5G Network Slicing:
Security Considerations for Design, Deployment, and Maintenance

Disclaimer

This document was written for general informational purposes only. It is intended to apply to a variety of factual circumstances and industry stakeholders. The guidance in this document is provided "as is" based on knowledge and recommended practices in existence at the time of publication. Readers should confer with their respective network administrators and information security personnel to obtain advice applicable to their individual circumstances. In no event shall the United States Government be liable for any damages arising in any way out of the use of or reliance on this guidance.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes. All trademarks are the property of their respective owners.

Purpose

The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / Inquiries: Enduring Security Framework nsaesf@cyber.nsa.gov

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov

Table of Contents

Intended Audience 5
Scope 6
Introduction 7
PRINCIPLES AND CONCEPTS 9
What is Network Slicing? 9
Mobile Network Infrastructure 9
User Equipment 9
Transport Networks 10
Radio Access Networks 11
5G Core Network 11
Interconnect and Roaming 12
Components of a 5G Network Slice 13
Roles 13
5G System Components 13
Network Slice Composition 14
Network Slice Service Level Characteristics 16
Network Slice Profile 17
Network Slice Service Profile 18
Security Management of a Network Slice 19
Network Slice Orchestration Frameworks 20
5G Threat Vectors 20
Goals for End-to-End Network Slicing 21
DESIGN CRITERIA 23
Network Slice 23
Open RAN 25
Core Networking 27
User Equipment 28
Cloud and Virtualization 30
Interconnect & Roaming 32
Data Networking 33
Management and Orchestration 35

Network Slice Creation and Deployment 36
OPERATIONS AND MAINTENANCE CRITERIA 39
Introduction 39
Definition of Operations and Maintenance 39
Importance of Operations and Maintenance 39
Orchestration of Network Slices 40
Policy Considerations 40
Workflow Considerations 40
Maintenance of Network Slices 40
Monitoring 40
Alerting 42
Reporting 42
Conclusion 43
APPENDIX: Abbreviated Terms 44

FIGURES

Figure 1: RAN in a 5G System....11
Figure 2: 5G Core Architecture Containing the NFs....12
Figure 3: The Life Cycle of Service / Slice Instance Orchestration....14
Figure 4: Network Slice Composition....15
Figure 5: Network Slice Model....19
Figure 6: End-to-End 5G Network Slicing Architecture....21
Figure 7: Independent Logical Networks....24
Figure 8: O-RAN Service Management and Orchestration....26
Figure 9: Reference Architecture for 5G Network Interworking....34

TABLES

Table 1: Traffic to network slice matching schemes....10
Table 2: Network Slicing Domains....15
Table 3: An Example Service Level Characteristic Value....16
Table 4: 3GPP Specified Values for 5QI = 2....17
Table 5: Traffic to Network Slice Matching Schemes....29
Table 6: The following is an example URSP rule for enterprise traffic....30
Table 7: Examples of Network Monitoring Activities for 5G Networks....41

Executive Summary

The Enduring Security Framework[1] established a working panel comprised of government and industry experts and conducted an in-depth review of the fifth-generation technology for broadband cellular networks standalone network slicing network architecture. This panel assessed the security, risks, benefits, design, deployment, operations, and maintenance of a 5G standalone network slice over two papers- Parts 1 and 2.

The working panel published in *Potential Threats to 5G Network Slicing*[2] which identifies some 5G network slicing *threat vectors* that pose significant risks to network slicing and serves as Part 1. This document is Part 2 of the two-part series - it focuses on addressing some identified threats to 5G SA network slicing, and *provides industry recognized practices* for the design, deployment, operation, and maintenance of a hardened 5G standalone network slice(s).

For the purposes of this paper, a network slice is defined as *an end-to-end logical network that provides specific network capabilities and characteristics for a user*. More specifically, it is a network architecture that allows infrastructure providers to divide their network up into several virtual networks to satisfy different 5G use cases with varying quality of service requirements and was not intended to be a security mechanism to isolate different 5G user sets.

Since a mobile network operator can create specific virtual networks that cater to different clients and use cases, security is a major consideration. In a 5G infrastructure this necessitates that the confidentiality, integrity, and availability triad of each network slice must be ensured.

This document will help foster communication amongst mobile network operators, hardware manufacturers, software developers, non-mobile network operators, systems integrators, and network slice customers in the hopes that it may facilitate increased resiliency and security hardening within network slicing.

Intended Audience

It is not the goal of this document to provide an exhaustive how-to list for the design and operation of a network slice; rather, to introduce best practices that can help mitigate threats against a 5G network slice. The threat landscape in 5G is dynamic; due to this, advanced monitoring, auditing, and other analytical capabilities are required to meet certain levels of network slicing service level requirements over time.

It is assumed the audience has some familiarity with 5G networks and the overall concept of network slicing. Readers of this document are expected to augment the information contained here with individual studies on current best practices for designing, deploying, operating, and maintaining a network slice.

---

[1] The Enduring Security Framework (ESF) is a cross-sector working group that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. national security systems. It is comprised of experts from the U.S. government as well as representatives from the Information Technology, Communications, and the Defense Industrial Base sectors. The ESF is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges.

[2] https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL%20THREATS%20TO%205G%20NETWORK%20SLICING_508C_FINAL.PDF

Scope

This document contains forward-looking statements that may change or evolve as time passes, as the standardization of the 5G network slicing evolves. Existing 5G implementations do not fully realize the breadth of available standards. Current and future 5G standards do not and are unlikely to prescribe exactly how 5G standalone network slicing must or should be implemented. This will allow for network slicing to have varying implementations between infrastructure providers/vendors. Further discussion is needed between infrastructure providers and current/potential customers.

While most of the 3GPP technical specifications supporting basic Network Slicing have been sorted out, the industry is still at the "Minimum Viable Product" stage, with Mobile Network Operators looking to commercialize slicing in their own mobile networks. GSMA is facilitating collaboration on defining minimum standard slice templates, which will facilitate roaming.

As with most emerging technologies, with increased benefits come increased risks. This paper is intended to introduce 5G stakeholders to the benefits associated with network slicing, provide guidance in line with industry best practices, and present perceived risks and management strategies which may address those risks.

As of the time of this writing, the commercial availability of standards-based 5G network slicing within an operator's mobile network only appears to be a reality within one year, possibly longer. Given that 5G roaming is still in the future, the expectation is that 5G network slicing across multiple operators' networks is as well. Work also appears to be progressing for slicing within a data network—that is, a network external to the mobile network—however that still falls into the "future" category. The same can be said for any network slicing seamlessly coordinated across mobile networks and data networks.

Nonetheless, network slicing is not principally a security mechanism and cannot be relied on for that purpose. 5G threats, which are beyond the scope of this paper, continue to apply to network slicing. Network slicing introduces additional security concerns, where the details for many of these are beyond the scope of this paper and should be discussed with infrastructure providers/vendors, such as:

- Inter-slice communications.
- Authentication/Authorization among network slice managers, instances, and elements.
- Different security protocols and policies between slices.
- Denial of service, especially in one slice that affects other slices.
- Exhaustion of security resources, especially in one slice that affects other slices.
- Side channel attacks across slices.
- User equipment connection to multiple slices.
- Shared network functions, compute (hypervisor or container engine), data, and other resources (storage, networking) across slices.
- Slice separation via physical machines, virtual machines, or Linux containers.
- Shared management and orchestration systems across slices.
- Shared human administrators across slices.
- The network slice itself and the network slice identifier transmitted by the user equipment may represent anonymity concerns for the user and a focal point for an attacker.

Introduction

In a world where communications requirements seem to change as soon as specifications are fielded, the expected high technology adoption of smart households, smart grids, and smart meters will require a large number and high density of Internet of Things devices cellular wireless network connectivity to be efficient and cost-effective. The best way to field such a 5G telecommunication systems is to divide a network into slices- principally, a way to provide similar communication services with similar network characteristics to different vertical industries.[3]

A standard 5G standalone network consists of user equipment connected by an over-the-air link to a radio access network, which then interfaces with the core network. In a 5G standalone infrastructure, network slicing is a network architecture that enables multiplexing of independent logical networks. The multiple logical networks may share the same physical resources (computers, networking, network resources, management, and administrators). This sharing has the potential to enable more efficient resource utilizations and enables cost savings with the potential expense of lesser assurances of confidentiality, integrity, and availability triad.

A *network slice* provides a virtual network service that connects an application running on user equipment, such as a cell phone or Internet of Things sensor, with applications that may be running on other user equipment or servers that are connected to a data network.

This document assesses the current state of 5G network slicing technology, including common industry definitions, as well as physical and logical architectural references, and provides information necessary to understand and mitigate some potential threats to 5G network slicing.

Network slicing can help augment security of 5G systems and communications carried over 5G networks. Logical isolation of network traffic (both control and user-planes), 5G network functions and other compute workloads, and storage of subscriber profiles and other data could help protect information in one slice if another slice were to be compromised.

Additional authentication and authorization, as well as specialized policies and configurations, can be applied on a per-slice basis. Security elements, monitoring, and analytics could also be customized per slice. Many of these concepts would help apply a Zero Trust Architecture paradigm to the network slice itself, noting that the capabilities and options for a network slice may vary by operator and does not address zero trust beyond the slice, e.g., in the operator's network, external data networks, and the application itself.

The logical isolation afforded by network slicing for network functions and more generally compute tasks deserves additional discussion. Logical isolation, in this context, could mean compute tasks separated in virtual machines or in containers, and those workloads may or may not be run on the same physical machine or interconnected set of physical machines.

In the case of the same physical machine, then the workloads may share the same hypervisor and container execution engine; in the case of separate physical machines but interconnected group of machines, then the systems themselves share network connectivity and the workloads may share the same orchestration system.

Taking logical isolation one step further, a specific network slice could be configured such that its

[3] 3GPP TS 23.501

network functions and other related workloads are executed only on a dedicated set of physical machines, which host no other compute tasks; noting, however, the isolated group of physical machines may share network connectivity, orchestration systems, and human administrators with other slices.

From a security perspective, network slicing is a logical part of a larger system, where security is inherently intertwined. Network slicing provides benefits and trade-offs, from both functional and security perspectives, that must be considered.

Existing alternatives to network slicing, depending on use case, include:

- Using a custom fourth-generation technology for broadband cellular networks 4G Access Point Name or 5G Data Network Name to logically separate some network traffic. This does not provide all the functionality of an end-to-end network slice.
- Implementing a Mobile Virtual Network Operator model which requires significant investment in cost and time.
- Deployment of a private 5G network infrastructure, which could be a private 5G non-standalone or private 5G standalone, that could implement 5G network slices, or a combination of both private 5G non-standalone and private 5G standalone.

PRINCIPLES AND CONCEPTS

What is Network Slicing?

5G network slicing is a network architecture that provides a way to divides a network to provide independent logical networks over physical network resources and functionality. This can help operators provide differentiated services and more quickly deploy new cases. An operator can use network slicing to logically allocate physical resources across one or more slices, where each slice may have a different Quality of Service (QoS) and other performance characteristics, as well as configurations and policies, to meet a variety of use cases and possible Service Level Agreements (SLAs). For example, a slice supporting mobile broadband users requires high data rates and traffic volumes, a slice supporting Internet of Things devices may optimize high-density devices and power consumption, and a slice supporting autonomous driving may provide high-reliability and low-latency communications.

Mobile Network Infrastructure

The 5G ecosystem uses radio resources for some part of the communication between an originating and a destination application. While there are standards defining specifications for how operators build their 5G networks, but currently network slice specifications requirements are insufficient and need to evolve for the development, implementation, and maintenance of security for network slicing.

Currently network slice specifications do not get into the implementation detail level and allow for wide ranging varying of the network slice implementations. The placement of functional components onto a physical computing platform is a choice that may affect the level of service provided by the network slice. Multiple functions may run on the same computing platform or may be distributed across multiple computing platforms.

User Equipment

User Equipment (UE) consists of the Mobile Equipment (ME) and the Universal Integrated Circuit Card (UICC), where the Universal Subscriber Identity Module (USIM) application resides.

The UICC, also referred to as Subscriber Identity Module (SIM) cards, are used to store UE-specific credentials required for access to an operator network. The credentials are used as part of the 5G Authentication and Key Agreement (5G-AKA) or Extensible Authentication Protocol Authentication and Key Agreement Prime (EAP-AKA') authentication procedures before establishing connectivity with the operator's 5G network. The UICC also has the capability to run network security applications in a secure and trusted environment.

In the design of device system architecture, network slicing features require the coordination between the upper operating system and the lower communication modem. Table 1 shows two ways to implement network slicing features in the device system architecture:

Table 1: Traffic to network slice matching schemes

Scheme	Description
Modem-centric	The modem matches traffic by its attributes to a network slice.
OS-centric	The operating system matches traffic by its attributes to a network slice.

Implementation of these two schemes may include changes to the operating system and application programming interfaces (API), respectively. The overall impact of this is determining that the network slice termination point will be on the 5G device in one of three locations:

- Modem,
- Operating System, and
- Application.

The UE Route Selection Policy (URSP) is a set of rules for routing application packets to the appropriate network slice. Input to the policy includes:

- Network Slice Selection Assistance Information (NSSAI),
- Protocol Data Unit (PDU) session,
- Session and Service Continuity (SSC) mode, and
- Type of access (e.g., 3GPP or non-3GPP such as Wi-Fi[4])).

The URSP rule is composed of Traffic Descriptor (TD) and Route Selection Descriptors (RSD). The application specifies the TD and the modem uses the TD to look for a URSP rule matched to the TD. Based on policies, the URSP rules can be updated based on network conditions (e.g., overload conditions).

Transport Networks

Introduction

Transport networks are the connective links between the network connected elements that implement a network slice between two elements.

Transport Networks Inside of the Mobile Operator Network

Transport networks are categorized by the types of elements that they connect. The fronthaul network connects the radio unit to a distributed unit in the radio access network (RAN). The mid-haul network connects a distributed unit to the other elements in the RAN, including the central unit. The backhaul network transports the user plane and the control plane to the 5G core. The 5G core network connects all NFs and repositories in the 5G core. The user plane function (UPF) connects applications and services that are outside of the 5G system via a data network.

Transport Networks Outside of the Mobile Operator Network

To meet organizational needs, many 5G networks need to connect to data, applications, and devices outside the 5G network boundary. These connected data networks may have wide-ranging

[4] Wi-Fi™ is a trademark of the Wi-Fi Alliance.

topologies and support a wide range of protocols at the Internet, transport, and application layers. It is critical to mission success that network planners, implementors, and operators carefully plan for these connections to ensure continued confidentiality, integrity, and availability of mission-critical data across a full end-to-end (E2E) connection. The N6 Reference Point demarks the boundary between the 5G network and external data networks.

While most of this paper focuses on network slicing exclusively within the context of an operator controlled 5G network, it is important to note that many data network protocols also support network slicing natively – or will soon develop the ability to do so[5]. Even when an external network does not support slicing natively, when properly configured and coordinated it can often extend specified Quality of Service (QoS), and latency service levels that a 5G network slice provides. A network slice that originates on a 5G network can be delivered across non-5G data networks to provide E2E service; critically, this will extend the physical and logical reach of 5G networks to connect users with needed applications and data outside the 5G boundary. With well-orchestrated internetworking, certain critical features might be supported E2E for customers.

5G interworking is rapidly evolving. Standards Development Organizations (SDOs) are rapidly developing non-5G slicing standards and protocols (e.g., the Internet Engineering Task Force (IETF)[6])[7], while those SDOs work along with 3GPP to update 5G data network interworking standards that connect to these and other services while enabling E2E automation of service fulfillment and service assurance.

Radio Access Networks

The RAN logically connects radio unit (RU) interfaces through distributed units (DU) and at least one central unit (CU) and to the interface of multiple network functions in the core network.

RANs have evolved as technology has evolved. Today RANs can support multiple-input, multiple-output (MIMO) antennas, wide spectrum bandwidths, multi-band carrier aggregation, and more.

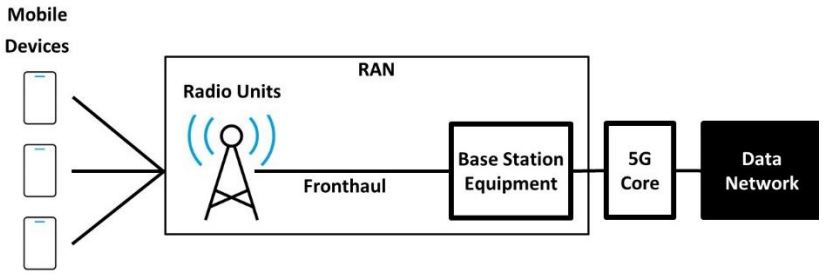

Figure 1: RAN in a 5G System

5G Core Network

The 5G *core network* consists of several well-defined services called network functions. An network function refers to either an abstract service definition or an instance of that service. An instance of an network function may be shared by multiple network slices or may be allocated

[5] See "MEF 84: Subscriber Network Slice Service and Attributes" document.
[6] https://www.ietf.org/
[7] https://datatracker.ietf.org/doc/draft-ietf-teas-ietf-network-slice-framework/

exclusively to one slice.

A network function instance that provides a service is referred to as the *producer network function*, and an network function instance that uses a service is referred to as the *consumer network function*. The implementation of a network function may be physical, virtual, or cloud native. Network functions utilize a cloud native design to enable flexible scaling and upgrades.

The number of network function services can be scaled up or down as needed. As a result, 5G network functions can be quickly created, deployed, and scaled, using automated life cycle management. An example 5G core network is depicted in Figure 2.

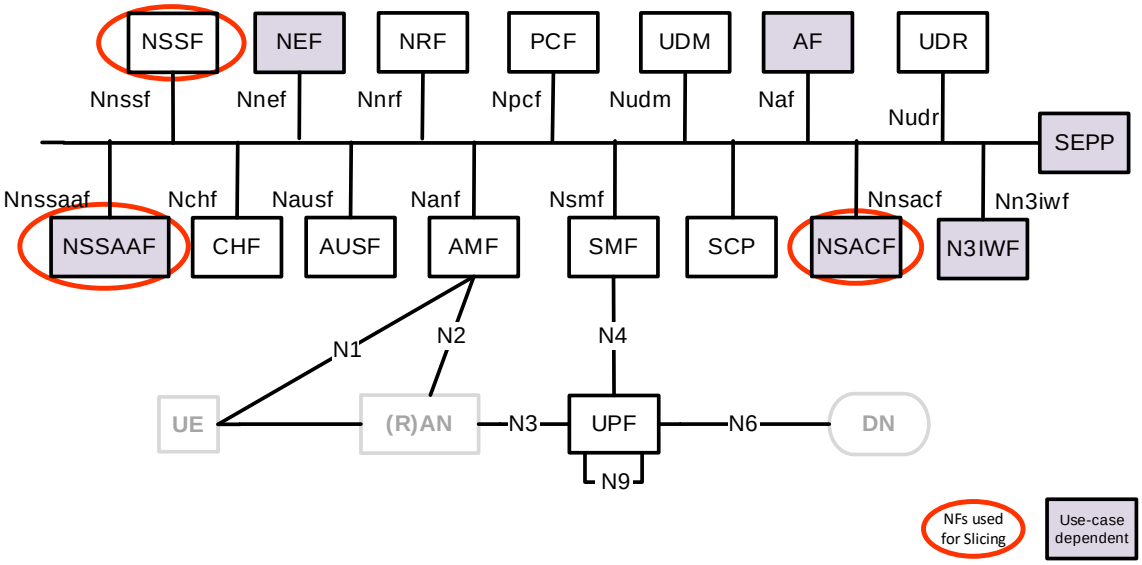

Figure 2: 5G Core Architecture Containing the NFs

The control and user plane functional separation (CUPS) architecture enhancement was introduced in evolved packet core (EPC) and the same continues in the 5G core. This separation allows the control plane functions to interact with multiple user plane functions and in turn provides for more scalable deployment choices. The NFs that have been introduced by 3GPP for supporting network slicing within the control plane are the Network Slice Selection Function (NSSF), Network Slice-specific Authentication and Authorization Function (NSSAAF), and the Network Slice Admission Control Function (NSACF).

Interconnect and Roaming

Roaming for 5G network slicing requires several new capabilities, network slicing standards, and business agreements to be developed. If agreements exist between service providers, then roaming occurs when there is an interconnection between the user's home network and another mobile network.

Roaming between mobile network operators (MNOs) typically take place in two difference ways- via direct connections between each MNO, or via an IP Service Interconnection (IPX). An IPX facilitates interconnection between MNOs according to agreed inter-operable service definitions and commercial agreements.

The GSM Association (GSMA)[8] provides technical guidance to MNOs for connecting their IP-based networks and services together to achieve roaming and/or inter-working services between them.

Roaming services enable mobile subscribers to use services in countries or areas outside of their home networks. Roaming is only usable in areas or countries where MNOs have signed a roaming agreement. Connections can be established, and roaming agreements can be signed between MNOs to ensure service continuity while roaming. Roaming agreements allow MNOs to set policies to control network access for roaming subscribers and manage roaming services.

Components of a 5G Network Slice

Roles

5G network slices may be designed and managed by various entities. The recognized worldwide leaders of 5G standards creation - the 3rd Generation Partnership Project (3GPP)[9] and the GSMA- define multiple roles related to network slicing, specifying them in publications 3GPP TS 28.530 and NG.116, respectively. The roles of relevance used in this paper, in no particular order, are:

- Network Operator (NOP),
- Network Slice Customer (NSC),
- Network Slice Provider (NSP), and
- Network Slice User (NSU).[10]

Depending upon the scenario(s):

- Each role can be filled by one or more organizations simultaneously.
- An organization can fill one or more roles simultaneously (e.g., a company can fill the NOP and NSP roles simultaneously).[11]

5G System Components

Network slicing is a crucial piece of technology that allows for the needs of each industry/or organization to be fulfilled by having multiple logical networks to be tailored and created on top of shared physical infrastructure: Radio Access Network (RAN), Core Network, Transport Network (TN), and a service orchestrator.

The life-cycle management of a slice includes slice design, the virtualized network function (VNF) on-boarding, network preparation to support the slice, slice creation and instantiation, operationalizing, and day-to-day management of the slices including scaling in/out based on service assurance. Service assurance is provided by constant supervision/monitoring, reporting, and modifying the network in an automated manner. Modifications may involve configuration changes, instantiation of networks and/or network function resources.

[8] https://www.gsma.com/
[9] https://www.3gpp.org/
[10] Although this distinction is not acknowledged by 3GPP or GSMA, ESF ascertains there is a difference between a network slice customer and a network slice user.
[11] 3GPP TS 28.530

The implementation of a network slice consists of multiple interconnected elements across some or all the access, core, and data network domains:

> As previously mentioned, the *RAN* logically connects the RU interfaces through DUs and at least one CU and to the interface of a network function in the core network.
>
> As previously mentioned, the *core network* consists of several well-defined network functions. A *network function* can an abstract service definition or an instance of that service. An instance of a network function may be shared by multiple NSs or may be allocated exclusively to one slice.
>
> The *data network* (DN) is a non-5G TN that connects elements in the core network to applications or services outside of the 5G network.

Service orchestration frameworks (Management and Network Orchestration (MANO), Open Network Automation Platform (ONAP), etc) are popular means to provide life-cycle management of a network slice and services.

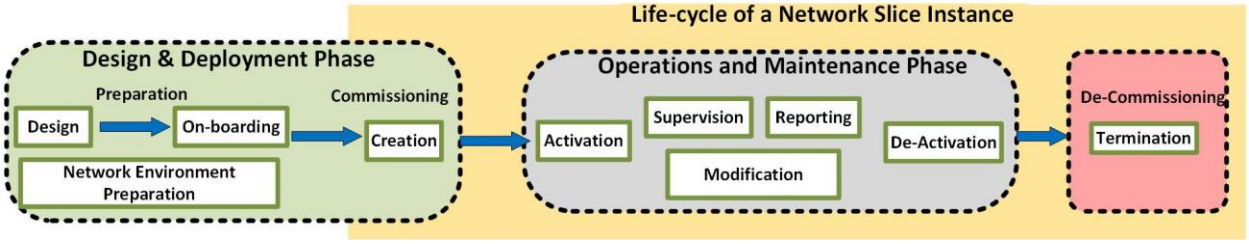

Figure 3: The Life Cycle of Service / Slice Instance Orchestration[12]

The ETSI MANO framework has been used as an example framework; however, the security features, controls and mitigations mechanisms described in this paper are generic enough and therefore would be applicable to any service orchestration framework.

Network Slice Composition

A network slice is composed of portions of the 5G network resources that collectively implement a logical network. The components are selected and configured so that the network slice provides a specified level of service.

From an application point of view, a network slice provides a connection to another application or service. The network slice is implemented by active components in one or more access, core, and data networks.

Each of those components is a service or function, hosted on a computing platform. Each computing platform may be physical or virtual. Each component consumes resources and may also consume other services. The placement of components onto computing platforms is a policy choice made to assure a negotiated level of service. Thus, the implementation of a network slice may include many computing platforms.

A network slice may use entirely physical resources, or it may consist of a mix of physical and virtual resources. In 5G, network slicing allows operators to create logical data pipelines and

[12] Derived from 3GPP.

control/management functions for each type of service, thereby assuring the requirements of each service.

Figure 4 illustrates a sample composition of network slices. Each network slice is a logical resource that is provisioned to deliver a level of service. The level of service delivered by a composition of network slices is typically different from the level of service delivered by each component network slice. That level can be higher, lower, or the same as the levels of service of each of the component network slices.

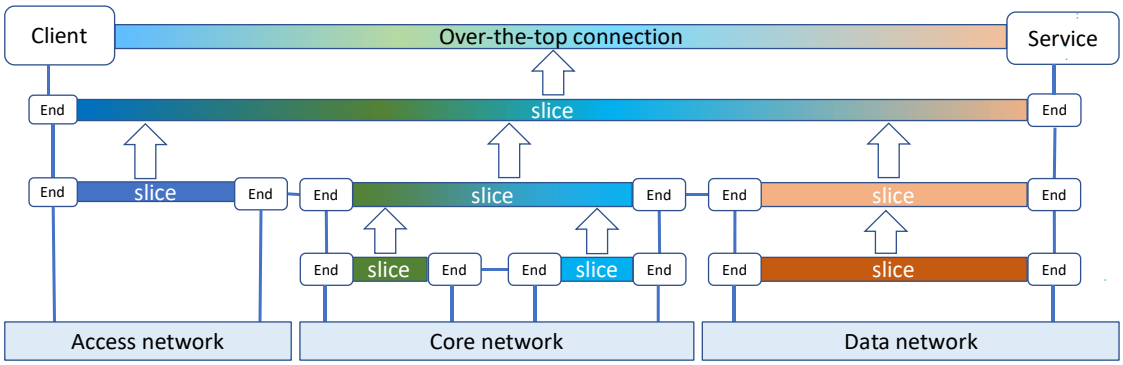

Figure 4: Network Slice Composition

A network slice might span across multiple network domains used by an NSP (e.g., access network, core network, and transport network) and is comprised of dedicated and/or shared resources in terms of functionality, processing power, storage, and bandwidth. A network slice available in the Home Public Land Mobile Network (HPLMN) to their own subscribers may also be available when the subscriber's UE is roaming.

A fully E2E enabled slice requires support across each of the domains shown in Table 2, not all which support slicing at the time of this document's publication.

Table 2:
Network Slicing Domains

Domain	Description
RAN Slicing	The next natural step, once slicing aware Radio Resource Management policy management and associated models get consolidated.
Core Network Slicing	5GC was designed to support network slicing from the very beginning, i.e., 3GPP Rel-15. Since the 5GC is cloud-native consists of a microservice architecture, dynamic slicing will be easier and available earlier.
Transport Network Slicing	Programmable service-tailored connectivity throughout the E2E data path, across all network segments (fronthaul, midhaul, backhaul) and technology domains (IP/ Multiprotocol Label Switching, optical, microwave). The existing heterogeneity (in terms of resources and topology) on the transport underlay makes TN slicing a challenge, and naturally the last part to be consolidated. This requires the completion of Software Defined Network Controller (SDN-C) standards and a wider adoption of SDN technology across the different domains.

A Network Slice Selection Assistance Information (NSSAI) is used to identify a network slice uniquely within the NOP domain. The UE subscription information can contain at least one default

NSSAI to be used when the UE performs initial registration.

The Access Management Function (AMF), or the NSSF of the serving Public Mobile Network (PLMN), maps the subscribed NSSAI values from the home PLMN to the respective NSSAI values being used in the serving PLMN. This mapping is based on PLMN policy or on agreements between the visited and home PLMNs.

Network Slice Service Level Characteristics

Organizations like the 3GPP, GSMA, IETF, and the MEF[13] have specified service level characteristics (SLCs) that describe aspects of a provided network slice. From their documents, a working group of government and industry experts, led by ESF, identified over 90 independent SLCs.

Service level characteristics can be used to specify service level requirements (SLRs), including security and other, on a network slice. When applicable, additional SLCs, such as described in the GSMA Generic Network Slice Template (NEST) document, can be used. SLCs related to QoS are defined in the *3GPP TS 23.501* document.

Each identified SLC is described by the attributes shown in Table 3 below:

Table 3:
An Example Service Level Characteristic Value*[14]*

Attribute	Description
Name	A meaningful alphanumeric identifier for the characteristic. Example: packetDelayBudget
Description	A meaningful statement of the purpose and behavior of the characteristic. Example: An upper bound in milliseconds for the time that a packet may be delayed between the UE and the UPF that terminates the N6 interface. For a certain 5QI, the value of the PDB is the same for uplink and downlink.
Unit of Measure	An expression that specifies a standard of measurement (UCUM). Example: ms
Multiplicity	The possible number of values: Scalar (zero or one) or Array (zero or more). Example: Scalar
Type	A specification of the range of possible values; Specified as either an enumerated list, or as a simple data type (ex: Boolean, integer, float, or string). Example: Integer

Each network slice can provide the agreed service level for specific functionality requested from different service providers or tenants.

SLRs on a network slice specify NSC requirements. A meaningful implementation of a network slice must be able to determine when customer's requirements are not met. Each network slice SLC is intended to specify a metric that is measurable within a network slice implementation.

[13] https://www.mef.net/ In 2015, the Metro Ethernet Forum voted to shorten its name to "MEF" to better reflect its expansion into setting standards for network virtualization.
[14] This table was developed within the Network Slice service level characteristics subgroup.

Each SLRs specifies a value for SLC. That value is then used to determine if the implementation meets the SLRs. Multiple values may be specified for a SLC that is an array.

> *Example*: An SLR on the latency between a UE and the UPF can be specified as a requirement that the packetDelayBudget is 300 ms.

Two strategies are used to simplify the specification of SLRs:

> *First*, there is no need to specify a SLC when any of its possible values are sufficient to meet the customer's requirements. No implementation assumptions are to be made for service level characteristics which are not referenced by an SLR.
>
> *Second*, the remaining SLCs can be bundled into standard, or industry defined subsets called network slice profiles (e.g., 3GPP 5G QoS Identifier (5QI)). When applicable, standardized 5QI values described there can be used.

Network Slice Profile

A network slice profile is the set of SLRs that are applicable to the constituents of a network slice. These include both the NFs and the connecting transport networks.

An example of a network slice profile is the 5G QoS model, specified in 3GPP TS 23.501 and shown in Table 4. The set of 5G QoS network slice characteristics are:

- averagingWindow,
- maximumDataBurstVolume,
- packetDelayBudget,
- packetErrorRate,
- priorityLevel,
- resourceType.

Each combination of values for these six characteristics is assigned a 5QI. Each 5QI identifier implies the corresponding values for the six corresponding network slice characteristics. Table 4 shows the standard values for 5QI = 2.

Table 4:
3GPP Specified Values for 5QI = 2

Characteristic	Value
averagingWindow	2000
maximumDataBurstVolume	N/A
packetDelayBudget	150ms
packetErrorRate	1.00E-02
priorityLevel	40
resourceType	GBR

A network slice can be composed from multiple lower-level network slices. Each segment is represented by a NetworkSliceSubnet. Regardless of how a network slice how is implemented, its network slice profile defines the requirements that need to be met.

In addition to authentication and authorization measures, confidentiality requires protection of data within a network slice both while that data is in transit or while at rest (i.e., stored in transient or persistent storage). Transmission methods include, but are not limited to, shared memory, data busses or networks within a computing platform, and networks between computer platforms. Storage includes any type of persistent, or transient storage device.

Two methods used to protect against data leakage are isolation and encryption. Isolation can be physical or virtual. Dedicated physical resources are required for physical isolation. Isolation may be accomplished using virtual resources, such as sessions, or virtual storage with restricted access.

The level of isolation and encryption are governed by the SLRs specified for a network slice. The implementation of the network slice is responsible for assuring that all functional components sufficiently support the confidentiality, integrity, and availability requirements.

Availability requirements for a network slice are specified as part of its SLRs. The implementation of the network slice is responsible for assuring that the functional components provide sufficient capability to meet those availability requirements. The NSC can negotiate with NSPs to agree on a service profile for each over-the-top connection. For example, a network slice service profile might include a “missionCriticalCapabilitySupport” of “High” or an availability requirement of “High.”

Network Slice Service Profile

Figure 5 shows an abstract model for slice and service profiles that is derived from 3GPP TS 28.541. It is intended to illustrate the relationship between SLCs and SLRs to the slice and service profiles defined by 3GPP. Requirements need to be specified by a slice profile. Slice specific requirements will evolve over time to contain new requirements beyond those currently captured by 3GPP.

An NSP is responsible for evaluating their customer use cases to determine the set of network slices that need to be provided. Each network slice can be characterized by the requirements that met by the respective NSP. The NSP has an obligation to match those requirements with existing slice profiles, such as those from GSMA. If necessary, modify or add SLRs as needed to meet the design requirements.

As shown in Figure 5, network slice requirements are defined by associating a value to one or more network slice characteristics. By preference, network slice characteristics from the GSMA ought to be used. If an appropriate characteristic is not defined there, in 3GPP TS 23.501, or in this document, a new network slice characteristic can be defined as previously discussed in this paper.

Custom network slice requirements are created by choosing values for each of the chosen set of network slice characteristics. The completed set of network slice requirements is then associated with a network service profile. That profile is the basis for a service level agreement (SLA) between an NSC and an NSP. The NSC can negotiate with NSPs to agree on a service profile for each over-the-top connection.

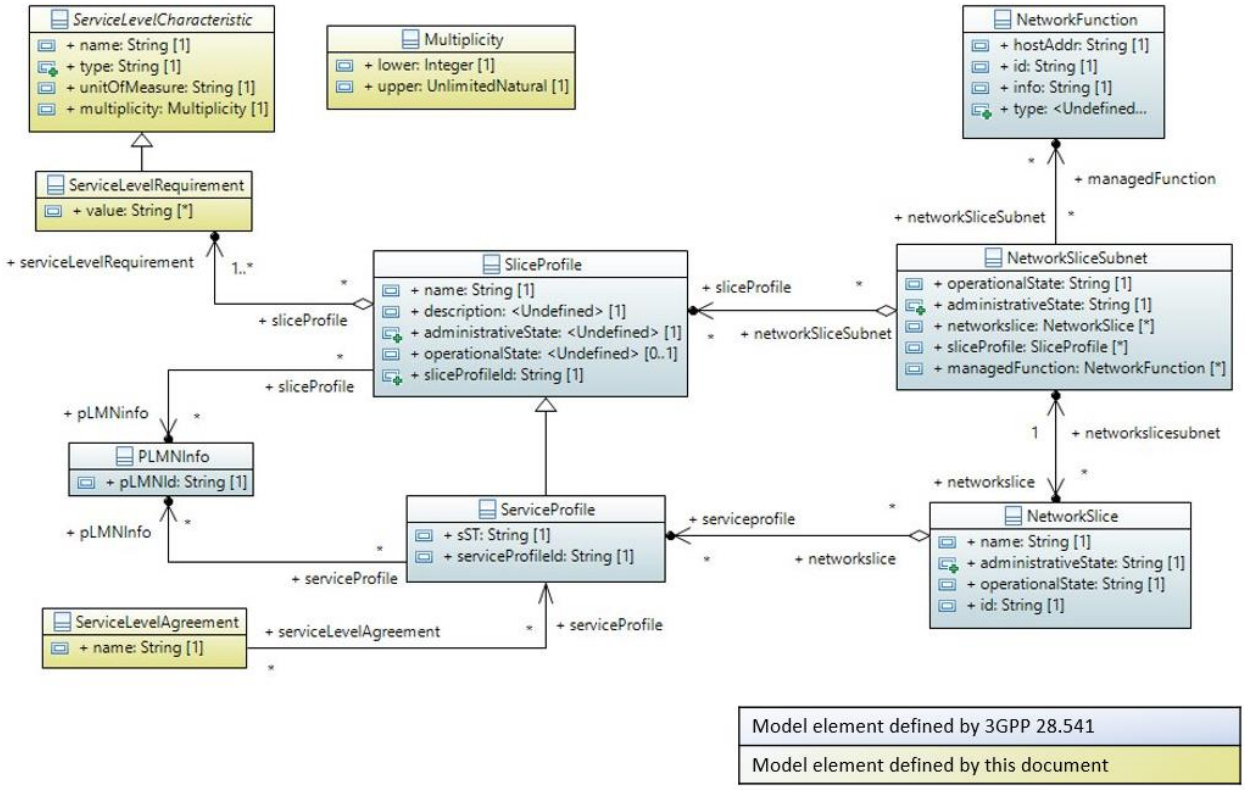

Figure 5: Network Slice Model

Security Management of a Network Slice

Once a network slice has been designed and implemented, it enters the operations phase of the lifecycle. This phase includes activation, modification, and deactivation of the network slice. Activation of a network slice must not commence until all SLRs have been met. Ideally, the network slice needs to stay activated throughout the intended deployment period until deactivation. However, mission objectives or the operational conditions might change over time, so modifications to the network slice might be needed during the deployment period so that specific SLRs are met.

A baseline of security related network slicing features must be established for day-to-day operations. Those features must support confidentiality, integrity, and availability requirements. Zero trust architecture (ZTA) methodology can be implemented and exercised to ensure the secure activation, supervision, reporting, modification, and the de-activation of a slice.

To ensure smooth network slice operations, these security features need be deployed as might be recommended by the 3GPP. 3GPP standards define functionalities of Communication Service Management Function (CSMF), the Network Slice Management Function (NSMF), and the Network Slice Subnet Management Function (NSSMF). These interact with functions of the Operations Support System and Business Support System (OSS/BSS), and the Virtualized Network Function Manager (VNFM) within the MANO architecture. These three components plus the capability exposure platform make up the network slice management components.

Network Slice Orchestration Frameworks

The ETSI MANO and ONAP service orchestration frameworks have been developed with detailed specifications that support the design, deployment, operations, and maintenance phases of slices. In short, the life cycle of a slice can be carried out in an automated manner.

MANO defines an NFV architecture that enables design, management, and allocation of virtual infrastructure resources to VNFs and slices. The main functional blocks within the NFV-MANO are:

- Network Functions Virtualization Orchestrator (NFVO),
- Virtualized Network Function Manager (VNFM), and
- Virtualized Infrastructure Manager (VIM)

Additional functionalities that have been defined for managing containerized VNFs are the Container Infrastructure Service Management (CISM) and the Container Image Registry (CIR) functions. The CISM is responsible for maintaining the containerized workloads while the CIR is responsible for storing and maintaining information of operating system container software images. The behavior of the NFVO and VNFM is driven by the contents of deployment templates (a.k.a. NFV descriptors) such as a Network Service Descriptor (NSD) and a VNF Descriptor (VNFD).

The 3GPP defined functionalities of the NSMF and the NSSMF map to functionalities within the OSS/BSS, and the VNFM within the MANO architecture.

ONAP is an open-source platform that enables product-independent capabilities for design, creation, and life cycle management of network services. The ONAP E2E Network Slicing Use Case realizes functionality of a slice across 5G RAN, core, and transport network slice subnets. The Use Case demonstrates the modeling, orchestration (life cycle and resources) and assurance of a network slice implemented in alignment with relevant 3GPP, ETSI, IETF, and other standards.[15]

5G Threat Vectors

There are many threat vectors that affect a 5G network slice. Of these, Denial of Service (DoS) attacks on the signaling plane, Misconfiguration Attacks, and Man-in-the-Middle (MITM) Attacks pose significant risks to network slicing. Relative to the commonly known confidentiality, integrity, and availability triad, DoS directly attacks the availability of the system and its functionality, including loss of access to the 5G infrastructure, loss of access to remote data, or compromised communication services.

ZTA methodology can help harden a 5G deployment; a big part of ZTA can be accomplished by employing authentication, authorization, and audit (AAA) techniques. Proper implementation of authentication and authorization can also mitigate threat vectors stemmed from misconfiguration attacks.

Both misconfiguration attacks and MITM attacks can have a broad range of adverse effects on confidentiality, integrity, and availability. Misconfiguration attacks refers to a situation where adversaries take advantage of misconfigured system controls. It might include security features

[15] https://docs.onap.org/projects/onap-integration/en/latest/docs_E2E_network_slicing.html#e2e-network-slicing-use-case

that are inadvertently turned off or system monitoring services being disabled.

MITM attacks imply that the adversary secretly relays and possibly alters the communications between two endpoints. Such an attack could be devastating as misinformation and disinformation could be resulted. If ZTA principles are applied, this could be an effective means to help mitigate these MITM 5G attacks.

Cyber hygiene must be followed to ensure cyber impacts due to inherent system vulnerabilities and misconfigurations are minimized:

- ZTA requires AAA techniques that are employed within and between all 5G components and between supporting infrastructure connected elements.
- Perform cyber risk assessment periodically as new and emerging threats continue to be produced to the operating environment.

Goals for End-to-End Network Slicing

A network slice user data is shown flowing from the UE to the data network, passing through RAN functions, TN, and the 5G Core. Orchestration frameworks (e.g., MANO) configures and orchestrates the Open RAN, TN, and 5G Core to realize a network slice. The combination of all these system components is the attack surface for the network slice user data flow.

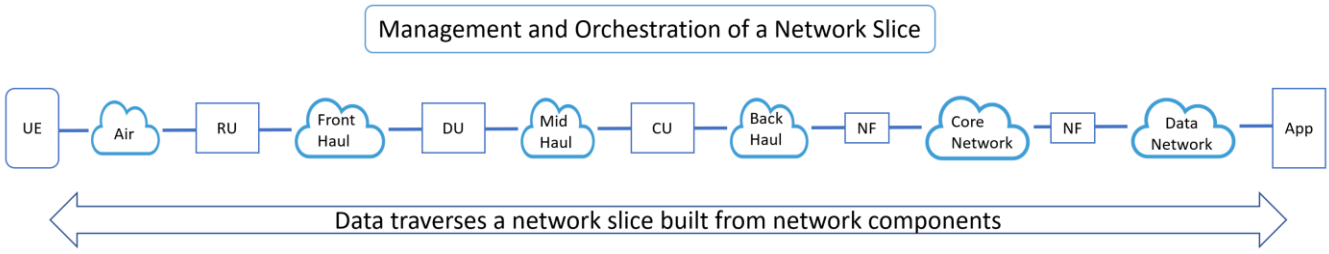

Figure 6: End-to-End 5G Network Slicing Architecture

The high-level goals for E2E 5G network slicing influences the network slice profile. The following are some high-level security objectives for E2E 5G network slicing:

1) Ensure availability of the network slice user data in transit as required by the NSC.
2) Ensure integrity of network slice user data in transit as required by the NSC.
3) A network slice must enforce the physical and logical constraints on its path over its lifetime.
4) A network slice must ensure confidentiality of data in transit as required by its SLRs.
5) Ensure confidentiality of the owner of the network slice user data in transit as required by the network slice customers.

Specific use cases may comprise other high-level objectives for E2E 5G network slicing. The high-level security objectives address the following key assets of a 5G network slice:

- Network slice user data flow.
- Identity of NSCs and NSUs using a network slice.
- Geographic location of the components of a network slice.

Specific use cases may comprise other key assets than what is enumerated in the aforementioned list for E2E 5G network slicing. In this scenario, a single UE connected to two sliced to support two different applications:

1) Demand from a large number of live streams of an on-site sporting event to enhance or argument the real time experience.
    a. Support many subscribers.
    b. Ultra-low latency (to match events in real time) and high bandwidth.
        i. Use of edge compute (to minimize latency and minimize data network backhaul requirements).
    c. Potentially low confidentiality requirement.
2) Support for real time update of fantasy sport team stats.
    a. Support many subscribers.
    b. Ultra-low latency, low bandwidth, high frequency update of odds.
    c. High confidentiality, integrity, and availability triad.
    d. A centralize real time scores statistics server system in a regional cloud.

DESIGN CRITERIA

Network Slice

The requisite criteria to adequately define a 5G network slice is specified by the end-user (NSU/NSC) in the form of a network slice service profile and confirmed by the supplier of the NSP.

A NSP implements a service that realizes a network slice. An NSP might implement multiple network slices. Each network slice may be composed of one or more underlying network sub-slices. At the lowest level and without additional SLRs, a network slice is equivalent to the underlying physical network. Conceptually, any composition of two or more underlying network slices is a new network slice. The NSP has the privileges necessary to use the underlying network slices in the implementation of the new composite network slice.

A network slice can be tailored based on the specific requirements agreed between customer and slice provider and can span across multiple network domains used by an NSP (e.g., access, core, transport, and data networks) and is comprised of dedicated and/or shared resources in terms of functionality, processing power, storage, and bandwidth.

5G network slicing offers a NSP the opportunity to increase the utilization of their physical infrastructure while meeting the SLRs of multiple NSCs. Currently NSCs must have significant in-depth discussions with NSPs on meeting the confidentiality, integrity, and availability of slices by an NSP. 5G network slice standards are immature/nonexistent regarding confidentiality, integrity, and availability SLCs. Standardization efforts and adoptions by NSPs in this area is required before the SLRs for confidentiality, integrity, and availability can be uniformly applied between operators.

Currently, 5G network slicing specifications do not prescribe how network slice are implemented. For instance, a fundamental tenet of the 3GPP is to create specifications, while implementation is left to MNOs and mobile network vendors.

Figure 7 shows some the ways an NSP might choose to implement 5G network slices. The potential variability and inconsistency will have significant effect on both the QoS and confidentiality, integrity, and availability of the 5G network slice. Network slices are implemented as independent logical networks that are separated and managed for each service type within a common infrastructure. Network slicing can guarantee the quality of data transmission for time-sensitive services or mission-critical services, such as connected cars, by allocating isolated and dedicated resources.

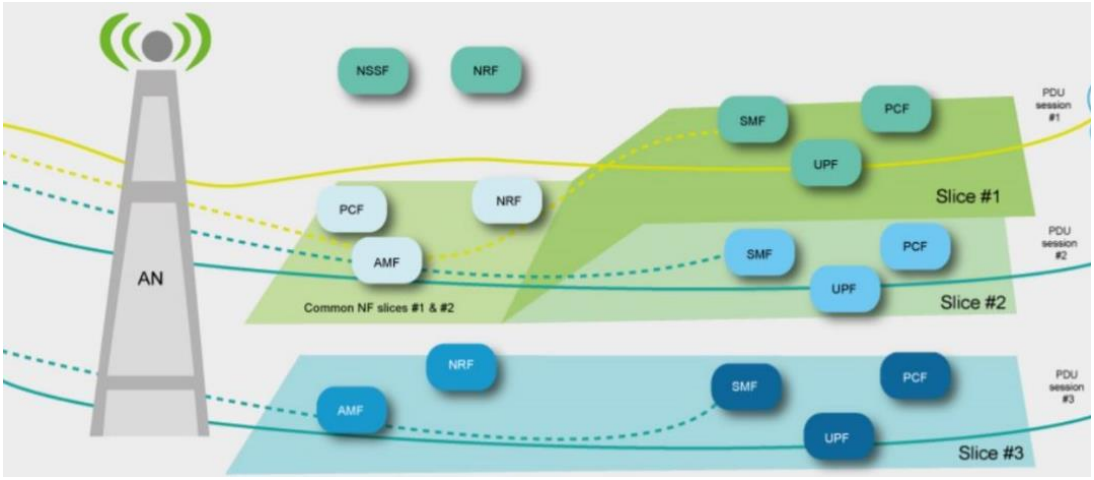

Figure 7: Independent Logical Networks[16]

Slice #1 shares 5G core NFs (Network Resource Function (NRF), Policy Control Function (PCF), and Access Management Function (AMF)) with Slice #2.

However, Slice #1 and Slice #2 do not share other NFs (Session Management Function (SMF) and UPF) and may have their own additional dedicated PCF for each of their slices.

Slice #3 does not share any NFs with the other two slices and therefore from a core network perspective it is isolated from the other two, even though the access network (e.g., RAN) is shared between all the three slices.

Network Slice Service Profile Recommendations

1) Establish and define a comprehensive list of the slice profiles (across all SLAs) to be accommodated by the NSP.
2) Establish the types and requirements of the UE that will connect to the RAN for each individual slice profile (across all SLAs) accommodated by the subject 5G network.
3) Establish the types and capabilities of data networks that will connect to the N6 Interface for each individual slice profile (across all SLAs) accommodated by the subject 5G network slice.
4) Establish the full list, and associated metric value ranges (e.g., SLRs), of all SLCs contained within the slice profiles (across all SLAs) accommodated by the subject 5G network slice.
5) Establish the maximum of number of concurrent slices, for each individual slice profile (across all SLAs), that will be accommodated by the subject 5G network slice.
6) Establish the requisite combinations (including types and quantities) of component NSPs (across all SLAs) that will be concurrently accommodated by the subject 5G network slice.

[16] From 3GPP web

7) Establish the method, frequency, requisite response timing, and prioritization policies for the dynamic administration of network slicing across all SLAs accommodated by the subject 5G network.
8) Define each network slice service profile using SLR names and values as specified by 3GPP, GSMA, or other industry or standards development bodies.
9) Before provisioning, the NSP assures the requested network slice can conform to requested SLRs and other requirements.
10) Changes to the security or other requirements of an existing network slice is denied if the NSP cannot assure that the implementation of that network slice will conform to the requested changes.
11) Once provisioned, the implementation of a network slice continues to conform to the requirements specified when the network slice was provisioned or modified.
12) Evaluate and confirm that the subject 5G network can accommodate the types and requirements specified by the NS service profile.
13) Evaluate and confirm that the subject 5G network can concurrently accommodate the requisite combinations (including types and quantities) of individual slice profiles (across all SLAs).
14) Evaluate and confirm that the subject 5G network can accommodate the method, frequency, requisite response timing, and prioritization schema for the dynamic administration of network slicing across all SLAs.

Open RAN

To support the overall security goals described in the previous section "Goals for End-to-End Network Slicing," any Open RAN implementation must meet the following security objectives:

1) Ensure the confidentiality, integrity, and availability triad of the network slice user data in transit within the Open RAN.
2) Ensure integrity of the physical and logical path of the network slice user data within the Open RAN.
3) Ensure confidentiality of the identity of the owner of the network slice user data within the Open RAN.
4) Ensure confidentiality of the geographic location of the network slice user data within the Open RAN.

Although there are many methods to compromise a network slice, the design of an Open RAN implementation should specifically mitigate unauthorized access and misconfiguration compromises. The remainder of this Open RAN section addresses these security objectives and mitigations for an Open RAN based on O-RAN Alliance specifications.[17]

Unauthorized access to a network slice within an O-RAN system requires access to the 5G System user plane and control plane. The 5G System provides for optional Packet Data Convergence Protocol (PDCP) confidentiality and data integrity mechanisms to prevent unauthorized access of the user plane and control plane within the O-RAN system. If these mechanisms are not

[17] https://www.o-ran.org/

implemented by an operator, then an attacker could have access to the user plane and control plane within the entire O-RAN system.

O-RAN supports optional 3GPP confidentiality and data integrity mechanisms for the N2 and N3 back haul interfaces between the 5G RAN and 5G Core[17]. If these optional mechanisms are not implemented by an operator, then a threat actor could have access to the 5G system (5GS) user plane and control plane between the O-RAN system and the 5G Core.

Like any component of a 5G RAN, the CU requires security controls to prevent unauthorized access to the user plane and control plane. A virtualized CU requires similar security controls.[18][19][20][21]

Misconfiguration exploits target the availability and integrity of a network slice. An O-RAN system misconfiguration attack on the availability of a network slice could deny service with precision ranging from targeting an operator RAN down to a specific network slice. An O-RAN system misconfiguration attack on the integrity of a network slice could modify the physical and/or logical path of the network slice user data in transit from RU to CU.

An O-RAN system misconfiguration attack surface consists of the system that manages O-RAN network functions and transport networks. As illustrated in Figure 8 below, the system is known as the Service Management and Orchestration framework (SMO).[22] Many features of the SMO follow the network orchestration and management systems defined by 3GPP, ETSI, and ONAP.

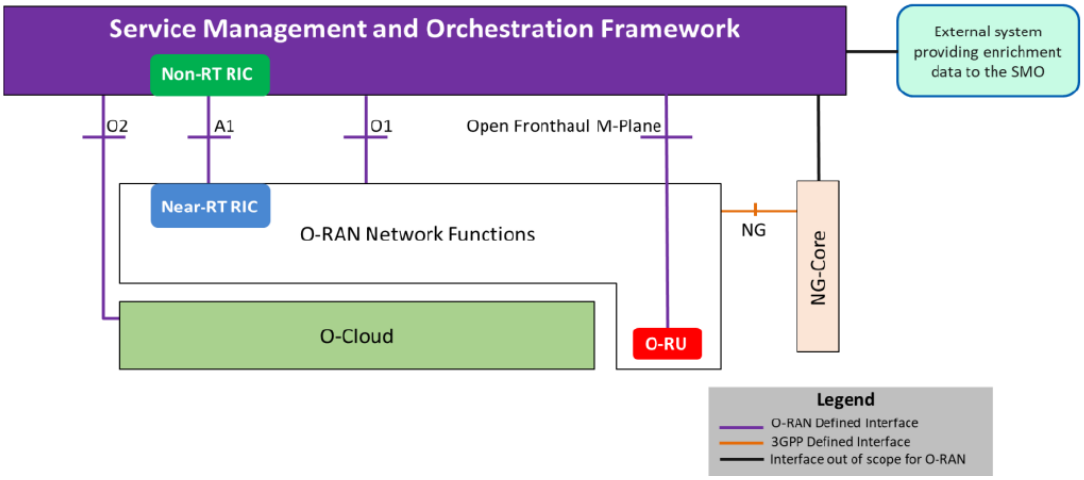

Figure 8: O-RAN Service Management and Orchestration

The "Management and Orchestration" section describes the attacks, attack surface, and potential mitigations for service orchestration frameworks. This section pertains to aspects of the SMO to

[18] https://media.defense.gov/2021/Oct/28/2002881720/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_I_20211028.PDF
[19] https://media.defense.gov/2021/Nov/18/2002895143/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_II_20211118.PDF
[20] https://media.defense.gov/2021/Dec/01/2002901540/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_III_508%20COMPLIANT.PDF
[21] https://media.defense.gov/2021/Dec/16/2002910260/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_IV_20211216.PDF
[22] "O-RAN Minimum Viable Plan and Acceleration towards Commercialization White Paper," 29 June 2021.

include the architectural framework, onboarding procedures, and security procedures.

Other attack vectors arise from new SMO management capabilities and interfaces. The non-Real-Time RAN Intelligence Controller (non-RT RIC) configures network slices based on applications called rApps. An attack on or by an rApp could impact the availability of a network slice. The ESF publication *Open Radio Access Network Security Considerations* discusses rApp and non-RT RIC security objectives, threats, and mitigations.

The SMO consists of management interfaces to O-RAN NFs as shown in Figure 8. The O1 interface manages the DU, CU, and other ORAN NFs. The Non-RT RIC manages the Near-Real-time (Near-RT) RIC network functions using the A1 interface. The Open Fronthaul M-Plane interface manages the O-RAN Radio Units (O-RU)s. The O2 interface manages the O-Cloud, where the O-Cloud is the cloud infrastructure for the O-RAN system. Security controls must be in place to help prevent an attacker from modifying O-RAN system configurations with unauthorized access to these interfaces.

To address these and other O-RAN security concerns, see the recommendations for security controls and mitigation in ESF publication *Open Radio Access Network Security Considerations*.[23]

Core Networking

The high-level potential threats that have been identified to slicing with respect to the core network, include attacks that may originate from UEs, unauthorized humans, and unauthorized machines towards the core NFs. The attacks may include spoofing of customer specific NSSAI by the UEs and other identity thefts. Other attacks of this class include un-authorized access to customer NFs by NFs from another slice using the control plane. For example, when Unified Data Management (UDM) in one slice makes a request for subscription information of members of another slice to a unified data repository (UDR) that is in a different slice.

Misconfiguration and tampering attacks can lead to Denial-of-Services (DoS) to legitimate slice users. Examples of such attacks include:

- Tampering of NSSAI information when data is in flight between NFs (e.g., from UDR to UDM, 5G radio node (gNB), and AMF etc.);
- Tampering of slice-specific data-usage;
- Tampering slice-specific authentication data between NSSAAF and AMF;
- Replay attacks; and
- Misconfiguring of slice-specific info (e.g., NSSAI at the UDR, policies related to slices at the PCF, NSSF, charging and logs related to slices etc.).

Passive or active eavesdropping could lead to leakage of highly sensitive customer slice such as: leakage of NSSAI over the air, and subscriber information (e.g., Subscription Permanent Identifier (SUPI), UE location information, subscription information, slice information) as to who is using which slice may be leaked between slices. Also, leakage of slice-specific Network Information (e.g., routing information from NRF) and leakage of sensitive slice information to external networks (e.g., application function).

Signaling storms on N2, N3, and over service-based interfaces (SBI) can cause DoS to legitimate slice users, and attacks from UE over N1 can impact N2 and N3 interfaces. Similarly attacks from N6

[23] https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Enduring-Security-Framework/

and N9 interfaces could impact the customer-slice user plane.

Recommended Core Network Security Mitigations:

1) Security mitigations to protect the 5G system identified by the CSRIC VII[24] include using non-access stratum (NAS) signaling integrity and confidentiality between the UE and the core network as well as using mutual Transport Layer Security (TLS)-based authentication and secure communications between NFs using the service-based infrastructure. For NFs-to-NFs communications over non-SBI interfaces, CSRIC VII recommends using Internet Protocol Security (IPSec).
2) Use of network slice-specific authentication and authorization by leveraging a Network Slice-Specific Authentication and Authorization (NSSAA) to protect against un-authorized access to slices by UEs using NSC-specific credentials (these credentials are different from NOP credentials that are used for 5G-AKA).
3) Provide capability to enable logical / physical isolation of the control plane and user-plane NFs belonging to each of the NSCs. Each can provide logical isolation of NSC slice subscriber info (e.g., using separate UDR instances per slice) and based on SLRs, provide physical isolation of NFs per slice (e.g., separate UDM / Authentication Credential Repository and Processing Function (APRF) by means of hardware security models)).
4) Employ a dedicated intermediate certificate authority (ICA) that is used for life-cycle management of the certificates issued to the NFs belonging to a particular slice.
5) Employ an authorization server to provide attribute and role-based access control (RBAC) of humans and machines to perform per slice configuration, fault, and performance management. Ensure that slice-specific logging can also be performed.
6) Employ a security vault to provide confidentiality and integrity of all sensitive and security data (e.g., private keys, open authorization [OAuth] tokens, cert chains) used as part of control and management plane messaging and to isolate sensitive and security data from the rest of the platform. This makes the data available only to the respective authorized NFs within a slice.

Store subscription information associated with a NSC's subscriber within encrypted databases and employ backup and data recovery processes from "golden" data. Protect subscriber data-at-rest using a secure environment (e.g., hardware security module (HSM)). Similarly, an HSM can be used to protect applicable credentials used for network slice-specific authentication.

User Equipment

Current 3GPP 5G standards allow a UE to access up to eight network slices. The 5G UE must be hardened to prevent the UE from being used as a means for network slices to interact inappropriately.

In the design of device system architecture, network slicing features require the coordination between the upper operating system and the bottom communication modem. Table 5 shows two ways to implement network slicing features in the device system architecture:

[24] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii

Table 5:
Traffic to Network Slice Matching Schemes

Scheme	Description
Modem-centric	The modem matches traffic by its attributes to a network slice.
OS-centric	The operating system matches traffic by its attributes to a network slice.

The two approaches include two OS-Centric scheme solutions, namely, changes to the operating system and Application APIs respectively. The overall impact of this is determining where the network slice termination point will be in on the 5G device in one of three locations:

- The Modem,
- The Operating System, and/or
- The Application.

To hide details of data connection management and maintenance from applications, native operating system characterizes a data connection by network capability. Each network capability stands for a certain kind of capability. Since operating system manages data connections based on Access Point Name (APN) and Data Network Name (DNN), the capabilities associated to individual services provided by system identified by the APN/DNN are the most important.

Given the complexity of the OS-Centric scheme and fragmentation, the recommendation is to select a “modem centralization scheme" which provide users with more diversified, flexible, and evolvable high-quality network slicing services.” However, the network slicing at the OS/Application layer provides greater flexibility and enhanced user experience at the same time.

It is understood that implementing an OS-Centric scheme for OS/applications is challenging since an operating system does not natively support URSP for the following reasons:

- A URSP rule is composed by a traffic descriptor (TD) and RSDs.
- The upper layer (e.g., an application) specifies the TD and the modem uses the TD to look for a URSP rule matched to the TD.
- The modem with a matched TD tries to establish a PDU session using the corresponding RSDs in the order of precedence.
- Since operating system designs data connection framework based on APN type, the operating system can be modified for the reason explained below to use TDs.

Table 6:
The following is an example URSP rule for enterprise traffic.

URSP Rule (enterprise)	
Precedence:	1 (0x01)
Traffic Descriptor	
Operating System Id + Operating System App Id Type	0x97A498E3FC925C9489860333D06E4E470A454E5445525052495345
Route Selection Descriptor	
Precedence:	1 (0x01)
Component #1: S-NSSAI	SST:1 SD:2 (0x01000002)
Component #2: DNN	enterprise

Recommended User Equipment Security Mitigations:

1) Start with the current modem-centric approach, and then move to an OS-centric approach once the issues about a standards-based uniform approach can be developed in the future.
2) When available, terminate the slice in the application. This might provide greater security from a confidentiality or privacy perspective when compared to the current modem-centric approach.
3) Implement mobile device management (MDM) to protect network slice thus protecting the device since it is all self-contained. MDM agents may not be applicable on all UEs.
4) Protect NSSAI from being tampered and therefore recommend storing it within a secure environment (e.g., UICC).
5) Perform authentication and authorization of application requests to access a network slice.

Cloud and Virtualization

Most 5G systems will be instantiated on virtualized compute, network, and storage resources; and will utilize on-premises virtual machine management (private cloud) or in commercial cloud platforms (public cloud). Mapping most of the 5G system into the virtualized, managed resources of a private or public cloud will require security controls on all uses of those resources.

Depending on the type of cloud deployment for 5G system, the set of security controls that are required to harden the 5G system need to be considered and deployed appropriately. There are Industry standards and guidance that provide the list of security controls. These are generic in nature and need to be configured specifically for the cloud provider/technology.

The configuration of the cloud controls depends on the responsibility for the security of the data, which depends upon the type of cloud deployment that is being leveraged such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), etc.

Recommended Mitigations for Virtual Systems:

1) Ensure that controls implemented by the 5G system cannot be bypassed using direct access to cloud resources.
2) Establish necessary network connections between the components of the 5G system are established and permit no other connections.
3) Protect data storage used by the 5G system from access, tampering, or deletion by any unauthorized parties.
4) Establish and maintain mechanisms for monitoring operation of the 5G system, especially resource usage, actions of authorized cloud administrators, and network traffic flows. (This supports both real-time and forensic analysis of cloud operation to support assurance for the 5G services.)

A cloud platform (public or private) does two things to support the hardening of network slicing: provide a foundation for overall 5G operations, and provides resources to set up, manage, monitor, and tear down security services and dynamic resources allocations for slices.

Assured 5G operations are foundational to network slicing – To gain this assurance, 5G operators leverage cloud services in their design and deployment as described below. In all cases, the principle of least privilege is essential: assign to every person or non-person entity only the privileges and accesses necessary for operation.

Recommended Cloud Platform Hardening Mitigations:

1) Employ cloud tenant separation mechanisms (e.g., "virtual private cloud") to ensure separation between the 5G system and other workloads within the supporting cloud platform.
2) Employ cloud identity and access management (IAM) features to ensure that only authenticated and authorized administrators can create or alter cloud resource configurations. Manage authorized identities centrally.
3) Configure monitoring mechanisms across the cloud platform (public or private) to record all critical actions and resource usage. (General principles for monitoring are given by NIST SP800-92; specific guidance for each cloud platform is offered by that platform's vendor.)
4) Configure storage supporting the 5G system to use access control, integrity assurance, and encryption, with keys managed by the cloud platform.
5) Configure network segmentation to separate user plane from 5G control plane traffic.
6) Ensure that control plane entities, such as VNFs/CNFs, have only necessary network connectivity.

Secure instantiation of security services and allocation of securely configured resources to assure the integrity and selected security attributes of slices. To meet this objective, 5G operators can leverage the resource management and security services offered by cloud platforms.

A network slice provides network connectivity for authorized UEs while enforcing specific network performance, integrity, and confidentiality guarantees. Therefore, certain entities (such as VNFs) in the 5G logical architecture possess privileges to dynamically allocate, manage, monitor, and

deallocate network paths to support slice operations.

Recommended Security Mitigations for Network Slice Creation:

1) Do not configure such dynamic network assets "manually;" instead, invoke an approved template or script to set up the slice assets. (E.g., Terraform, CloudFormation, etc.)
2) Do not deploy vulnerable components in production; continuously monitor for new vulnerabilities and remediated. Follow guidance provided in National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF) "PR.IP-12: A vulnerability management plan is developed and implemented."
3) Employ secure software development and operations processes for any code being used in production, including the management scripts and Infrastructure as Code (IaaC) scripts.
4) Configure security controls, monitoring, and resource usage constraints onto the dynamic network path and its elements before enabling operation or connecting any UEs to the slice.
5) Ensure that the network path resources/assets associated with the slice are 'owned' by a dynamically created identity specifically designated for this purpose. (e.g., provisioning a dedicated identity to serve as the owner for the slice aids separation between slices and helps with slice monitoring.)
6) Instantiate the requisite computing resources with an approved template, control image, or script such as a dedicated VNF/CNF.

Interconnect & Roaming

Roaming between network operators is based on dedicated roaming agreements, which typically are established, along with technical requirements, prior to any roaming. This applies to network slicing roaming agreements too. Roaming agreements are necessary to allow operators to configure an E2E network that provides the desired overall functionality and service parameters. The GSMA broadly outlines the content of such roaming agreements in standardized form.

For network slice roaming to become a reality, several technical and business aspects first need to be in place:

1) MNOs need to rollout slicing in their mobile networks and have a network slice product offering.
2) Extended roaming agreements including slice definitions with SLAs based on slice attributes.
3) Operational support (management and orchestration, and service assurance) in roaming environments.
4) Global availability of slicing compatible UEs.

An NSP can consider the following when procuring network slicing services:

1) The visited network could provide to the roaming user a network slice with equivalent functionality of the slice used in the home network, e.g., the roaming partners may agree to support a common set of standardized slices.

2) The home network might export the blueprint of a custom network slice used by a user so that it can be instantiated and administered by the visited network.
3) The home network might extend the slice into the visited network, provided it has authorization from the visited network to control the resources.

Interconnection refers to the technical physical and logical connection between two or more MNOs. Interconnection is a necessary component of roaming between two or more public land mobile networks (PLMN)s.

3GPP specifications offer an interconnection solution based on the Security Edge Protection Proxy (SEPP). All signaling traffic across and between operator networks MNOs is expected to transit through these security proxies.

The SEPP mitigates attacks on the N32 interface by protecting 3GPP control plane messages between interconnecting MNOs. Security controls for protecting confidentiality and integrity for the N32 include either TLS or Protocol for N32 Interconnect Security (PRINS). Additionally, 3GPP TS 33.501 specifies protection for the N32 interface in clauses 13.1 and 13.2.[25] [26]

Recommended Controls and Mitigations for 3GPP Interconnect Security:

1) Transit the signaling traffic between MNOs through SEPPs.
2) Enable filtering of traffic coming from the interconnect with authentication between SEPPs.
3) Employ application layer security solution on the N32 interface between the SEPPs to provide protection of sensitive data attributes while still allowing mediation services throughout the interconnect.[27]

Data Networking

Given the dynamic nature of the 5G data network interworking environment, and since the data network may not necessarily belong to the NSP or the NSC, there are various threat actors and associated threats that would have to be considered such as: misconfiguration and tampering attacks, passive and active eavesdropping, spoofing, and signaling and user-plane flooding attacks causing DoS.

Examples of tampering or misconfiguration attacks include:

- Replay of Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), or Protocol-Independent Multicast (PIM) messages,
- Tampering with NSSAI information carried between AAA Proxy (AAA-P) and DN-AAA servers as part of the slice-specific authentication procedure, and
- Tampering with authentication and authorization data carried within Extensible Authentication Protocol (EAP) messages, modification, and replaying slice-specific user plane messages between data network and UPF over N6.

[25] REPORT ON RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY, FCC CSRIC VII
[26] 3GPP TS 33.501
[27] Additional resources for security framework, data models, and APIs are the MEF 117 SAS Service Attributes and Service Framework; MEF 118 Zero Trust Framework for MEF Services; and MEF 128 LSO API Security Profile

Passive and active eavesdropping could lead to information disclosure to un-authorized entities. Example of such attacks include subscriber info (e.g., SUPI, UE location, subscription info, and more importantly slice info) leakage, as to who is using which slice may be leaked between slices and to external entities. Such disclosures are possible if EAP messages are not protected. Additionally, leakage of sensitive network info to other slices (customer or non-customer) or to external entities: Leakage of slice-specific network Information (e.g., routing information: DHCP, DNS messages). Remote Authentication Dial-In User Service (RADIUS) and Diameter messages may also leak such information which can then be used by an attacker to target the N6 or the data network network.

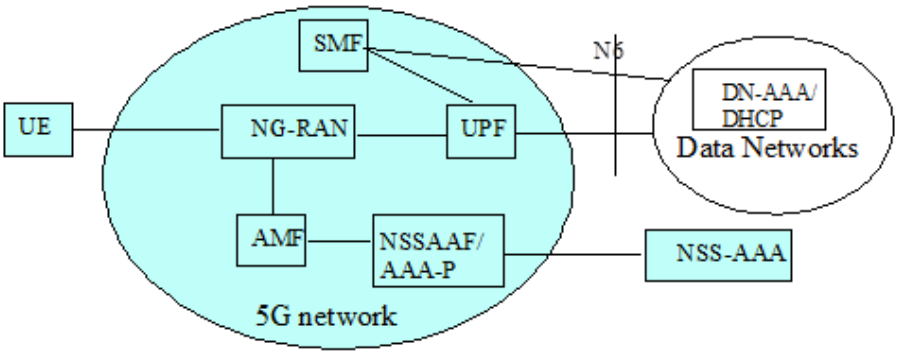

Figure 9: Reference Architecture for 5G Network Interworking[28]

Mitigations to Facilitate Future Data Network Interworking Security in the Earliest Stages of Design:

1) Leverage "sandbox" and test environments to model E2E 5G-to-external data network interworking, including leveraging native slicing specifications in other network types, Virtual Private Network (VPN) and tunneling protocols, and Management and Orchestration frameworks to facilitate secure data network interworking.
2) Engage in follow-on work through the ESF or other suitable mechanism to develop more detailed guidance for the rapidly evolving network slicing work of MEF, TMForum, GSMA and others to extend the capabilities of 3GPP/5G slicing into the broader global networking frameworks.
3) In requests for proposal and system design documents, requestors assess and specify full-E2E connectivity requirements, including slice parameters and/or key 5G slice-defined QoS requirements that are to be maintained E2E across non-5G environments (e.g., security, physical/logical separation, encryption, QoS, latency, etc.)
4) Network providers pre-negotiate internetworking agreements necessary to provide E2E connectivity across the full geographic footprint where connectivity is needed.

Regardless of how data network interworking is implemented, network design and deployment need to consider the threat environment at the N6 interface to ensure the confidentiality, integrity, and availability triad of the overall information system.

[28] 3GPP TS 29.561 V17.5 figure 6-1

Recommended Mitigations to Counter the Risks Previously Described:

1) Protect integrity and authenticity for all signaling (e.g., Use DNSEC to protect DNS messages.) and control plane messages.
2) Transport EAP messages carrying authentication and authorization data over secured transport mechanisms that provide the confidentiality, integrity, and availability triad as well as replay protection (e.g., Diameter messages that are protected for integrity and authenticity).
3) Protect all policies and data associated with network slicing at the UPF for the N6 interface from tampering using data-at-rest integrity protection.
4) Control human or machine access to the N6 configuration on the UPF by leveraging an IAM system that uses granular access control. Such controls include attribute-based access control or using multi-factor authentication for humans.
5) Protect the user plane traffic dedicated to a customer slice at the IP layer for integrity and confidentiality. Recommend using IPSec between the UPF to the customer network in an E2E manner. In some cases, the protection may be done in a hop-by-hop fashion.
6) Instantiation of a customer dedicated N6 interface associated may be reside on a shared UPF or on a dedicated UPF for customer.
7) Use mutual authentication for communication between the AAA-S / DN-AAA and the NSSAA and SMF respectively, by means of X.509 certificates that have been issued by a mutually trusted certificate authority. Similarly, use mutual authentications for all communications between the SMF and the DHCP servers over the N6 using X.509v3 certificates.
8) Each instance of the N6 interface at the UPF that is dedicated to a slice shall have the capability to rate-limit and firewall user traffic per slice based on current policies.
9) For each network slice, support rate-limited signaling /control plane messages for each N6 interface used to communicate to DN-AAA, DNS, DHCP servers etc.

Management and Orchestration

A very highly sought-after target for compromising a 5G network slice is attacking the MANO system. This is because the design, deployment, and operation of the slice will be done by the management platform, mostly via IaC, programmed automation playbooks, and orchestration of functions. Commandeering the MANO system enables the ability to introduce security configuration vulnerabilities that attackers can use to compromise the integrity of the network slice. The threats encompass unauthorized modifications of the playbooks, compromised software supply chains, alterations of the IaC scripts physical network function (PNF) and VNF (xNF) images.

The set of security controls required to protect the MANO system are the same as protection of an application, guidance can be found in NIST publications such as:

- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST 800–190 – Application Container Security Guide

In addition, ensure that the security controls are tailored towards the specific needs of the NOP system- such as the API security system- consider the structure of the API's as defined by 3GPP and

TMF in evaluating attacks against them.

Ensure that only authorized entities (humans and machines) have the capability to modify or update slice characteristics. The authorized entities need to be granular and different for each of the processes (ex: slice design, activation, etc.) associated with the slice lifecycle.

Network Slice Creation and Deployment

The requirements specified by a network slice at inception are expected to be met throughout its lifecycle. Network cyber-attacks need to be considered. These potential vulnerabilities include traffic injection attacks, impersonation attacks, and DoS attacks, including exhaustion of resources.

More specifically to roaming scenarios, new vectors of attack related to interconnect can arise especially considering management and orchestration across different administrative domains.

Slicing across domains will most likely use heterogeneous platforms and solutions: slicing components can be implemented in firmware, operating system kernel level, in the virtualization software systems or even in regular software. In this wide spectrum of environments, the slicing components may be provided by different vendors thereby making difficult a common level of security for a network slice.

Since roaming requires additional interconnect interfaces, these can be used as attack points and expose vulnerabilities between slices and services.

The threats covered here focus primarily on newer threats related to NFV with a focus on slicing. Threats relating to the infrastructure, e.g., cloud infrastructure, or generic 5G system threats or generic threats relating to trust enabling functions and services, (e.g., time service, NTP, DNS, DHCP etc.), are not addressed in this document.

Regardless of which frameworks (e.g., MANO, ONAP) are used, the threats described here are applicable to the service and slice design and deployment infrastructure, and ought to be mitigated to ensure the confidentiality, integrity, and availability triad of the overall information system. Some of the key threats that would have to be addressed include, un-authorized access and elevation of privileges.

A threat actor gains access and elevates privileges and thus on-boards a malicious network slice containing malicious VNFs that will attack the NFs of other tenants. A threat actor could perform an un-authorized request for reservation of compute, store, and network resources (e.g., using the Or-Vi or Vnfm-Vi interface). The impact could be network slice SLA and service degradation to legitimate slices.

A threat actor attacking a weak RBAC mechanism or exploiting a vulnerability on the system can allow the threat actor to further deploy malicious code into the telecommunications environment by modifying the deployment patterns. The OSS/BSS system may be used (e.g., using the Os-Ma interface) by an attacker to gain privileges to modify slice design and orchestration/activation of the slice and associated NFs, and modify changes to slice connections (e.g., modifications to service chaining).

Another class of attack that must be addressed as a high priority includes tampering. An attacker may tamper with policy registries (e.g., authorization policies), VNF or CNF packages and artifacts, modification of affinity and anti-affinity rules, VNF instance information, VNF / CNF attestation

data, etc.

Spoofing of user or machine identities attacks using password/private key stealing, or Man-in-the-Middle (MITM) may allow the impersonator to conduct activities in deploying malicious code into the telecommunications environment using the OSS/BSS, NFVO, VNFM or VIM/CISM. An attacker could also spoof the URL of a legitimate repository from where the orchestrator is expected to pull images.

To Counter the Above Threats, and Ensure Network Slices Are Designed and Deployed in a Secure Manner, Recommended Security Mitigations Include:

1) A centralized identity management system that is part of the NSP's PKI system, which is capable of issuing and managing X.509v3 certificates to the various orchestration components (MANO or ONAP functions). The certificates are then used for mutual authentication between the different components before service requests can be processed.
2) Granular attribute and role-based access control (RBAC) that limits access to a "resource" by "scope" and "duration" and the type of "actions" (e.g., Create, Read, Update, and Delete [CRUD] operations) that can be performed.
3) Ensure that the authenticity- that every artifact is from a trusted vendor- and integrity of the packages and artifacts are maintained throughout the life cycle of the xNF. Another class of attack that must be addressed as a high priority includes tampering. An attacker may tamper with policy registries (e.g., authorization policies), VNF or CNF packages and artifacts, modification of affinity and anti-affinity rules, VNF instance information, VNF / CNF attestation data, etc.
4) Finally, ensure that the NSP certifies the VNF packages do not contain any known vulnerabilities once the package has been on-boarded by running security scans. Additionally secure "supply-chain" requirements may need to be adhered to by the NSP.

The security features listed above, and using zero-trust framework, would help mitigate attacks on on-boarding and instantiation of the network slices.

Network slice design and deployment across networks will rely on defined standardized slice types (in 3GPP) and the GSMA-defined Generic Slice Template (NEST). End to end inter-operator design and deployment of slices is currently unlikely with roaming and interconnect relying mostly on SLAs between operators. This is in part because one MNO's network management cannot be imposed on another MNO's operations. Particularly challenging is in the case of local breakout for slice orchestration as both the home and the visited networks are involved.

Orchestration of a slice will require service agreements to be in place between transport, RAN/core, and slice providers in advance of a service request. Coordinated management is essential between the RAN/core, interconnection, and the transport domains to ensure the E2E SLAs, which may include cross-domain orchestration. In addition to that, transport and mobile network capabilities are expected to be harmonized to ensure that mobile network capabilities are not compromised by limitations in the transport network.

Network Slice Isolation and Segregation Recommendations:

1) Logical isolation and performance isolation between network slices.
2) Physical isolation of physical resources for network slices, and separate management systems and administrators will be required to meet high confidentiality, integrity, and availability triad requirements.
3) Data plane on one slice ought not influence other network slices.
4) Control plane actions (e.g., creation/update/deletion) have no influence on other slices.

ETSI recognized that leakage of data between network slices as a significant problem. To avoid leakage or breach issues between network slices, it is recommended that any implementation provide risk mitigation from attacks from one slice to another.

Network Slice Implementation Recommendations:

1) Usage-specific security policies regarding authentication and authorization requirements (e.g., IoT vs. mobile broadband user) must be configurable.
2) Slice-specific authentication that is performed over and above the 3GPP primary authentication is carried out to meet customer user authentication requirements.
3) Network Slice and the provider take into consideration privacy of user information and device identifiers, including following regulations like Customer Proprietary Network Information (CPNI).[29]
4) Confidentiality must be considered for network slice selection information when sent over the RAN.
5) Isolation of network traffic ought to be maintained when a common control plane between different network slices is used.
6) Security of sensitive shared network elements, such as the UDR that stores subscriber profiles, needs to be secured and actively monitored.

[29] Customer Proprietary Network Information (CPNI), June 9 2008, **https://docs.fcc.gov/public/attachments/DA-08-1321A1.pdf**

OPERATIONS AND MAINTENANCE CRITERIA

Introduction

5G network slicing adds complexity to a network. While there are standards defining specifications for how operators build their 5G networks, there are no clear specifications for how network operators and slice providers develop, implement, and maintain security for network slicing.

During operations and maintenance, improper NS configurations and management may present an opportunity for malicious actors to access data from different slices that they otherwise do not have access to, or to deny access to authorized slice users. This is the reason authentication and attribute-based access controls (ABAC) are fundamental to a network slice.

Definition of Operations and Maintenance

When a systems engineer fields a system, it enters the Operations Phase. Operating a 5G network typically involves day-to-day operational and management activities, including (but not limited to) scaling in/out based on service assurance, health monitoring, security scans, etc.

Maintenance refers to the general upkeep of the network slices. Preventive maintenance is a schedule of planned actions aimed at preventing breakdowns and failures before they occur and at preserving and enhancing equipment reliability by replacing worn components before they fail. Preventive maintenance for a 5G network slicing might include software patching and periodic updates.

Operations and maintenance (O&M) involve monitoring configuration, fault, and performance management by humans, or by automation. To ensure security, all intra-datacenter communications must use standards-based and approved encryption, and be mutually authenticated security (e.g., mutual TLS or IPsec) to ensure confidentiality, integrity, and availability.

Importance of Operations and Maintenance

For 5G network service providers, the O&M phase includes activation, supervision, reporting, deactivation, and modification activities. Each network slice may have unique SLRs. The actions of operators and O&M tools must assure that those requirements are met. These need robust O&M tools, processes, and capabilities. For example, maintaining the integrity of the O&M platforms is extremely critical and therefore their trust-enabling functions (e.g., PKI authorization server) need to be always validated for integrity leveraging hardware roots-of-trust and remote attestation.

Backwards compatibility or at least co-existence of multi-mode network elements from previous generations also poses architectural challenges to 5G operators. These complex structural problems are exacerbated in roaming situations, or in use cases that involve multi-operators working together. Additionally, network slice providers work with the vendor of VNF packages, platform software vendors etc. to ensure that the authenticity (ensuring every artifact is from a trusted vendor). Each NSP must assure the integrity of each package is maintained throughout the life cycle of the VNF. To achieve this the NSP and the vendors need to agree on a trust model that either uses third-party CA or the NSP's PKI system. Also, the NSP needs to certify that the VNF

package does not contain any known vulnerabilities once the package has been on-boarded by running security scans.

Effective O&M solutions strike a delicate balance between cost, performance, and functionality/security. Techniques to meet this objective include centralized monitoring, fault root cause analysis, performance data analysis, automatic O&M controls, etc.

Basic 5G network performance assurance capabilities require network/user behavioral visualization, fault demarcation/isolation, and self-diagnosis capabilities. NSP provides service assurance to key performance indicators and visibility to their customers. For example, customers can clearly know the details on both security and service assurances that the slice provides. Detailed logs on performance, faults, and security events could be provided to authorized customer personnel or machines. Based on measurements, the service assurance platform (e.g., using Artificial Intelligence/Machine Learning (AI/ML)) can tailor the service and security assurances to match the SLR.

Orchestration of Network Slices

Policy Considerations

Each network slice operates on a specific tracking area associated with a collection of logical 5G radio nodes (gNBs) and the associated set of Access and Mobility Management functions. Emblematic transport data plane technologies include IP, VPN, and Virtual Local Area Network (VLAN). It is paramount that the collection of 5G technologies comply with organization security policy. Additionally, E2E QoS requirements need to be supported within the slices designated deployment area; in practice, the E2E QoS uniquely define the combination of the QoS in the RAN and the QoS in the 5G Core for a given network slice use case.

Workflow Considerations

Complex workflows might be required to handle a network slicing request. One example is the provisioning of transport specific resources. Provisioning can involve intelligent and dynamic tuning of QoS, and intelligent admission control to determine available resources. Resources involved might belong to the RAN, the 5G Core, or both.

Maintenance of Network Slices

Maintenance of a network slice includes assuring that all SLRs are met. Service assurance includes resource management and making sure SLRs and policies (internal or intra-operator) are met. Once a network slice has been created and configured to meet certain SLRs, it needs to be monitored and maintained over time as threats continue to evolve.

Monitoring

It is expected that network monitoring covers all SLRs specified by associated network slice service profiles, including the operational state of each hardware and software component of a network slice. Monitoring the usage of a network slice is not limited to fraud detection, revenue assurance, or device behavior analysis for obvious network impacts, e.g., DoS signaling storm or user traffic saturation. Monitoring can be used by the system to protect itself from an attacker that may gain

access directly to that system.

It is important to identify where the security monitoring interfaces are within the 5G ecosystem. This is especially important in multi-vendor implementations where functionality from different sources might be deployed.

Table 7 describes recommendations for typical types of mobile network monitoring activities. For example, in NIST 5G Cybersecurity, it highlights the value of having good visibility across the 5G infrastructure; consequently, there is a need to continuously monitor communications patterns, see threats within the extended network, and detect and respond to threats using methods such as behavioral modeling, supervised machine learning, and unsupervised machine learning.[34]

The reference materials in Table 7 contain various attributes needed to maintain consistency and reliability of each network slice. Implementations provide timely and efficient access that information.

Table 7:
Examples of Network Monitoring Activities for 5G Networks

Types of Network Monitoring	Explanation
Performance Management	Due to the complex nature of mobile networks and vendors diversity of hosting platforms, a unique overarching performance management technique across different networks and vendors is required
Quality of Service	5G QoS include network performance metrics (e.g., latency, throughput, etc.) but might also include availability, reliability, accessibility, retainability, etc.
NIST 5G Cybersecurity	NIST SP1800-33B provides examples of 5G standard features and third-party security controls for successful 5G implementations.
Control Plane Communication	Control plane communication is not only protected for privacy but also protected against attacker's malicious modifications, performance issues, and anomalous behaviors.
User-Plane Communication	This is the communication which connects the actual data coming over the RAN to the Internet which is helpful to detect acceptable use violations e.g., a DDoS attack, DNS tunneling, spoofing, etc.
Anomaly Detection	Anomaly detection is a capability of identifying unusual activities or behaviors in networks. A variety of sensors, filtering and advanced (e.g., AI/ML-based) security analytics are necessary to detect sophisticated and zero-day threats.

To conduct O&M activities successfully, the service requirements as defined by a network slice profile need to be monitored. As noted in the Figure 10 above, monitoring a network slice can either be functional monitoring and/or security monitoring.

Typically, functional monitoring is already provided by the equipment CORE, RAN, and that element manager assuming the network is operating in a healthy state. It is paramount that security monitoring is built with zero-trust tenets in mind. Hence, monitoring solutions from the previous generations need to be integrated or updated to include 5G specific features. Otherwise,

carriers will have to build a standalone separate monitoring capability to support 5G O&M.

In the federated roaming scenarios, where slices are traversed into another carrier network, SLA needs to be established before deployment; a common methodology of monitoring and security mitigation schemes needs to be present at the gateways or logical borders between carriers.

Monitoring incorporates the collected data from various sources in the 5G networks. The acquired data will be analyzed first to see what insights and conclusions may be drawn. The analysis is followed by alerting, visualizing, and reporting. These steps are discussed in the following clauses.

Alerting

Alert capability is an important management tool. It is recommended that any alerting program support the ability to subscribe to user specified asynchronous alert messages. Alerts can notify a cyber protection team (CPT) or network operators of unusual activities and possible cyber events.

Alerts can be used in conjunction with Security Incident Event Management (SIEM) for correlating cyber events. For example, periodic UE and network scanning can identify anomalous behavior that shows malicious code has compromised certain 5G network element. For example, this may trigger an alert to the security orchestration, automation, and response (SOAR) platform, which instructs the network monitoring system (NMS) to disconnect the UE and prevent it from registering to the network until the malicious code has been removed from the UE.

In this simple example, SIEM supports threat detection, compliance, and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources[30]. A SIEM cannot address alerts by themselves, and will not mitigate any threats directly; however, having them allows CPT and operators to respond quickly and efficiently. Together, they provide CPT and cyber operations near-real-time benefits, deep insights over time-based data analysis, and underlying support for cybersecurity visualizations and dashboards.

Reporting

Reporting functionality includes providing status of updates, metrics that can be used to assure that an installation is correct, and metrics that can be used to detect potential issues. The reporting can include a summary of network slice health status and overview.

Reporting and storage of past historical data are both important in O&M; they provide troubleshooters the ability to review and later analyze a problem. For example, cyber forensics and anomaly detection, at both the network level and user behavioral level, rely on past reports and historical data. Summary reports can be periodically generated for management, but these would be different than reports required by maintenance personnel, as reports for maintenance personnel need to be comprehensive to encompass all relevant technical details and be in a readable format.

[30] https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Conclusion

5G SA network slicing is poised to become a key technology feature within 5G, so it is imperative we understand potential security threats to 5G network slicing. Hence, it is important to recognize industry-recognized best-practices of how 5G network slicing can be implemented, designed, deployed, operated, maintained, potentially hardened, and mitigated as they affect QoS and confidentiality, integrity, and availability triad SLAs. The goal is to promote collaboration amongst MNOs, hardware manufacturers, software developers, other non-MNOs, systems integrators, and network slice customers, in order to facilitate increased resiliency and security hardening within 5G network slicing.

APPENDIX: Abbreviated Terms

Acronym	Meaning
3GPP	Third Generation Partnership Project
5G	Fifth Generation Cellular Network
5G-AKA	5G Authentication and Key Agreement
5GC	5G Core Network
5GS	5G System
5G SA	5G Standalone Cellular Network
5QI	5G QoS Identifier
AAA	Authentication, Authorization, and Accounting [Server]
ABAC	Attribute-based Access Controls
AF	Application Function
AI/ML	Artificial Intelligence/Machine Learning
AMF	Access Management Function
API	Application Programming Interface
APN	Access Point Name
APRF	Authentication Credential Repository Processing Function
CIA	Confidentiality, Integrity, and Availability
CIR	Container Image Registry
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Container Infrastructure Service Management
CP	Control Plane
CRUD	Create, Read, Update and Delete
CPT	Cyber Protection Team
CSMF	Communication Service Management Function
CU	Central Unit
CUPS	Control and User Plane Function Separation
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DN	Data Network
DNN	Data Network Name
DNS	Domain Name Service
DoS	Denial of Service
DU	Distributed Unit
E2E	End-to-End
EAP	Extensible Authentication Protocol
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ESF	Enduring Security Framework
EAP-AKA’	Extensible Authentication Protocol Authentication and Key Agreement Prime
GSMA	GSM Association
HPLMN	Home Public Land Mobile Network
IaC	Infrastructure as Code
IAM	Identity & Access Management
IETF	Internet Engineering Task Force
IoT	Internet of Things

Acronym	Meaning
IPsec	Internet Protocol Security
IPX	IP Packet eXchange
MANO	Management and Network Orchestration
MDM	Mobile Device Management
MEF	(Formally known as the) Metro Ethernet Forum
MIMO	Multiple-input/Multiple-output
MITM	Man in The Middle
NEST	Network Slice Template
NAS	Non-access Stratum
RBAC	Role-based Access Control
NF	Network Function
NFV	Network Function Virtualization
NFVO	Network Functions Virtualization Orchestrator
NIST	National Institute of Standards and Technology (US DOC)
non-RT RIC	Non-Real-Time RAN Intelligence Controller
NRF	Network Resource Function
NSACF	Network Slice Admission Control Function
NSP	Network Slice Provider
NSSAAF	Network Slice-Specific Authentication and Authorization Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSMF	Network Slice Subnet Management Function
O&M	Operations and Maintenance
OAuth	Open Authorization
ONAP	Open Network Automation Platform
OSS-BSS	Operations Support System- Business Support System
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PLMN	Public Land Mobile Networks
PLMP	Public Mobile Network
PNF	Physical Network Function
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RBAC	Role-based Access Control
RSD	Route Selection Descriptor
RU	Radio Unit
SBI	Service-Based Interface
SDN-C	Software Defined Network Controller
SDO	Standards Development Organization
SEPP	Security Edge Protection Proxy
SIEM	Security Incident Event Management
SLR	Service Level Requirement
SMF	Session Management Function
SMO	Service Management and Orchestration [Framework]
SOAR	Security Orchestration Automation and Response

Acronym	Meaning
TD	Traffic Descriptor
TLS	Transport Layer Security
TN	Transport Network
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UICC	Universal Integrated Circuit Card
UP	User Plane
UPF	User Plane Function
URSP	User Equipment Route Selection Policy
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VNFD	VNF Descriptor
VNFM	Virtual Network Function Manager
VPN	Virtual Private Network
ZTA	Zero Trust Architecture