and 6.1.2).

6.2.2.2.2 SMSF Implementations

The SMSF may be prone to attacks similar to what was seen in earlier generations on the MSC/VLR. Attacks via SS7/Diameter in 3G/4G networks could be repeated in a 5G network using the IWF, or through new attacks against the HTTP protocol.

CSRIC VII recommends that remediation against known SS7/Diameter attacks be implemented at the IWF, and that safeguards for the SMSF be implemented.

6.2.2.3 Workforce

CSRIC VII recommends that industry leverage CSRIC's collection of Best Practices[37] [38] [39] to ensure the workforce is prepared to operate and maintain carrier grade reliability and security in a 5G SA environment. This includes workforce training on network elements introduced in the 5G SA architecture such as virtualization and network slicing.

6.2.2.4 Risks of Open Source in 5G

One of the common misconceptions about an open source architectures is that open interfaces introduce security risk. In fact, these same open interfaces, defined in technical specifications, provide a foundation and architecture for improving security. Although operators procure and integrate open source into network elements functions in new ways, operators bring the same expertise, diligence and requirements for security and resilience to these environments. 5G and open source also enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers and network operators to assess and to manage security risks.

An open architecture opens the ecosystem to new suppliers, increasing the diversity of virtualized solutions, inherently increasing the security of a network vs. a proprietary, single vendor network. Standards play an important role in 5G security and an open source. The opportunity to build open, interoperable and standards-based 5G networks has already begun to spur innovation and competition among diverse companies worldwide, enabling greater security for 5G. In addition to the advantages and disadvantages highlighted the risks around the use of open source can be managed. Consistent with the National Security Telecommunications Advisory Committee (NSTAC) report, open source and SDN etc. are different operating architectures that introduce some challenges and some benefits but can be managed with due diligence and leveraging a variety of security practices that are well defined in the industry.

CSRIC VII recommends the industry continue to advance open architectures for 5G and continue to address security as a fundamental consideration of all open source architectures.

6.2.2.5 Network Slicing Security

CSRIC VII recommends that the industry should consider the following factors to ensure security in Network Slicing.

---

[37] 12-12-0588: Network Operators, Service Providers, Equipment Suppliers and Public Safety should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture.
http://bp.atis.org/best-practice-detail?bp_id=1964

[38] 12-12-8129: Network Operators, Service Providers and Public Safety should ensure that technical staff participate in ongoing training and remain up-to-date on their certifications for those technologies to remain current with the various security controls employed by different technologies.
http://bp.atis.org/best-practice-detail?bp_id=2122

[39] 12-10-0589: Network Operators, Service Providers, Equipment Suppliers, and Public Safety should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network.
http://bp.atis.org/best-practice-detail?bp_id=2299

Slicing Isolation:

- Isolation is the crucial security aspect in network slicing. It is important to make sure that resources dedicated to one slice cannot be consumed by another slice. Also, data/traffic cannot be intercepted/faked by entities of another slice.
- Slice isolation needs to be achieved assuming sound implementations in the cloud, SDN transport and non-virtualized equipment.
    - The cloud infrastructure that host the slices needs to provide adequate protection and isolation at the platform level, hypervisor level and at individual virtual machine (VM) or Containers levels with proper configuration and monitoring tools.
    - The SDN transport infrastructure needs to achieve isolation by using VPNs.
    - The non-virtualized equipment (e.g., RAN) should achieve isolation by equipment-specific mechanisms.

Automated Slicing Security Management and Orchestration tools:

- Automated Security Management and Orchestration is needed to cope with the dynamic nature of slicing. Some security tools may only run within one slice, not aware of other slices, but there must be others that have the complete network view.

Slice-specific assurance level:

- Network functions may have diverse security assurance levels. All network functions used in a slice (as well as the platform on which they are deployed) must meet the assurance level required for the services deployed in the slice.
- This may also allow fast, lightweight deployment of experimental services in slices without a high security assurance level.

Protection of slicing-specific procedures (such as slice selection, slice-specific authentication and authorization, or slice management access by third party tenants):

- Current and future state-of-the-art protection measures for such interfaces and procedures must be applied.
- Use standardized security measures to standardized slicing-specific procedures (e.g., 3GPP security specification TS 33.501 [Ref 3])

Per slice network security measures: A slice is a virtual network, so general network security measures must be applied per slice:

- “Legacy” measures applied to a virtualized network: virtual firewall, zoning and traffic separation by virtual networking, intrusion detection, authentication, cryptographically protected protocols, access control etc.
- Integrity protection for platform and virtualized functions using remote attestation based on strong trust anchors
- “Modern state-of-the-art”: Pervasive Monitoring, AI/ML based analytics, automated response loop, automated threat intelligence sharing etc.

7 Conclusions

CSRIC VII analyzed key features of 5G security to identify any potential areas of risk. Based on this analysis, CSRIC VII offers several recommendations on how to mitigate potential 5G security threats, as well as proposed future work in the area. Additional work on optional 5G features related to security and privacy will be the focus of CSRIC VII's second report on this issue.