December 2022

Communications Security, Reliability, and Interoperability Council VIII

REPORT ON HOW VIRTUALIZATION TECHNOLOGIES CAN BE USED TO PROMOTE 5G SECURITY AND RELIABILITY

Drafted by
Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks

Table of Contents

1 Executive Summary

The world's mobile networks have begun a multiyear transition to 5G that will see one third of all mobile connections on 5G by 2025. This transition will allow operators over the coming decade to migrate their network operations from proprietary systems, to virtualized/cloudified environment, and transform their businesses.

Virtualization is a well-established and understood practice across the span of small through medium and planet scale enterprise IT environments. In general, the trend for decades has been for what was rendered in hardware (e.g., specialized appliances) to be subsumed by software-based implementations that can be easily distributed and adapted to execute in many different environments.

The advantages conceived in these enterprise IT topologies have permeated the network service provider segment with 5G's Service Based Architecture being deployed in virtualized environments. This confluence between wireless networking and computing technologies continues to evolve in fundamental ways, legacy networks largely existed as a distinct entity embodied in purpose-built hardware platforms and its primary function was to interconnect the general-purpose computers which executed applications.

Virtualization, along with cloud scale and geographic dispersion of computing resources now enable networking functions to be defined in software and rendered in general purpose computing platforms. Increasingly the cloud embodies all facets of the network except for the physical layer (e.g., modulating wireless wave forms, illuminating fiber, etc.) and 5G is, by definition, "cloud native"[1] meaning the service leverages the approach of building applications and services for the cloud.

This confluence of practices, standards and interests across multiple industries requires the adequate policy intervention to ensure a predictable, secure, diverse, and vibrant ecosystem whilst maximizing the trust and security of the network. Achieving this outcome requires both funding and non-funding approaches with intra governmental partnering requirements as well as liaisons with international governmental partners and the public sector. Further it is recommended that adequate industry support be provided to create and sustain a leading local talent pipeline which emphasizes Radio / RF and the crossover capabilities between the IT and Telecom domains.

Summary of Key Findings and Recommendations:

Intra governmental partnering: For the supply chain, consider ways to partner across the federal government to continue to incentivize digital solutions in 5G network deployments to mitigate supply chain risk. Also, to monitor and collaborate with other government agencies

[1] In this document, the term "cloud native" is based on the CNCF® definition, "Cloud-native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach."

who have similar concerns and are undertaking proactive actions or developing tools relevant to the secure and successful application of virtualization and related technologies including Zero Trust.

Public and private sector partnering: Convene a virtualized 5G industry information sharing group comprised of experts from government, research, academia, service providers, and equipment providers. This syndicated development of common patterns and playbooks of migration could be convened and incented including driving standards development or product capabilities.

Overcoming obstacles and increasing vendor diversity: To overcome obstacles and increase 5G vendor diversity for virtualized systems the ecosystem should embrace voluntary certification practices for virtualized network functions. It is also recommended that specific incentives be provided for rural carriers to improve security.

To address best practices for reliability and interoperability by enabling the 5G ecosystem to be open and create interworking between small and large vendors in the same 5G system, it is recommended that both the FCC and NIST (including other U.S government agencies as necessary) develop consistent and co-branded guidance.

Skilling needed to support virtualized 5G networks: Build the Workforce for Cloud based 5G networks which will bring more diversity and innovation to the 5G and next generation wireless networks. Specifically, provide support in building and sustaining a leading talent pipeline which emphasizes Radio / RF and the crossover capabilities between the IT and Telecom domains

2 Introduction

This report documents the cross industry expert collaboration to inform CSRIC VIIII on Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks.
To address this broad and complex topic in a useful way, the report is aligned around the following pillars:

Chapter 3	Scope and premise for leveraging virtualization technology to promote secure, reliable 5G networks.
Chapter 4	The broad concept of virtualization as a practice.
Chapter 5	How virtualization is impacting 5G and its embrace by the network provider ecosystem.
Chapter 6	View on security and operating integrity when virtualizing a 5G network.
Chapter 7	Complexities introduced by the confluence of multiple industries, and standards practices.
Chapter 8	Recommendations abstracted from deep technical insight to inform at a policy creation level.

2.1 CSRIC Structure

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

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII					
CSRIC VIII Working Groups					
Working Group 1: 5G Signaling Protocols Security	Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment	Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks	Working Group 4: 911 Service Over Wi-Fi	Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure	Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts
Co-chairs: Brian Daly, AT&T & Travis Russell, Oracle	Co-chairs: Mike Barnes, Mavenir & George Woodward, RWA	Co-chairs: Micaela Giuhat, Microsoft & John Roese, Dell	Co-chairs: Mary Boyd, Intrado & Mark Reddish, APCO	Co-chairs: Todd Gibson, T-Mobile and Padma Sudarsan, VMware	Co-chairs: Farrokh Khatibi, Qualcomm & Francisco Sanchez, SBA
FCC Liaison: Ahmed Lahjouji	FCC Liaison: Zenji Nakazawa	FCC Liaison: Jeff Goldthorp	FCC Liaison: Rasoul Safavian	FCC Liaison: Saswat Misra	FCC Liaisons: James Wiley Tara Shostek

Table 2-1 - Working Group Structure

2.2 Working Group 3 Team Members

Working Group 3 consists of the members listed below.

Name	Company
Marla Dowell	NIST
Andrew Drozd	ANDRO Computational Solutions, LLC
Bob Everson	Cisco
Michael Gallagher	Verizon
Micaela Giuhat	Microsoft Corporation
Martin Goldberg	National Security Agency (NSA)
Jeff Goldthorp	FCC
Javed Khan	Altiostar Networks
Douglas Knisely	Qualcomm Incorporated
Jennifer Manner	Hughes Communications
Serge Manning	T-Mobile USA
Timothy May	NTIA

Martin McGrath	Nokia
William Mikucki	Comtech Telecommunications Corp.
Keith O'Brien	Palo Alto Networks
Jitendra Patel	AT&T
Leo Popokh	ATIS
John Roese	Dell Technologies
Tom Sawanobori	CTIA
Scott Poretsky	Ericsson
Jane Shen	Mavenir
Paul Steinberg	Motorola Solutions
Frank Suraci	Cybersecurity and Infrastructure Security Agency (CISA ECD)
Peter Tomczak	FirstNet
Claire Vishik	Intel Corporation
Damien Whaley	Cox Communications
George Woodward	Rural Wireless Association

Table 2-2 - List of Working Group Members

Alternates for members are listed below.

Name	Company
Reza Arefi	Intel Corporation
Kevin Green	FirstNet
Bryan Larish	Verizon
Doug Montgomery	NIST
Vishwamitra Nandlall	Dell Technologies
Stere Preda	Ericsson
Rowland Shaw	Dell Technologies
Matthew Sneed	EchoStar
Darrell Stogner	Motorola Solutions
Ryan Stokes	Rural Wireless Association
Megan Stapleton	Comtech Telecommunications Corp.
Richard Tenney	Cybersecurity and Infrastructure Security Agency (CISA ECD)
Afeite Dadja	CTIA
Timothy Woods	ANDRO Computational Solutions, LLC

Table 2-3 - List of Working Group Alternates

2.3 Subject Matter Expert Contributors

Name	Company
Dr. Jithin Jagannath and Dr. Keyvan Ramezanpour	ANDRO Computational Solutions, LLC
Sundeep Rangan, Garg Siddarth, Elza Erkip, Christina Poepper	NYU Wireless
Dr. Ian Levy	National Cybersecurity in NCSC (National Cyber Security Center) in UK
Dr. Suku Nair	SMU AT&T Center for Virtualization
Nagendra Bykampadi	Rakuten
John Morello	Palo Alto
Scott Poretsky	Ericsson
Leo Popokh	HPE

Table 2-4 - List of Subject Matter Experts

3 Objective, Scope, and Methodology

3.1 Objective

The Chairwoman of the FCC directs CSRIC VIII to develop recommendations on how virtualization technology can be used to promote the availability of secure, reliable 5G technologies and services solutions from a diverse market of 5G equipment vendors.
Most 5G network product sets are vertically integrated and proprietary - factors that contribute to important communications supply chain risks.
CSRIC VIII will develop recommendations for how vendor-agnostic, horizontal stack solutions for 5G can be promoted to foster a diverse, competitive, and more secure 5G environment despite the wider attack surface presented. These recommendations should address ways to provide opportunities for smaller vendors that cannot yet manufacture all parts of a vertically integrated, traditional 5G stack.

3.2 Scope

The objective is to be addressed in two reports and should be read in conjunction with CSRIC VIII WG2.

This first report on How Virtualization Technologies can be Used to Promote 5G Security and Reliability, for CSRIC VIII will include recommendations on:

- Ways in which funding and non-funding methods can be deployed to promote virtualized environments that result in improved 5G security and reliability.
- Recommendations on ways to promote and overcome obstacles and increase 5G vendor diversity for virtualized systems including Distributed Unit (DU), Central Unit (CU), Radio Unit (RU) and Service Based Architecture (SBA).
- Best practices for reliability and interoperability by enabling the 5G ecosystem to be open and create interworking between small and large vendors in the same 5G system. These recommendations should also broadly focus on reducing the cost of entry for 5G and making it more accessible to smaller adopters of the technology.
- CSRIC VIII will also identify whether any additional work is needed from a broad landscape of IT, Cloud and Telecom standards and initiatives that virtualized 5G is dependent on.

The second report on Recommendations on the Role of the FCC in Promoting the Availability of Standards for More Secure, Reliable 5G Environment Through the Use of Virtualization Technology, for CSRIC VIII will include recommendations on:

- Steps that the FCC should take (if any) to help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space
- Recommendations on how the FCC can promote 5G collaborations and innovation labs
- Recommendations on actions the FCC can take to build confidence in virtualized 5G solutions using open-source cloud computing software

- Any other ways in which FCC can promote a diverse, competitive 5G environment.

3.3 Methodology

CSRIC VIII WG3 is comprised of numerous industry experts across the domains of Telecom, Wireless, IT, and Security from both the demand and supply sides. For the purposes of this CSRIC VIII report, the deep technical insight and knowledge of the team was elevated to provide policy level insight.

Specifically, the team:

- Reviewed industry lessons learned from use of virtualization and increased vendor diversity in strengthening security, increasing competition, and creating a more secure supply chain.

- Gathered insights and input from researchers, technologists, thought leaders and standards development organizations on availability of solutions, and technical issues to be addressed.

- Performed an assessment of implementation best practices and reviewed results from test labs or real-life deployments around the world.

- Performed comparison between virtualized and non-virtualized security vulnerabilities in a 5G network.

- Identified issues to be addressed by the commission and provided high level recommendations on how best to support a secure diverse vendor ecosystem.

4 Virtualization: Definition, Benefits, and Concerns

As new hardware and software technologies emerge, an increasing number of use cases emerge. Infrastructure and software, from hardware to operating systems to applications, now require increased number of transactions, minimal latency, compute, and memory power. Virtualization makes digital transformation to support the emerging use cases possible by enabling a single compute environment to act like multiple. Virtualization makes a single physical computer to act like multiple different virtual versions of itself.

4.1 What is Virtualization?

The virtualization idea and technology dates to the 1960s. But it was not generally accepted until the early 2000s. Hypervisors, platforms supporting Virtualization, were developed decades ago to give multiple users and processes simultaneous access to computers. In the 1990s, Enterprises and Service Providers had physical servers and mostly single-vendor IT stacks in their

datacenters. In late 1990s, IT environments transitioned to less-expensive commodity servers, operating systems, and applications from a variety of vendors. The common practice was to utilize each server dedicated to run one vendor-specific task and hence were under-utilized (usually running less than 50% capacity).
This was the main stimulus for modern day Virtualization.
Virtualization addressed two problems:

- Partitioning datacenters' servers.
- Run legacy applications on multiple operating system types and versions.

Physical servers became more efficient. Virtualization allowed users to reduce vendor or provider lock-in and made the foundation of cloud computing.

Virtualization technology accelerated in the early 2000s when IT companies decided to shift from underutilized and mostly dormant physical servers in their datacenters to virtualize them for greater performance and efficiency. As a result, virtualization grew into an industry-wide standard practice, while bringing in many more advantages.
Virtualization is the process of using software to create and run a virtual version of a computer system by abstracting from physical hardware. Virtualization enables creation of a virtual version of IT services like storage, memory, server, operating system, or network resources, and running them on single, physical hardware simultaneously and secure. Virtualization simulates hardware functionality to create a virtual environment known as a Virtual Machine (VM). Each VM behaves like an independent computer. Multiple VMs can run on the single physical computer.

4.2 Why Do We Need Virtualization?

Virtualization enables application isolation by keeping programs running inside a VM completely secured from other VMs on the same physical host. Virtualization makes it possible to run applications from a variety of different vendors designed for a different operating system without having to change or reboot the system. Virtualization allows for greater workload portability, high availability, enhanced scalability, and more efficient cost management.

4.3 How Does Virtualization Work?

Software called hypervisors separate and provide the abstraction layer from the physical resources to the virtual environments. Hypervisors can be installed within any operating system (personal laptops) or installed directly onto bare-metal hardware (like a server). Hypervisors (Figure 4-1) take physical resources and provide them to the virtual environments to consume by clients at the Application Layer.

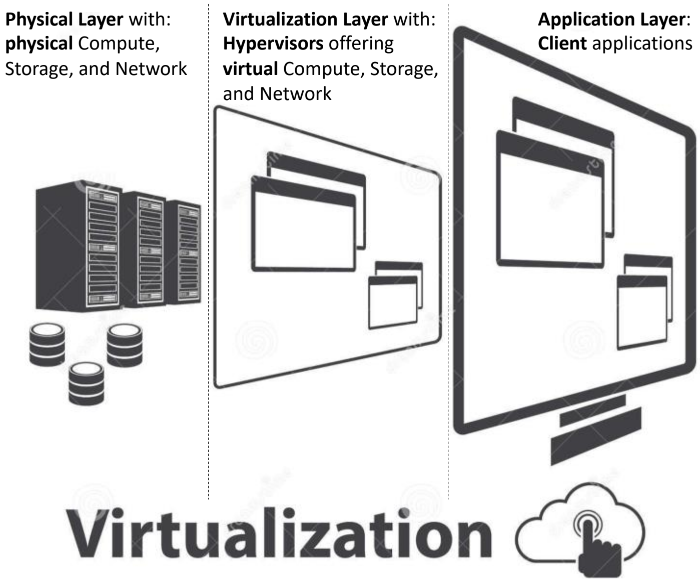

Physical Layer with:
physical Compute, Storage, and Network
Virtualization Layer with:
Hypervisors offering **virtual** Compute, Storage, and Network
Application Layer:
Client applications
Virtualization

Figure 4-1 - Hypervisors and abstraction from hardware

Virtualized Infrastructure Management (VIM) is a cloud-like operating system (**Error! Reference source not found.**) that controls large pools of compute, storage, and networking resources. Virtual compute, storage, and networking resources are managed and provisioned through APIs with common authentication mechanisms.

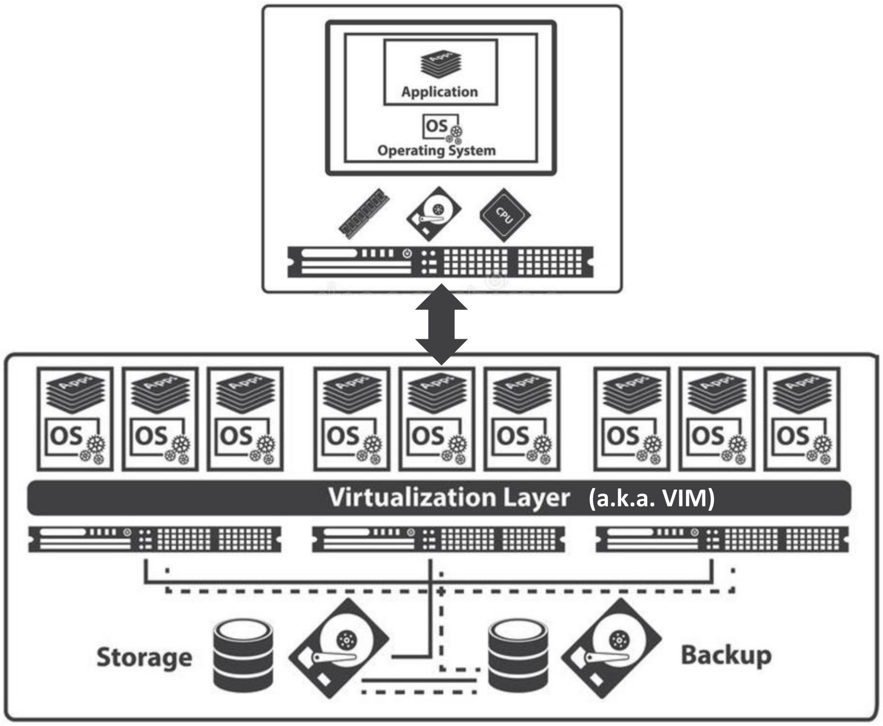


Figure 4-2 – Virtualized Infrastructure Management (VIM)

Resources are partitioned and allocated as needed from the physical environment to many VMs. The VM functions as a single data file. And like any digital file, it can be moved from one computer to another and expected to work the same.

4.4 Different Types of Virtualizations

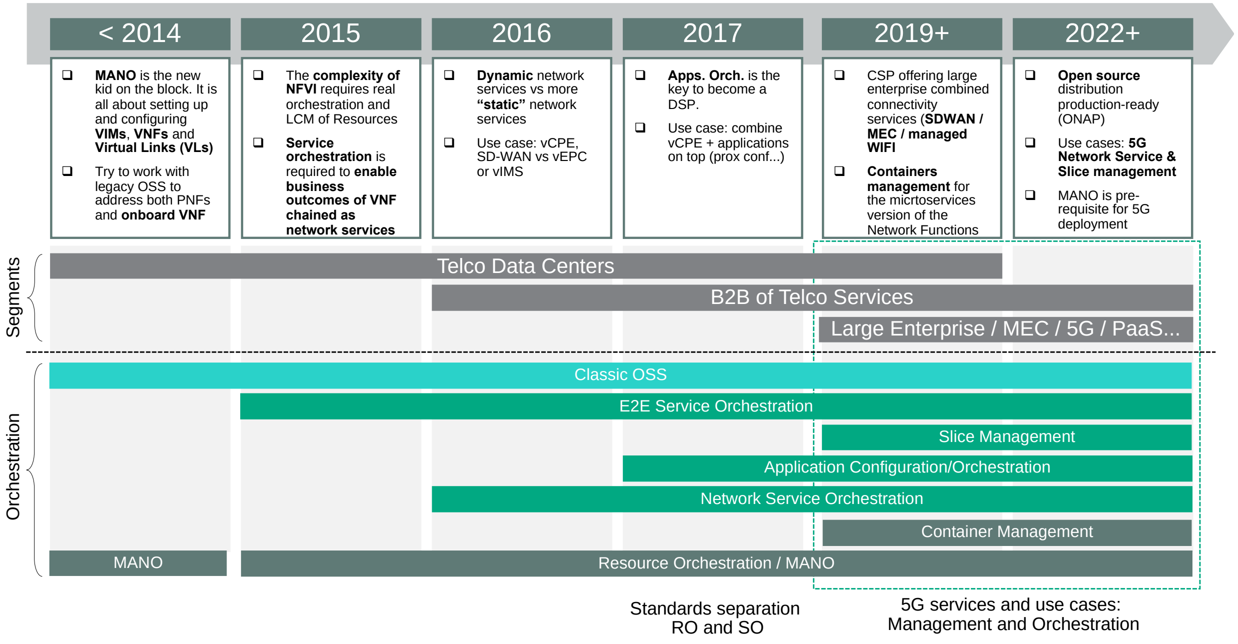
There are multiple types of virtualizations prevalent in the industry today:

Network Virtualization

Network virtualization is a critical component of Network Management. IT Administrators can modify and control abstracted hardware and software functions of a network using a single console. This includes two major types:

- Software-Defined Networking (SDN) is the rendering of network functions (routing, control plane, etc.) in software on general purpose computing environments vs. in specialized hardware (e.g., ASICs) and appliances. SDN doesn't necessarily require virtualization; however, it is a necessary precondition for virtualization and NFVs.
- Network Function Virtualization (NFV) is the replacement of dedicated network appliance hardware with virtual machines thus providing abstraction from the underlying forwarding and control hardware.

Significant evolution has occurred over the last decade as shown in Figure 4-3. In the early stages, NFV was focused on management automation and network orchestration (MANO) and virtual network function (VNF) instantiation to accelerate the use of general-purpose compute platforms, but the requirements for ease of operation and service orchestration were only partially addressed. Around 2016, enterprise user adoption of SDN branch services and SD-WAN took off and CSPs soon began to integrate those capabilities with existing value-added services. Over the next two years, the need for E2E connectivity with service and applications orchestration finally began to be addressed. In addition, enterprise customers were now demanding Continuous Integration/Continuous Delivery (CI/CD) and DevOps as part agile lifecycle management (LCM) support for service software delivery. To meet these requirements NFV evolved to deliver these capabilities across different Industry Segments and Orchestration Domains.



< 2014
❑ **MANO** is the new kid on the block. It is all about setting up and configuring **VIMs**, **VNFs** and **Virtual Links (VLs)**
❑ Try to work with legacy OSS to address both PNFs and **onboard VNF**

2015
❑ The **complexity of NFVI** requires real orchestration and LCM of Resources
❑ **Service orchestration** is required to **enable business outcomes of VNF chained as network services**

2016
❑ **Dynamic** network services vs more **"static"** network services
❑ Use case: vCPE, SD-WAN vs vEPC or vIMS

2017
❑ **Apps. Orch.** is the key to become a DSP.
❑ Use case: combine vCPE + applications on top (prox conf...)

2019+
❑ CSP offering large enterprise combined connectivity services (**SDWAN / MEC / managed WIFI**
❑ **Containers management** for the micrtoservices version of the Network Functions

2022+
❑ **Open source** distribution production-ready (ONAP)
❑ Use cases: **5G Network Service & Slice management**
❑ MANO is pre-requisite for 5G deployment

Segments
Telco Data Centers
B2B of Telco Services
Large Enterprise / MEC / 5G / PaaS...
Orchestration
Classic OSS
E2E Service Orchestration
Slice Management
Application Configuration/Orchestration
Network Service Orchestration
Container Management
MANO
Resource Orchestration / MANO
Standards separation
RO and SO
5G services and use cases:
Management and Orchestration

Figure 4-3 NFV Evolution

Desktop & Server Virtualization

Desktop virtualization allows multiple desktop operating systems to run on the same hardware. There are two types: Virtual Desktop Infrastructure (VDI) and Local Desktop Virtualization (LDV).
Servers are computers designed to process a high volume of specific tasks well so other computers (i.e., laptops, desktops) can do a variety of other tasks. Virtualizing a server allows one to do more specific functions and involves partitioning so that the components can be used to serve multiple functions.

Storage Virtualization

Storage virtualization is done to maximize and simplify storage provisioning for VMs. This process involves access and management of all the storage devices, both installed on servers or as standalone units, in a network as a single pool.

Data Virtualization

Consolidating various sources of data into a single source is called data virtualization, thus delivering the required data in the right form and at the right time to a certain user or application. Data virtualization helps in easier management of data for modern enterprises that have tons of data of various formats, kinds, and in different locations.

Application Virtualization

In application virtualization, a user can interface with the application without the need for installing it on the operating system. It is of three types: local application virtualization, application streaming, and server-based application virtualization.

Operating System Virtualization

Operating system virtualization happens at the kernel level. It is a useful way to run different operating systems environments, such as Linux and Windows, side-by-side on the same platform.

Data Center Virtualization

Data center virtualization is what makes the migration to the cloud possible for data centers. Using this process, data centers can virtualize their servers along with networking, storage, and other infrastructure, making it software-defined and highly automated.

Hardware Virtualization

The abstraction of physical computing resources from software that uses them is called hardware virtualization. This is achieved by embedding VM software in the server’s hardware components. Other common types of virtualizations include CPU virtualization, GPU virtualization, Linux virtualization, and cloud virtualization.

Virtualization & Security

Managing virtualization involves monitoring, administering, and maintaining virtual servers and guest VMs. Virtualized environments are complex and consist of 2 or more interconnected VMs, containers, private cloud, or public cloud environments. Virtualization security benefits come from the advancements in computing, networking and storage that enable securing virtual environments from the physical world. Virtualization enables the creation and isolation of a secure area in memory from the OS. For example, to store and protect sensitive information from malicious code. VMs can also roll back to a previously secured and stable state if infected with viruses and malware. Virtualization can also filter, and segment traffic prevent performance-related security threats.

Difference between Virtualization and Cloud Computing

Both virtualization and cloud computing are interconnected but have different terms referring to different processes. Virtualization is a process which involves the creation of virtual versions of physical hardware. Cloud computing is a process for users to connect to a single pool of virtualized resources on demand and through the internet. Virtualization is necessary to create resources that the end-user can access via cloud computing.

Difference between Virtual Network Functions (VNFs) and Containerized Network Functions (CNFs)

VNFs are stateful that can be reconfigured and upgraded throughout its lifecycle while providing hardware-level isolation to allow use of different operating systems. Security advantages CNFs have over VNFs include:

- CNFs provide immutability in which they are operated as stateless entities that cannot be changed, but instead must be replaced.
- CNFs use data stored outside of the container in persistent data storage so that data can be available for each deployed version.
- CNFs run on top of a shared Host operating system, providing operating system level isolation.
- CNFs and Host operating systems interact through a container runtime that manages:
    - APIs to enforce runtime policies
    - resource allocation so a CNF cannot interfere with the operation of another,
    - namespace isolation so that a CNF cannot view or have access to resources of another CNF.

While these inherent capabilities provide CNFs security advantages over VNFs, CNFs tradeoff some security disadvantages:

- CNFs provide less segmentation than VNFs because CNFs share the same kernel while running with varying privileges on a host.

- The portability of CNFs requires implementation of enhanced security controls to ensure the container is secure at runtime and the environment is secure from malicious or misbehaving CNFs.

Security controls needed to secure CNFs for 5G deployments can be grouped as follows[2]:

- Implement CI/CD and DevSecOps practices
- Secure Host OS and Hardware
- Secure 5G CNF run-time
- Secure 5G CNFs and traffic
- Secure 5G CNF orchestration and access controls
- Secure 5G CNFs in roaming scenarios

Additional security considerations need to be made when deploying CNFs for 5G critical infrastructure in hybrid and public clouds. The Enduring Security Framework (ESF), led by NSA with support from CISA, has published guidance for 5G cloud deployments[3]. It is recommended that further study of CNF security and secure deployment of critical infrastructure in hybrid and public cloud environments be considered for a future CSRIC WG and have it performed in collaboration with US DHS CISA.

5 Virtualization Benefits Applied to 5G

The publication by thirteen Tier 1 network operators of the whitepaper “Network Functions Virtualization – An Introduction, Benefits, Enablers, Challenges & Call for Action”[4] on October 22, 2012, was a watershed moment for the network equipment industry. The message from the network operators to their traditional network equipment providers was set out very clearly in this whitepaper. In essence, the network operators stated that they no longer wished to build their networks with proprietary appliances, but intended to rely instead on a generic, industry-standard hardware infrastructure with the network functions themselves being implemented entirely in software.

The traditional method of building networks and services with proprietary appliances has always been expensive, slow, and cumbersome. The combination of ubiquitous Internet access and the wide availability of large-scale cloud services have enabled software-based dotcom businesses to build IP-based communications services at huge scale and with very low cost – and in some cases these businesses have posed significant threats to telco revenues. It was only a matter of time before traditional network operators realized that they had to embrace a far more software-centric way of implementing networks and services. The concepts behind NFV reached a critical mass of acceptance among Tier 1 network operators in 2012 primarily due to the benefits NFV brings.

For NFV to make sense to network operators, it must be capable of supporting a useful

[2] Securing 5G and Evolving Architectures, Nair, Pramod, (ISBN: 9780137457939)
[3] Security Guidance for 5G Cloud Infrastructures, volumes 1 through 4, NSA ESF and CISA, Oct/Nov/Dec 2021.
[4] https://portal.etsi.org/nfv/nfv_white_paper.pdf

proportion of the network functions that are found in today's networks. NFV is all about applying IT technologies including virtualization, cloud, and data center hardware to the problem of building networks and network services.

Advances in cloud-based technology—both in the core and at the edge of the communications network—allow for the connection of billions of devices. The cloud can store vast volumes of data which can be accessed from anywhere broadband is available. These cloud characteristics enhance the operational efficiencies available to businesses across every industry. They also make the cloud an ideal technology to support the rise of the IIoT, particularly when combined with the modern wireless network, 5G.

5G's service-based architecture already defines how network functions (NF) can be deployed in virtualized environments.

5G is, by definition, "cloud native" meaning the service leverages the approach of building applications and services for the cloud. For instance, the networks can use cloud techniques including Open API, Control-User Plane Separation, Microservices, Continuous Integration and Delivery, and Virtualization[5].

The cloud currently provides a platform for operating critical infrastructure needs of many sectors across the global economy, including banking, energy, food and agriculture, healthcare, manufacturing, and government services. This is a domain which receives considerable ongoing industry and governmental attention including the Zero Trust framework.

Virtualization of 5G networks, and specifically of the Radio Access Network (RAN) is needed to enable operators to meet the growing demand 5G networks place on compute capacity, networking, and storage resources. With 3GPP release 15 that started 5G, 3GPP introduced the disaggregation of the Radio Access Network (RAN), splitting the 5G base station (gNB) between a distributed unit (DU) and central unit (CU).

Virtualization also helps decrease time-to-market. Virtualized implementation of Distributed Units (DUs) and Central Units (CUs) will provide further scaling and performance benefits and expected to lower costs for operators. 3GPP[6] defines a Distributed Unit as the logical node that manages the radio link, data link, and digital portions of the network, and controls coordinated multi-point and fronthaul capabilities among multiple Radio Units. Central Unit is the logical node that oversees the radio resource control and packet data convergence protocols of the network. The Central Unit controls one or multiple Distributed Units over mid-haul interface and facilitates network traffic load balancing among Radio Units. Virtualizing the RAN will also increase network vendor diversity by disaggregating network components. New vendors benefitting from a lower cost of entry to the network vendor ecosystem can play a role in developing individual network components, instead of only having the option of producing

[5] *5G and the Cloud*, 5G Americas, White Paper (Dec. 2019) p.39. https://www.5gamericas.org/5g-and-the-cloud/.

[6] 3rd Generation Partnership Project;Technical Specification Group Radio Access Network;NG-RAN;Architecture description (Release 16), https://www.3gpp.org/ftp/Specs/archive/38_series/38.401/38401-ga0.zip (Last accessed October 11, 2022)

proprietary bundles of products for operators.
The diverse vendor ecosystem enabled by a virtualized architecture paired with cloud will allow operators to choose the best-in-class vendors for each network function, avoid vendor lock-in, accelerate innovation coming from a vibrant vendor ecosystem.

There are three fundamentals that must converge to realize the benefits of the transformative effects that software defined networking can unlock.

Cloud Native Software: As with most cloud-based applications, the software that defines the network functions must be written with the cloud environment in mind. This doesn't simply include issues such as virtualization and multi-tenancy, but also must contemplate the software monitoring and lifecycle deployment models as well as the architectural considerations required to ensure security and resilience of the services. 5G is the first iteration of the 3GPP wireless standard that contemplates a fully cloud-native environment.

Distributed and Dynamic Systems: By its very nature, the network functions must be geographically distributed to optimize performance, localize computation and data movement, while minimizing latency. Networks must respond to dynamic changes in traffic profiles and capacity and must be able to do so almost instantaneously to avoid implications to the applications above.

Network Topology: The network topology must be mapped to the underlying computing resources to maximize resilience and security. Traditional cloud scale suggests that larger and more centralized data centers provide better economics; however, network functions must be distributed to optimize economics, meet networking SLAs (Service Level Agreements), and protect against all forms of faults and failure conditions. There are practical issues to consider such as who provides the various computing layers upon which the network topology executes (Hyperscale Cloud Providers (HCPs), Communication Service Providers (CSPs), etc.) and what are the business considerations and required SLAs for each. The next sections expand upon the opportunities and concerns incumbent in each of the above areas.

5.1 Cloud Native Software

Sofwarization[7] of 5G networks (i.e., converting them to be SDNs) is a key element in the migration of network functions from hardware-based elements to software-based architecture. Cloud-native architecture and technologies are an approach to designing, constructing, and operating workloads that are built in the cloud and take full advantage of the cloud computing model.

5.1.1 Software Delivery

Sofwarization of 5G networks is a key element in the migration of network functions from hardware-based elements to software-based architecture.

[7] "softwarization" – WordSense Online Dictionary (4th November, 2022), URL: https://www.wordsense.eu/softwarization/

Cloud-native architecture and technologies are an approach to designing, constructing, and operating workloads that are built in the cloud and take full advantage of the cloud computing model. One of the most important aspects of cloud native software delivery is continuous integration (CI) and continuous delivery (CD), commonly referred to as CI/CD, representing a set of processes that help software development teams deliver code changes more frequently and reliably. CI/CD is part of DevOps[8], which helps shorten the software development lifecycle. CI/CD allows software to be built, tested, and released more frequently and consistently. A properly constructed CI/CD environment enables an efficient 'mirror system' testing paradigm by allowing changes to be introduced and exposed to controlled traffic and carefully monitored (e.g., A/B testing[9], etc.) in a controlled and constrained environment before committing the changes to a full production environment.

DevOps is a compound of development (Dev) and operations (Ops), DevOps is the union of people, process, and technology to continually provide value to customers.
DevOps enables formerly siloed roles—development, IT operations, quality engineering, and security—to coordinate and collaborate to produce better, more reliable products
Due to the new way of delivering software, a cloud native software environment provides the following benefits:

- Agility
- Speed
- Resiliency
- Ease of use
- Scalability
- Efficiency

5.1.2 Securing the Software Delivery Practices

Leading security engineering practices, such as Secure Software Development Standards (SSDS), and operational security capabilities should be used to ensure secure delivery. This includes leveraging the Security Development Lifecycle (SDL) and other software assurance practices in alignment with the National Institute of Standards and Technology's (NIST) Secure Software Development Framework (SSDF)[6] and SAFECode's Fundamental Practices for Secure Software Development to further enhance software security with industry-leading techniques.

5.1.3 Using Software Bill of Materials

According to NIST and clearly outlined in the CSRIC VIII Report titled "Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure",[10] a Software Bill of Materials (SBOM) is a nested inventory for software, a list of ingredients that make up software components.

Why have a Software Bill of Materials?

[8] https://en.wikipedia.org/w/index.php?title=DevOps&oldid=1119119871
[9] A/B testing. (2022, October 20). In *Wikipedia*. https://en.wikipedia.org/wiki/A/B_testing
[10] CSRIC VIII Report on Recommended Best Practices to Improve Communications
Supply Chain Security (September 2022). https://www.fcc.gov/file/23839/download

A SBOM is useful to producers and consumers of software, as it provides software transparency, software integrity, and software identity benefits and summarized as follows:

- **Software transparency**: SBOMs provide a list of ingredients used in the creation of a piece of software, such as open-source software, components, and potentially even build tools. This enables producers and consumers to better inventory and evaluate license and vulnerability risk.
- **Software integrity:** While code signing is still the industry standard for trusting software and its integrity, SBOMs contain package and file checksums to enable consumers to validate the hashes, which can be useful in scenarios when signatures aren’t present.
- **Software identity**: When vulnerabilities (CVEs) are created, they are assigned to an Common Platform Enumeration[11] (CPE) identifier, which can have issues attributing a CPE to a specific piece of software. Software IDs within SBOMs provide a much more accurate way to identify software.

SBOM Considerations for 5G deployments:

- Most deployments at scale are expected to be mixed with legacy network elements. To achieve a completely cloud-native implementation of a RAN and Core network, it will be necessary to migrate, in place, a large multi-vendor and complex legacy installed base of traditional equipment and deployment paradigms that date back decades. Since the installed base represents a very large investment, with a long-life cycle, it will likely need to be amortized over time. Thus, there will be a lengthy period of co-existence and each service provider will have unique circumstances to contemplate. A detailed and cautious migration strategy is crucial for security integrity and service reliability. A syndicated development of common patterns of migration could be convened and incented by the FCC including driving some standards or product capabilities (analogous to the allowances that 5G non-standalone option affords).

- The paradigm shift from traditional telecommunications and networking architecture practices is substantial and will require a considerable new base of expertise. The UK National Cyber Security Center (NCSC) undertook a ground-up analysis of the UK’s telecommunications infrastructure and summarized those findings in a report. The NCSC concluded that the UK’s telecommunications sector is vulnerable to a range of cybersecurity and supply chain risks. They concluded that virtualization coupled with other contemporary IT practices could help alleviate these vulnerabilities. The NCSC also recognized that adoption of this implies a fundamental shift in design and deployment of telecommunications services, so they developed a set of Telecom Security Requirements (TSRs) and playbooks to help guide the industry. They coupled the TSRs and playbooks, which are not openly published, with some regulatory changes to encourage adoption. It was the opinion (verbalized) of NCSC experts that enterprise cloud computing offers a better (more

[11] https://nvd.nist.gov/products/cpe

modern, adaptable, and agile) framework upon which telecommunications services could be built in the future.

5.2 Distributed and Dynamic Systems

Cloud platforms at scale are intrinsically highly resilient to failures. Cloud service providers construct their facilities across geographically redundant data centers (regions) and take great pains to minimize correlated faults between within and across regions (availability zones). Failures and state replication across regions and availability zones are not transparent to applications but the services can be constructed to minimize service disruptions across failures. Network functions can also be designed with multi-cloud in mind, in theory allowing for redundancy across different cloud platforms to further decouple some (typically design or operator level) failure modes.

Increased automation is a key objective and increasingly a necessity of future network deployments. Automation will enable networks to be monitored, managed, and predictively assessed for service level deviations through algorithms that operate increasingly in real-time. Moving network operational functions into open software along with standardized interfaces that can be deployed in a virtualized environment facilitates the creation of an ecosystem of solution providers for automation functions (analogous to applications in an app store).

Cloud architecture enables a uniform experience regardless of where the workload is deployed, whether far-edge, near-edge, or region. It also extends the cloud services to the edge.

Edge computing, which is needed for massive scale 5G deployments, is another important component of next generation wireless networks. Edge computing is the movement of computing closer to where applications and services operate. Moving computing closer to the user of the application supports applications that are highly time sensitive and require very low latency.

As more aspects of the RAN become virtual, the edge has become divided into “near edge” and “far edge” elements. Near edge elements include those parts of a RAN that are located closest to an operator’s facilities or cloud data center. Far edge elements sit closer to end users yet remain controlled by the operator. For example, a disaggregated and virtualized RAN enables operators to distribute Open RAN functions across cell sites, near and far edge, and the central or regional cloud. Centralizing some aspects of RAN functionality increases efficiency and lowers costs. Operators can leverage energy- efficient algorithms of cloud platforms and improve failover scenarios across servers. Because the RAN functions are disaggregated, for example into the DU and the CU, this centralization can be achieved for less-latency sensitive applications while still maintaining the most latency sensitive functions at the far edge. Real world deployments will have varying architectures based on their practical needs; distributed open and virtualized RAN gives operators the flexibility to optimize networks depending on the unique needs of a particular deployment.

Edge computing has the potential to improve performance, scalability, reliability, and regulatory compliance options for many critical applications. It offers the promise of near real-time insights, faster localized actions, and cost reduction because of efficient data management and operations. A major benefit of edge computing is that it improves time to action and reduces response time down to milliseconds while also conserving network resources. It reduces latency

–the most widely cited reason for placing computation capabilities at the edge –and network bottlenecks because data does not have to traverse over a network to a mega data center for processing.

Edge computing also supports interoperability or mediation by converting the communication protocols used by legacy devices into a format that contemporary smart devices and the cloud can leverage. Edge computing may help address the security and compliance requirements that have prevented some industries from using the cloud.

More intelligence can be added at the edge to secure systems, making them more resilient to hacks and intrusions. At present the third-party ecosystem is nascent with multi-tenancy/shared infrastructure for edge computing advancing rapidly. This progression is expected to remove a barrier for users who want to take advantage of the benefits of the public cloud along with the low latency of edge computing. Multi-tenancy promises to enable multiple applications and services to work on the same edge device (see more on multi-tenancy in Chapter 5.3.1)

5.3 Network Topology

This section will cover the benefits of 5G having a different network topology compared to previous generations through virtualization technology, such as multi-tenancy, isolation, and resiliency. Virtualization of the network functions allows them to be in different parts of the network, a capability that was not possible before, and create efficiencies for applications that require low latency, taking in considerations elements such as cost, data overhead and delays. Papers such as “Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges”, by Massimo Condoluci and, Toktam Mahmoodi provide different views of the benefits of placement of functions such as Serving Gateway (SGW) and the PDN Gateway (PGW), argue that the advantages and disadvantages of function placement into the central cloud can be summarized as follows:

- In terms of costs, placing functions in the cloud would introduce a significant cost reduction.
- In terms of data overhead, signaling functions in the cloud would not significantly impact performance, placing other functions in the cloud could drastically increase the data overhead.
- In terms of end-to-end delay, signaling, resource management logic and filtering in the cloud would not significantly impact performance, while placing into the cloud both charging and GPRS Tunnelling Protocol (GTP) would result in significant latency increases.

5.3.1 Multi Tenancy

Another important benefit of virtualization is multi-tenancy, which basically means the ability to share computing resources. Multi-tenancy can be achieved on multiple levels, from everything shared to customized by tenant. This approach allows different security level implementations. A multi-tenant system is scalable to an arbitrarily large number of customers, because the number of servers and instances on the back end can be increased or decreased as necessary to match demand, without requiring additional re-architecting of the application, and changes or fixes can be rolled out to thousands of tenants as easily as a single tenant.

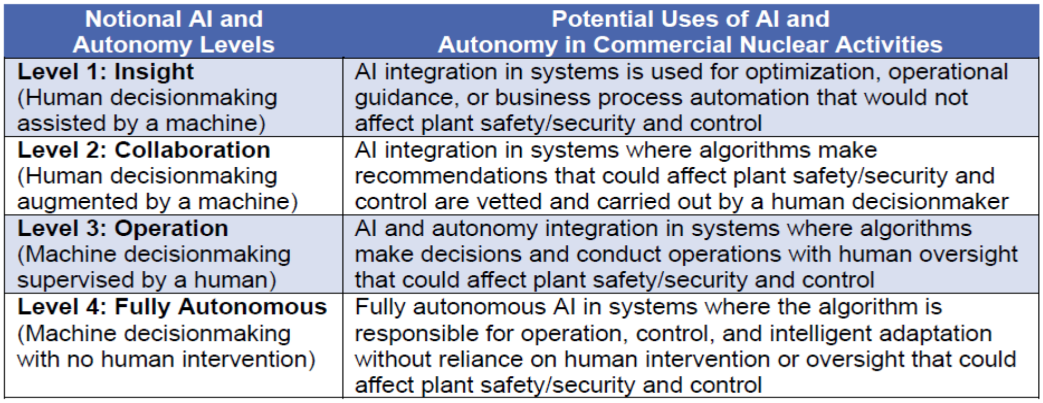
5.3.2 Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning models rely on cloud for heavy lifting. Typically, a machine learning model is trained in the public cloud and deployed in the edge for near real-time predictions. Edge computing has become an essential component of data-driven applications. Virtualization and all the benefits that cloud-based computing offers Artificial Intelligence and Machine Learning (AI/ML) capabilities at scale. This affords access to powerful new capabilities that can be broadly, efficiently, and flexibly applied across the network architecture. AI will undoubtedly be increasingly applied to optimize, operate, and protect network services as the (software defined and virtualized) networking environment because:

- The network is more complex to understand, operate and optimize due to dynamic adaptations along with an ever-increasing number of operational indicators and "knobs".
- The CSP's environment is comprised of multi-party services from an ecosystem of providers with inter-dependencies that must be orchestrated and coordinated.
- The network and computing topologies are increasingly distributed.
- Anomaly detection, as a leading indicator of other events or due to malicious activity, can be conducted with high fidelity.
- The cybersecurity attack surface is broader and has different facets. Over time, the ability to optimally navigate these issues will become a differentiator among function providers and end service providers to optimize costs, tailor user experiences, and mine intelligence from their operations. As such they will increasingly turn to machine algorithms and AI vs. Human beings to engage in these issues. As noted, the trends increasingly lend themselves to the applications of AI operationally.

The use of AI brings intrinsic risks and concerns since it is such a new technology. Literature is filled with research around how to produce, assess, and verify trustworthy AI applications (meaning that they predictably and understandably do what they are expected to do in the face of all environmental circumstances in which they operate). The risks and considerations are a function of the responsibility that is entrusted to AI. For example, the US NRC[12] categorized the levels of AI involvement in the following table with ever increasing risk involved as one steps up through the layers.

[12] Artificial Intelligence Strategic Plan Fiscal Years 2023-2027 – Draft Report for Comment, US Nuclear Regulatory Commission, June, 2022.



Notional AI and Autonomy Levels	Potential Uses of AI and Autonomy in Commercial Nuclear Activities
Level 1: Insight (Human decisionmaking assisted by a machine)	AI integration in systems is used for optimization, operational guidance, or business process automation that would not affect plant safety/security and control
Level 2: Collaboration (Human decisionmaking augmented by a machine)	AI integration in systems where algorithms make recommendations that could affect plant safety/security and control are vetted and carried out by a human decisionmaker
Level 3: Operation (Machine decisionmaking supervised by a human)	AI and autonomy integration in systems where algorithms make decisions and conduct operations with human oversight that could affect plant safety/security and control
Level 4: Fully Autonomous (Machine decisionmaking with no human intervention)	Fully autonomous AI in systems where the algorithm is responsible for operation, control, and intelligent adaptation without reliance on human intervention or oversight that could affect plant safety/security and control

Another factor in the integrity of algorithms is whether they are pre-trained in a controlled environment, tested and then deployed or if they are allowed to train and adapt in an operational environment (which obviously increases the risk of unexpected outcomes).

The FCC has commissioned a study group in its Technological Advisory Council[13] to assess various implications of AI and ML[14]. Rather than assessing the implications of AI/ML in this context, it may make sense to create a liaison or linkage between these two initiatives (e.g., leverage the TAC to collaboratively analyze the implications).

5.3.3 Isolation

In a multi tenancy architecture, there is a need to provide logical isolation to segregate each customer's applications and data. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent customers from accessing one another's data or applications. There are different levels of isolation, as described below.

Compute isolation

There are two categories of compute isolation which are logical and physical isolation for processing.

Logical isolation can be implemented via:

- **Hypervisor isolation** for services that provide cryptographically certain isolation by using separate virtual machines and leveraging Azure Hypervisor isolation.
- **Drawbridge isolation** inside a Virtual Machine (VM) for services that provide cryptographically certain isolation for workloads running on the same virtual machine by leveraging isolation provided by Drawbridge[15]. These services provide small units of processing using customer code.

[13] https://www.fcc.gov/general/technological-advisory-council
[14] https://www.fcc.gov/file/22737/download
[15] https://www.microsoft.com/research/project/drawbridge/

- **User context-based isolation** for services that are comprised solely of controlled code and customer code is not allowed to run.

In addition to robust logical compute isolation, customers who desire physical compute isolation can utilize Dedicated Host or Isolated Virtual Machines, which are deployed on server hardware dedicated to a single customer.

Networking isolation

Network isolation helps ensure that each customer's private network traffic is logically isolated from traffic belonging to other customers. Services can communicate using public IPs or private IPs.

Storage isolation

To ensure cryptographic certainty of logical data isolation, data encryption at rest can be done using advanced algorithms with multiple ciphers.

5.3.4 Resiliency

Resiliency is another benefit of using virtualization, as it relates to network topology. Resiliency has many aspects, and as an immediate example, not having dependencies on hardware that may become unavailable, is an immediate effect of the virtualized environment. 5G is also defined as a microservice architecture, which adds an additional layer of resiliency, by the way microservices are being designed today.

6 Security and Resilience Implications Associated With 5G Virtualization

This chapter provides a non-comprehensive, overview of the most significant new and different attack surfaces that should be contemplated in the virtualization of 5G and telecommunications services.

6.1 Virtualization Security Risks

While the transition to 5G presents a wealth of opportunities and capabilities, it also introduces new vulnerabilities and threats. ETSI published Specifications ETSI GS NFV-SEC 001 V1.1.1[16], which provides a summary of the security risks associated with virtualization.

6.2 Supply Chain Risks

[16] ETSI Published Specifications ETSI GS NFV-SEC 001 V1.1.1: Network Functions Virtualisation (NFV); NFV Security; Problem Statement

The 5G supply chain is susceptible to the introduction of risks including malicious software and hardware, counterfeit components, poor designs, manufacturing processes, and maintenance procedures. Unauthorized deployment of software and hardware provides a good attack surface equipped with the opportunity for attackers to eavesdrop on traffic, shadow a victim’s process or VMs, modify security parameters, install hidden malware and backdoors, as well as many other potential damages to the operations. The exposure to these risks threatens the quick deployment of 5G networks. This may further lead to loss of confidence in the integrity of 5G networks or even the impairment of national security. Untrusted suppliers pose the great supply chain risk, for instance, 5G networks with compromised components, devices, software/hardware, or even services, could be vulnerable to the interception, eavesdropping, manipulation, disruption, or destruction of data.

6.3 Cross VM Shared Resource Threats

Virtualization hides the internal details of the underlying resources from the end users. Even though operated by the same host, multi-tenant VMs are separated from one another by a virtual machine manager (VMM) with the property of virtual isolation which means they are sharing physical resources at runtime. A shared pool of resources from VMs facilitates faster processing with limited resources, however this shared mechanism also invites many kinds of security attacks. One example is the use of the covert channel[17] to move (exfiltrate) secure information such as stored private keys from a shadowed VM. Another type of attack is a Side-Channel-Attack (SCA) that exploits shared physical resources like a CPU cache, a memory buffer, a branch target buffer, cache, or network queue to gain access or even shadow the targeted VMs.

6.4 Container Image Threats

A container is a standard unit of software that packages up code and all its dependencies, so the application runs quickly and reliably from one computing environment to another. A container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings. Several recent studies[18] uncovered supply chain attacks that use malicious container images to compromise their victims. The images can hijack organizations’ resources to mine cryptocurrency and can be used as part of a supply chain attacks to sabotage the target systems.

6.5 Platform Exploit Threats

A deployed 5G core is made up of thousands of servers, routers, and switches, each running security hardened OSs and firmware. The exploit of the BIOS (Basic Input/Output System) or

[17] Betz J, Westhoff D, Müller G (2017) Survey on covert channels in virtual machines and cloud computing. Trans Emerg Telecommun Technol 28(6):3134

[18] https://blog.aquasec.com/supply-chain-threats-using-container-images

firmware can result in malicious code residing in the kernel to acquire full control of the system. Additional hardware components could be exploited to give unauthorized users access to the system or the data without the system owner’s knowledge. Firmware management is another area of potential exploit. While firmware must be authorized before being deployed, some masquerading firmware upgrades can evade the authentication and authorization system through forgery of signatures and install malicious firmware into a 5G system. Some passive malicious “firmware” residing on a host is hard to detect with abnormality scanning. In security assessments, it’s always a best practice to “partition” or “sandbox” the running firmware in a trusted container. The trusted container must have strong authentication and authorization, and be equipped with the hardened hardware protection modules, such as TPM (Trusted Platform Module).

6.6 NFV Infrastructure Security Threats

NFV deployments could use Software-Defined Networks (SDN) either for the management and control planes or for the data plane. In many circumstances, the infrastructure network might use traditional distributed routing algorithms to build the routing and forwarding tables at each node (e.g., open shortest path first (OSPF), the Intermediate System to Intermediate System (IS-IS) protocol or the spanning tree protocol). Virtualized Network Routers/Switches could be exploited if no mutual authentication exists between them and the controller. This could lead to the exposure of the network topology to attackers, yielding critical routing and switching information.

6.7 VNF (Virtualized Network Function) Threats

ETSI NFVI is envisioned to endure various attacks from networks (remote or inside) with its security enabling technologies consisting of CIA triads (Confidentiality, Integrity, Authenticity), privacy, and trust for secure networking. However, some of the virtualized 5G networks functions, such as the mobility management entity (vMME) can be exploited to cause a signaling storm. Other types of network functions, such as a Virtual firewall, may be improperly equipped with VM escape exploits, that can be compromised to allow an attacker to gain illicit access privileges or involuntarily trigger VNF migration events to lower grade of security protection, known as downgrade attack.

If virtualized network functions were to be compromised through a network layer exploit, attackers could obtain unauthorized access to the 5G network, potentially disrupting operations and enabling interception, manipulation, and destruction of critical data.

6.8 Network Slicing threats

Network slicing is a key feature of 5G, and its implementation fully utilizes the virtualization paradigm specified in NFVI. Network slicing allows users to be authenticated for only one network area, enabling data and security isolation. However, network slicing can be difficult to manage, and the slices add complexity to the network. Misuse or misconfiguration of network slice management may allow attackers to obtain data from different slices or deny access to privileged users.

6.9 Multi-Vendor VNF Threats

5G network operators seek to offer the best technologies to their customers so VNFs are likely to be provided by many different vendors. This can result in interoperability issues causing security loopholes in the infrastructure. Hybrid virtualized network functions provided by different vendors are normally equipped with different technologies and run-on different platforms. The interworking among them needs not only standardized interfaces, but also the orchestration of secure bootstrapping, secure handshakes in establishing the communication channels and maintenance of the secure communication channels. Some exploits utilize the uncoordinated communications channels between VNFs to gain illicit access[19].

6.10 Multi-tenant AAA threats

NFV brings new security issues when it comes to Authentication Authorization and Accounting (AAA), as it implies using identity and accounting facilities at two or more layers: the network and virtualization infrastructure (e.g., identifying the tenants or guest service providers). ETSI GS NFV 001 proposes server use cases, such as NFVIaaS, VNFaaS, etc,, that could utilize a stack of identifications across multiple layers. This contradicts today’s AAA infrastructure that can only handle a single identity per user, single level of policy decision and enforcement paradigm. The comprehensive identity management requirements could lead to privacy breaches associated with the disclosure of user information at layers that are not intended to consume certain identity attributes, or illicit privilege escalation produced by piggybacking unrelated identities.

6.11 Security Operation Threats

More virtualized network functions within 5G also brings challenges to the 5G service provider’s security operation. Poor implementation and provision of VNFs can result in inadequate security control being placed on the VNF. Virtualization also brings more heterogenous system and virtualized components into services. User specific traffic and critical information are more intertwined together inside a physically constrained resource, such as cache, buffer, queue, and memory. This contrasts with traditional service provider NOC (Network Operation Center) model which can isolate the incidents and quickly recover. Improper management and operation procedures, for instance, image upgrade, could result in service disruption for prolonged time. Overall, 5G Virtualization provides great benefits for 5G service providers in terms of cost efficiency and dynamic service resilience; however, it is imperative to understand the incumbent security implications and threats.

6.12 5G Microservices Threats

[19] W. Yang and C. Fung. “A Survey on Security in Network Functions Virtualization,” 2016 IEEE NetSoft Conf. and Wksps. (NetSoft), 2016

The service-based architecture (SBA) of the 5G core network is designed with a cloud-native approach, and millions of microservices, which split NFs into individual parts with each providing an independent function. This helps 5G achieve flexibility, and service resilience. These risks are the same as many IT microservice scenarios. Some studies20 have identified a risk that an attacker can exploit in a Network Element (NE) which employs microservices in an SBA: the attacker may initiate a request from open interface to other microservices, resulting an anomaly access, for example, an Access and Mobility Management Function (AMF) function being exploited can circumvent an Authentication Server Function (AUSF) to initiate an authentication directly to the Unified Data Manager (UDM)) to obtain access. Another type of attack involves an exploited Network Element (NE) launching a Denial of Service/Distributed Denial of Service (DoS/DDoS) on another NEs. The nature of atomically distributed microservices in NEs may be challenge network management due to its topological complexity, as well as the exhaustion of the communication resources in connecting multiple microservices. To thwart the attacks on distributed microservices in a 5G core, one approach is to enable the detection of service anomalies by tracing the call sequences and parameters by deploying additional security perimeter framework.

6.13 API Security Risks

The 5G SBA architecture has been designed to support SDN and NFV, which have inherently made use of the HTTP and REST API services. Most of the APIs are gateways to application logic, such as the control of IoT devices and associated sensitive data or User Identity information. There are however assorted penetration tools that can exploit the vulnerabilities of these APIs. One attack scenario involves the detection of unpatched API versions with reported attack vectors. Another attack scenario led to attackers with knowledge of the victim system, which may lack sufficient logging and detection capabilities, to penetrate the host system without being detected.

7 Existing and Best Practices Standards

Standards by their nature are market level tools and mechanisms to drive operations, choices, and business critical decisions such as:

- Regulatory and compliance requirements
- Interoperability
- Supplier or vendor diversity including risk mitigation
- Quality
- Performance etc.

As outlined in prior chapters of this document, 5G deployments represent a confluence of architectures, build and operating practices from multiple and in many instances disparate industry standards development and open-source organizations. This confluence requires

[20] Chandramouli, R.: Security strategies for microservices-based application systems. Tech. rep. (2019)

specialized attention to ensuring comprehensive integrity across the entire system across all these organizations.

This chapter documents this expanding environment of networks and IT and provides a non-comprehensive list of organizations and standard bodies that should be consulted for exiting recommendations and best practices.

As Security remains a critical and universal concern, several international standards organizations have produced specifications covering different security elements of the 5G network. However, it must be noted that the security of a deployed network is the result of many participants, and processes working together. The mobile network specifications can be viewed as the initial blueprint taking into consideration the security of the architecture aimed to support a set of use-cases. This blueprint is materialized in products using the possibilities and security principles that Information and Communication Technology and particularly cloud technology offer in consideration of regulatory requirements.

Because a typical deployed network is a result of the orchestration of the Mobile Network Operator (MNO) on the cloud infrastructure, cloud providers and MNOs share security responsibilities.

The following sections of this Chapter cover an introduction to NIST security guidance on cloud and virtualization relevant for 5G. This is followed by the role of ETSI NFV SEC and is outlined alongside a series of NFV security areas subject to specification and relevant to this document. Finally, 3GPP SA3 standardization efforts for security and virtualization are also summarized, with an emphasis on the impacts of virtualization in 3GPP.

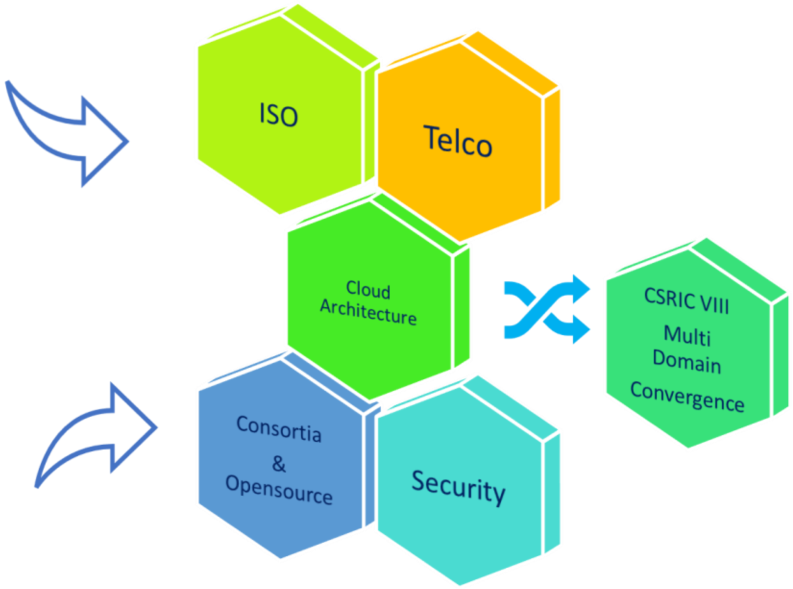


Figure 7-1 Convergence from multiple industry and standards environments

7.1 NIST Security Guidance

As outlined and explained in Chapter 4, cloud and virtualization technologies are base technologies in 5G network implementations. Recent 5G products increasingly use container technologies that will benefit and must coexist from the base technologies for cloud computing. The next sub-sections contain an overview of NIST guidance on cloud and virtualization and on containers.

It must be noted that secure communications represent a critical aspect for these networks. For example, the TLS protocol is a crucial component in the 5G networks as it is heavily used to protect the inter- and intra- communications of applications. Having guidance on secure implementations and use of TLS throughout the 5G system is therefore fundamental. The NIST SP 800-52 rev.2 [21] "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" publication is relevant in this context.

7.1.1 On Cloud and Virtualization

Known to be the de facto driver for key security areas such as long-term cryptographic standards and the NIST Cybersecurity Framework[22], NIST has already published significant guidance relevant for 5G security. The NIST Special Publications SP-800 series includes a set of 23 publications (18 final and 5 in draft stage, see Table 7-1) directly related to the topic of cloud and virtualization technologies. Other SDOs (e.g., ETSI) and agencies (e.g., ENISA) currently promote recommendations from several of these publications, which in turn reference other significant NIST guidance published for a wider range of security topics, such as security and privacy controls for information systems, cybersecurity practices, etc. The following is an introduction to the NIST guidance in the context of cloud and virtualization is given with the corresponding references:

- NIST SP 800-145 *The NIST Definition of Cloud Computing*[23], which globally persists as the seminal reference document for the cloud definition. It defines five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service); three service models (SaaS, PaaS, IaaS); and four deployment models (private, community, public, hybrid).

- NIST SP 800-125 *Guide to Security for Full Virtualization Technologies*[24], which provides recommendations for addressing the security concerns associated with full virtualization technologies, for server and desktop virtualization. Recommendations include: (1) secure all elements of a full virtualization solution and maintain their security; (2) restrict and protect administrator access to the virtualization solution; (3) ensure that the hypervisor is properly secured. The hypervisor types (Type-1 and Type-2) and the five typical baseline functions of a hypervisor (i.e., VM process isolation, devices mediation and access control, direct execution of commands from guest VMs, VM lifecycle management, management of hypervisor platform) are further described in SP 800-125 A[25] alongside recommendations for platform integrity in general and for

[21] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
[22] https://www.nist.gov/industry-impacts/cybersecurity-framework
[23] https://csrc.nist.gov/publications/detail/sp/800-145/final
[24] https://doi.org/10.6028/NIST.SP.800-125
[25] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125Ar1.pdf

each of the hypervisor functions. In addition, SP 800-125 B[26] provides an analysis of various virtual network configuration options for protection of VMs and present recommendations based on this analysis.

- NIST SP 800-204/-A/-B/-C, which address various aspects of microservices development and deployment:
  - NIST SP 800-204 *Security Strategies for Microservices-based Application Systems*[27] includes a study of the technology behind microservices-based applications and identifies the core features usually necessary for such application deployments (i.e., authentication, access control, service discovery, load balancing, response caching, application-aware health checks, and monitoring). Threats specific to the operating environment of microservices are identified and a set of security strategies for implementing the core features and to be considered for the architectural frameworks (API gateway and service mesh) are described.

  - NIST SP 800-204A *Building Secure Microservices-based Applications Using Service-Mesh Architecture* [28] defines the service mesh as a robust security infrastructure for supporting microservices-based applications. The short-lived behavior of containers calls for secure service discovery. In the state-of-the-art chapter, it is acknowledged that service meshes are "*most suitable and productive for application platforms*" where the microservices are implemented as containers and the application makes use of container clusters which are managed using container orchestration tools. The document provides deployment recommendations for service mesh components: service proxies, ingress proxies, egress proxies, identity and access management, monitoring capabilities, network resilience techniques, and cross-origin resource sharing.

  - NIST SP 800-204B *Attribute-based Access Control for Microservices-based Applications using a Service Mesh*[29] provides recommendations for the deployment of an ABAC-based authentication and authorization framework for microservices-based applications within a service mesh that provides the infrastructure for various services, including critical security services. While the objective is for the guidance to be agnostic to the platform hosting the application and the service mesh technology, Kubernetes®® [30] and Istio[31] are used as references for concrete examples. The recommendations address mechanisms for supporting both end-user and service level authentication and authorization policies. Several of these recommendations naturally fall into best practices to secure Kubernetes® -based deployments.

[26] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf
[27] https://doi.org/10.6028/NIST.SP.800-204
[28] https://doi.org/10.6028/NIST.SP.800-204A
[29] https://doi.org/10.6028/NIST.SP.800-204B
[30] https://kubernetes.io/
[31] https://istio.io/

- NIST SP 800-204C *Implementation of DevSecOps for a Microservices-based Application with Service Mesh*[32] describes the diverse code types (application code, application service code, infrastructure as code, policy as code, and observability as code) and the need of a different development, deployment, and runtime paradigm: the DevSecOps methodology. Guidance for the implementation of DevSecOps primitives for cloud-native applications is provided to achieve higher levels of security assurance. The chosen platform is a container orchestration and resource management platform (e.g., Kubernetes®).

- NIST SP 800-209 *Security Guidelines for Storage Infrastructure*[33] provides security recommendations for several storage technologies, including storage for VMs and containers. The document includes information regarding storage security threats, risks, and attack surfaces. Through the twelve classes of recommendations for storage deployments, the guidelines provide the basis for securing a storage infrastructure, which represents one of the three pillars of IT along compute and network infrastructures.

- NIST SP 800-210 *General Access Control Guidance for Cloud Systems*[34] presents cloud access control (AC) characteristics and a set of generic AC guidance for the IaaS, PaaS, and SaaS cloud service models. The characteristics considered to represent challenges in designing AC systems are broad network access, resource pooling, rapid elasticity, measured service, and data sharing. An important outcome is the mapping of the provided AC guidance to the AC control elements listed in the NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations* Revision 4 [35].

Table 7-1 : NIST publications in the SP-800 series related to cloud & virtualization

Series Number	Title	Status	Release Date
SP 1800-19	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	Final	4/20/2022
SP 1800-33	5G Cybersecurity (Preliminary Draft)	Draft	4/25/2022
SP 1800-35	Implementing a Zero Trust Architecture (Preliminary Draft)	Draft	8/09/2022
SP 800-215	Guide to a Secure Enterprise Network Landscape	Draft	8/05/2022
SP 800-210	General Access Control Guidance for Cloud Systems	Final	7/31/2020
SP 800-209	Security Guidelines for Storage Infrastructure	Final	10/26/2020
SP 800-207	Zero Trust Architecture	Final	8/11/2020
SP 800-204C	Implementation of DevSecOps for a Microservices-based	Final	3/08/2022

[32] https://doi.org/10.6028/NIST.SP.800-204C
[33] https://doi.org/10.6028/NIST.SP.800-209
[34] https://doi.org/10.6028/NIST.SP.800-210
[35] https://doi.org/10.6028/NIST.SP.800-53r5

	Application with Service Mesh		
SP 800-204B	Attribute-based Access Control for Microservices-based Applications using a Service Mesh	Final	8/06/2021
SP 800-204A	Building Secure Microservices-based Applications Using Service-Mesh Architecture	Final	5/27/2020
SP 800-204	Security Strategies for Microservices-based Application Systems	Final	8/07/2019
SP 800-190	Application Container Security Guide	Final	9/25/2017
SP 800-180	NIST Definition of Microservices, Application Containers and System Virtual Machines	Draft	2/18/2016
SP 800-146	Cloud Computing Synopsis and Recommendations	Final	5/29/2012
SP 800-145	The NIST Definition of Cloud Computing	Final	9/28/2011
SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing	Final	12/09/2011
SP 800-125B	Secure Virtual Network Configuration for Virtual Machine (VM) Protection	Final	3/07/2016
SP 800-125A Rev. 1	Security Recommendations for Server-based Hypervisor Platforms	Final	6/07/2018
SP 800-125	Guide to Security for Full Virtualization Technologies	Final	1/28/2011
NISTIR 8320	Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases	Final	5/04/2022
NISTIR 8320A	Hardware-Enabled Security: Container Platform Security Prototype	Final	6/17/2021
NISTIR 8310B	Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms	Final	4/20/2022
NISTIR 8310C	Hardware-Enabled Security: Machine Identity Management and Protection	Draft	4/20/2022

7.1.2 On Application Containers

NIST SP 800-190 *Application Container Security Guide* [36] explains the security concerns associated with container technologies and makes practical recommendations for addressing these concerns. The offered best practices are considered generic and applicable between all environments and networks. Many of these recommendations are already referenced by different organizations, e.g., ENISA *NFV Security in 5G - Challenges and Best Practices*[37].

The guidelines cover threats and countermeasures through the multiple layers of the stack, best practices around protecting the virtual machines and hosts applicable to the container world, fundamentals around vulnerability management, and secure configuration.

The chapter introducing the application containers recalls the five tiers of the container

[36] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
[37] https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

technology architecture:

- Developer systems generating the images (each container image is assumed to consist of several components, e.g., *layers*).
- Testing and accreditation systems which validate, sign the images, and send them to a registry.
- Registries storing and distributing images to the orchestrator upon request.
- Orchestrators (e.g., Kubernetes®).
- Hosts.

An analysis of the major risks associated with the container technologies' core components (i.e., images, registries, orchestrator, containers, hosts) is performed, with a focus on two specific types of risks: compromising an image or container, and misuse of a container to attack other containers, the host OS, etc. The set of countermeasures addressing the major risks in the scope of this document is described systematically and two examples are provided to illustrate their effectiveness.

Recommendations are articulated on the following aspects:

- Use container-specific host OSs instead of general-purpose ones to reduce attack surfaces
- Only group containers with the same purpose, sensitivity, and threat posture on a single host OS kernel to allow for additional defense in depth
- Adopt container-specific vulnerability management tools and processes for images to prevent compromises
- Use container-aware runtime defense tools

In its appendix, the NIST SP 800-190 document contains pointers to general references for securing non-core container technologies, in addition to listing the most important SP 800-53 Revision 4 [38] security controls for container technologies.

7.2 ETSI NFV SEC (Network Function Virtualization Security)

The Security Expert Group (SEC EG) of ETSI ISG NFV is a collaborative work between various security delegates representing operators, vendors, governmental organizations such as law enforcement agencies and others. The ETSI NFV SEC EG produces reports (also known as Group Reports – GRs) and specifications (Group Specifications – GS) for different security areas applicable to virtualization, such as:

- Identifying security problems related to NFV and how these may be solved,
- Providing guidance on key security topics like identity and certificate management,
- Authentication and authorization,
- Security architecture specifications covering security management, certificate management, etc.

NFV SEC works closely with other ETSI ISG NFV working groups such as:

[38] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

- ETSI NFV-IFA WG (Interfaces and Architecture – covering stage-2 specifications),
- ETSI NFV-SOL WG (Solutions – covering stage-3 specifications) and
- ETSI NFV-TST WG (Testing, Experimentation and Open Source – supporting stage-4 specifications used for interoperability and certification ETSI Plugtest events), as well as groups external to ETSI NFV such as TC Cyber, TC LI, etc.

7.2.1 Security and Trust Guidance

ETSI GS NFV-SEC 003 is a specification building on the problem statement described in ETSI GS NFV-SEC 001, to describe security and trust guidance unique to NFV development, architecture, and operations. Recall that the reference NFV-MANO high-level architecture includes the NFVO, VNFM, VIM. The NFVI represents the platform on top of which applications (e.g., 3GPP network functions) sit as VNFs. In order to have overall security in such a network, all layers must be taken into account conjointly and not in isolation**,** with trust being built dynamically wherever necessary, eventually relying on attestation mechanisms. The security guidance is organized into several categories such as NFV security use cases, external operations (physical/HW security, DNS, ID management, etc.), NFV security lifecycle management (which includes threat assessments, certificate management, and multiple security domains), and security technologies (such as trustworthy boot, attestation, and IAM). Several key security aspects identified by ETSI GS NFV-SEC 003 are applicable to container-based deployments and have become subject of study or specification in more recent work items (e.g., ETSI GS NFV-SEC 023 for container security including VNF packages and container image management, ETSI GS NFV-SEC 024 for security management applicable to both VM- and container-based deployments, etc.).

7.2.2 Threat Analysis and Mitigation for the Management and Orchestration Layer

A threat analysis of the NFV-MANO blocks (NFVI, VNFM, VIM) and corresponding reference points is performed and a set of requirements to mitigate the identified threats is specified in ETSI GS NFV-SEC 014. The analysis relies on the so-called pro forma of security and regulatory concerns for use in ETSI ISG NFV GS published in ETSI GS NFV-SEC 006. It includes:

- Assumptions (e.g., the attackers are attached to the network and have access to the NFV-MANO functional blocks and reference points);
- Identification of the assets to protect (e.g., assets are the NFV-MANO functional blocks, the various reference points in the scope of NFV-MANO, and the different credentials to access these blocks and reference points);
- Threats and threat agents, which comprise probes on the various interfaces and different users capable of accessing the NFV-MANO blocks and reference points.
- Security requirements given the security objectives for assets and the deployment environment, the various mitigations are captured as security requirements both for the assets and for the environment.

Several of the listed requirements in ETSI GS NFV-SEC 014 can be fulfilled by implementing an authentication and authorization framework with secure communications (e.g., TLS) on the different interfaces. The ETSI GS NFV-SOL 013 – "Specification of common aspects for Restful NFV MANO APIs" becomes relevant in this context. The various NFV-MANO entities are expected to communicate over secure channels. In recent versions of ETSI GS NFV-SOL 013, the TLS profiles are being aligned with the TLS profiles in 3GPP 5G security. ETSI GS NFV-SOL 013 also deals with the authorization framework and relies on OAuth2.0 with bearer tokens. Mapping the OAuth2.0 roles to the NFV-MANO roles in the typical use-cases of API requests and notifications, is further described in ETSI GS NFV-SEC 022. The ETSI GS NFV-SEC 022 specification – "Access Token Specification for API access" – is focused on the authorization framework adopted in ETSI GS NFV-SOL 013. Consequently, several of the security provisions and requirements dictated by ETSI GS NFV-SEC 022 are adopted as normative text in the latest ETSI GS NFV-SOL 013 versions for the security of RESTful NFV-MANO APIs. Note that ETSI GS NFV-SEC 022 is currently open for a new release.

7.2.3 Remote Attestation

Attestation is a tool useful to gain higher level of assurance as stated in ETSI GR NFV-SEC 007: "*MANO operators and Service operators need assurance that their VNFs are running securely so in order to achieve this they need to know that the host platform is trustworthy and that the VNF is securely launched and continues to run securely in VNFCIs on the platform. Such secure platform has to provide ways for VNFs to verify trust-related information about the NFV platform*". As such, attestation is a technology for implementing a Zero Trust type verification of a peer VNF before engaging in exchange of application traffic.

The ETSI GR NFV-SEC 018 report on NFV remote Attestation Architecture reuses definitions from earlier specifications like ETSI GS NFV-SEC 003, ETSI GR NFV-SEC 007/009. The high-level remote attestation architecture from ETSI GR NFV-SEC 018 is translated into a lower-level architecture described in the ETSI GS NFV-SEC 024 security management specification (currently ongoing draft) to address those VNFs that require secure bootstrapping with remote attestation and Hardware-Mediated Execution Enclave (HMEE). The ETSI GS NFV-SEC 024 proposes an example of VNF secure provisioning protocol where the Security Manager entity defined in ETSI GS NFV-IFA 026 plays an active role and is assumed to embed the attestation verifier function for the remote architecture procedure.

Note that the IETF RATS working group has defined an architecture for remote attestation and addresses objectives like the ETSI GS NFV-SEC 024 VNF secure bootstrapping protocol. There are indications that NFV SEC is seeking alignment with RATS. In addition to the progress made for VNF secure bootstrapping, NFV SEC shows recent efforts to use secure enclave technologies with remote attestation for two other topics: (1) for the SW supply chain to verify the container image authenticity at VNF instantiation; and (2) in the certificate management to distribute trust anchors.

7.2.4 VNF Package Security

The scope of the ETSI GS NFV-SEC 021 specification is to define VNF Package security requirements and to address issues related to integrity, authenticity, and confidentiality of the VNF Package artifacts, including the corresponding validations at VNF package onboarding and instantiation. The structure and format of the VNF package with its constituents (VNF descriptor ETSI GS NFV-SOL 001, manifest file, artifacts including VNF images, etc.) is specified in ETSI GS NFV-SOL 004. Several security constructs such as signatures and X.509 certificate file(s) are also part of the VNF package. ETSI GS NFV-SEC 021 specifies requirements at both VNF package onboarding and VNF instantiation phases. ETSI GS NFV-SEC 021 is presently open for Release-4. The certificate management topic undergoing specification at the time of writing is expected to trigger ETSI GS NFV-SEC 021 updates. We also note that container image validation at VNF instantiation is further refined in ETSI GS NFV-SEC 023 - Container Security specification (next section).

7.2.5 Container Security

Container Security specification is currently an open draft including a threat analysis for the container based NFV deployments and requirements to securely run container-based VNFs, be it on bare-metal or in VMs. ETSI NFV IFA WG does not define a new reference architecture dedicated to container-based VNF orchestration, but the NFV-MANO capabilities are enhanced to support container technologies based on the ETSI GR NFV-IFA 029 report (see ETSI Blog [39] for a summary of these enhancements). In this context, new functions with requirements for the services offered by these functions and for the interfaces exposing these services are published in ETSI GS NFV-IFA 040 and ETSI GS NFV-IFA 036. The ETSI GS NFV-SOL 018 specification will provide a mapping of the NFV object model for OS container management and orchestration to managed objects of Kubernetes® and Helm® as specified by the CNCF®. The latest ETSI GS NFV-SEC 023 covers aspects of:

1. container image management, including VNF package onboarding and VNF instantiation
2. an application of the hardware-based trusted execution environment (e.g., HMEE) to the software supply chain
3. and finally, considering the best practices published by e.g., CISA/NSA and NIST, for security container and related orchestration

7.2.6 Security Management

The ETSI GS NFV-SEC 013 specification proposes an architecture for monitoring and security management purposes. However, ETSI GS NFV-SEC 013 will be refreshed with new technologies and replaced by a new specification (currently ongoing draft) – ETSI GS NFV-SEC 024 “Security Management”. In the same area, the NFV IFA WG published two relevant documents for security management:

[39] https://www.etsi.org/newsroom/blogs/technologies/entry/os-container-object-model-and-management-interfaces-the-first-set-of-cloud-native-vnf-orchestration-specifications

- ETSI GS NFV-IFA 026 lists requirements to support security management and monitoring from ETSI GS NFV-SEC 013. A new functional block is defined – the Security Manager – and three reference points from Security Manager to NFVO, VNFM and VIM are introduced.
- ETSI GS NFV-IFA 033 shows how the new Security Manager reference points can be fulfilled by reusing existing NFV-MANO interfaces.

7.2.7 Certificate Management

Certificate management relates to identity management. This topic is increasingly becoming crucial for modern ICT systems due to the adoption of cloud compute and microservices technologies where larger functions are broken up in smaller components that are virtualized and instantiated through orchestration tools. These tools need to be connected securely, most often using Internet based protocols like HTTP(s), (D)TLS, etc. For that reason, certificate management is appearing in several standardization bodies, most notably, ETSI NFV, 3GPP, IETF, GSMA, and in ICT technologies like Service Mesh (e.g., as part of Istio). Also, with the Zero-Trust approach to holistically achieve security in an ICT system, identities and certificates are fundamental.

Certificate management was addressed by NFV SEC, with two versions of ETSI GR NFV-SEC 005 "Report on Certificate Management". In the first version, the report relies on IETF work to introduce general considerations on public key infrastructure (PKI), including the description of a typical certificate validation algorithm. In the second version of this report (published in 2021), several notable updates have been proposed related to the EST protocol, possible enhancements on the NFV-MANO functional blocks, and characteristics related to container-based VNFs. The normative work on certificate management has recently started with small feature enhancements being developed for ETSI GS NFV-IFA 010 and ETSI GS NFV-IFA 026 pertaining to the NFV Release 5 (ENH01.01). It is not surprising to find tens of different transport certificates associated with a VNFI realization (and several others at management layers) in complex deployments such as 3GPP SBA NFs. NFV SEC and 3GPP SA3 are expected to align in these aspects.

7.2.8 Secure End-to-End VNF and NS Management

The scope of ETSI NFV-SEC 025 (draft) covers the definition of new capabilities to enable a secure end-to-end management of VNFs and NS, starting from the VNF/NS on-boarding, instantiation and configuration, mobility scalability during the run time and termination of VNF/NS. The specification introduces a detailed threat analysis for both VNF and network service throughout their lifecycle (onboarding, instantiation, configuration, run-time, termination), using the template format for threat analyses published in ETSI GS NFV-SEC 006. In addition, knowing that "Some VNF suppliers make use of the underlying NFVI platform capabilities in order to accelerate performance and optimize throughput of their VNF products"[40] (e.g., accelerators), ETSI GS NFV-SEC 025 proposes additional security features on the NFVI

[40] https://nfvwiki.etsi.org/index.php?title=NFVI_Platform_Capability_Registry

platform to be added in the NFVI Platform Capability Registry.

7.2.9 Isolation and Trust Domain Specification

The ETSI GS NFV-SEC 026 specification (draft) is a recent work item started to detail security key issues in multi-tenancy scenarios. It aims at defining the requirements and solutions for the NFV system to enhance network functions and services isolation between tenants (see also Chapter 5.3.3). The first part of ETSI GS NFV-SEC 026 performs a threat analysis for the multi-tenancy scenarios described in ETSI GR NFV-EVE 018 and has already specified mitigation requirements for all of them. It will continue with requirements for trust domain separation, memory protection and access control, hypervisor trust portioning, escape protection, and key management systems.

7.2.10 NFVI and MANO Security Assurance

The ETSI GR NFV-SEC 027 report on NFVI security assurance is developed in NFV SEC. The objective is to study the security assurance of NFVI products and deliver security test cases including testing goals, testing steps, evidence of testing results for evaluating if the security requirements are fulfilled by NFVI products and based on the requirements published in previous specifications (e.g., ETSI GS NFV-SEC023/025/026, etc.). The NFV-MANO products will soon be subject to security assurance as well as a new corresponding normative work item (ETSI GS NFV-SEC 028) has been started. The expected outcome is a set of security requirements and test cases for evaluating the security MANO products leveraging the security assurance methodology introduced in 3GPP. Security requirements defined in previous specifications (e.g., ETSI GS NFV-SEC014/024/025) will be the input to this work item.

7.2.11 3GPP Security for Virtualized Networks

3GPP (the 3rd Generation Partnership Project) is the de facto organization that develops technical specifications for mobile networks (i.e., 2G, 3G, 4G, and 5G). Specifically, it provides specifications for network functions, their APIs, and test as well as assurance procedures. 3GPP unites telecommunications standard development organizations around the world (i.e., ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC). The technical specifications are published as "Releases", with a set of functionalities that are stable and implementable at a given point. 3GPP Release 15 delivered the first 5G technical specifications for RAN, transport, Core, Orchestration as well as roaming interconnect. Starting with 4G, the current specifications also cover interaction with non-5G network technologies such as WLAN.

The 5G System Architecture[41] is defined in 3GPP TS 23.501 as a Service Based Architecture (SBA) that is, a system architecture in which the system functionality is realized by a set of Network Functions (NFs) providing services to other authorized NFs to access their services.

[41] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

The SBA realization of the 5G Core network[42] is specified in 3GPP TS 29.500 and is built on web technologies and protocols. As 5G security in general, the security of SBA[43] is specified in 3GPP TS 33.501. The introduction of SBA resulted in that the 3GPP 5G specifications cover more mobile network implementation aspects than previous generations. The 5G SBA Release 17 includes over 35 different types of NFs supporting a wide range of use cases.

The 3GPP-defined 5G Network Function (NF) "can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform, e.g., on a cloud infrastructure" (3GPP TS 23.501)[44]. It is also widely accepted that "Virtualization is a fundamental building block of 5G and while not the only way of implementing a 5G network, it is nevertheless the primary implementation method being pursued to some degree (great or small) by all operators and manufacturers." (3GPP TR 33.848)[45].

The 3GPP Technical Specification Groups (TSGs) for Service and System Aspects (SA) produced several technical specifications (TSs) and technical reports (TRs) directly addressing virtualization and cloud areas. The primarily involved working groups are: (1) the 3GPP TSG SA5 – Management, Orchestration and Charging working group – for virtualization management functions with documents published in the 3GPP 28-series and 32-series; and (2) the 3GPP TSG SA3 – Security and Privacy working group – with documents published in the 3GPP 33-series (see Table 7.3-1). In what follows, an introduction to the 3GPP standardization area on the security assurance for virtualized networks as well as to the current 3GPP study on the security impacts of virtualization is provided.

Table 7.3-1: 3GPP SA3 documents covering cloud and virtualization

Reference	**Title**	**Technolog y**
TS 33.527	Security Assurance Specification (SCAS) for 3GPP virtualized network products	5G
TR 33.818	Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products	5G
TR 33.848	Study on security impacts of virtualization	5G, LTE
TR 33.927	Security Assurance Specification (SCAS) threats and critical assets in 3GPP virtualized network product classes	5G
TR 33.936	Security Assurance Methodology (SECAM) for 3GPP virtualized network products	5G

7.3 Security Assurance in 3GPP Virtualized Network Products

As stated in TR 33.916, "*Security of Network Products should be measurable, comparable, and follow a common standardised baseline.*". It is in this context that the Security Assurance

[42] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3338
[43] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
[44] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144
[45] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574

Methodology (SECAM) evaluation process is defined at 3GPP to comprise the Vendor Network Product Development process evaluation, the product lifecycle management process evaluation, and the Network Product evaluation. The five roles involved in the SECAM scheme are:

1. 3GPP network product Vendors, which are expected to implement security reliability models incorporating security and privacy considerations into all relevant aspects and phases of the products
2. Accredited Test laboratories (ISO 17025 accredited in the context of GSMA NESAS[46] , to evaluate the network product, the evidence of compliance to vendor development and product life cycle management requirements
3. Operators taking the security acceptance decisions
4. 3GPP that produces security assurance specifications (SCAS) (a list of 3GPP SCAS documents is available on[47] [ref-SCAS-docs])
5. SECAM Accreditation Body responsible for the accreditation tasks. This role is currently assumed by GSMA.

The development of a SCAS specification is further described in TR 33.916[48]. The normative work typically includes: (1) identifying the critical assets to protect for the specific network product class and a threat analysis; (2) identifying the relevant security requirements (e.g., from catalogues of security requirements such as those in TS 33.117[49] or derived from TS 33.501[50]) to mitigate the threats; and (3) designing the test cases to verify how the security requirements are fulfilled.

In TS 33.117[51], a generic set of security requirements to be met by all network products is specified in the so-called “technical baseline” to counter the generic security threats identified by TR 33.926[52]. The scope of TR 33.926 includes the network product class descriptions such as the Generic Network Product (GNP), threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications.

Currently in an early stage of development, the TS 33.527[53] specification will include the objectives, a catalogue of requirements, and a set of test cases for Virtualized Network Product (VNP) classes, which are described in the TR 33.927[54] report. Similar in principle to TR 33.926, the scope of TR 33.927 includes the identification of threats and critical assets for the VNP class descriptions.

According to TR 33.818[55], the Generic VNP (GVNP) class introduced by TR 33.927 and reused by TR 33.936[56] can be further decomposed into:

- VNP class “type 1” implementing 3GPP defined functionalities only.

[46] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[47] https://www.gsma.com/security/nesas-documents/
[48] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2345
[49] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928
[50] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144
[51] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928
[52] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3002
[53] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3976
[54] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3975
[55] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3543
[56] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3974

- VNP class "type 2" implementing 3GPP defined functionalities and virtualization layer.
- VNP class "type 3" implementing 3GPP defined functionalities, virtualization layer, and hardware layer.

For each of these GVNP types, there are generic assets and threats identified alongside security requirements. In addition to a significant number of requirements applicable from the technical baseline specified in TS 33.117, the TR 33.818 document proposes security functional requirements deriving from virtualization (see Table-1 of Appendix-F) with corresponding test cases. Several of them refer to key issues identified in TR 33.848[57] (next sub-section7.3.1).

> NOTE: other SDOs, e.g., ["O-RAN Security Requirements Specifications" (version July 2022)] have already considered the TR 33.818 security functional requirements deriving from virtualization.

7.3.1 3GPP SA3 Study on Security Impacts of Virtualisation

The scope of the TR 33.848 report states: "*The present document considers the consequences of virtualisation on 3GPP architectures, in order to identify threats and subsequent security requirements.* […] *The present document identifies security requirements which need to be addressed* [inside and] *outside of 3GPP in order for 3GPP to specify fully secure virtualised 3GPP functions.*"

TR 33.848 is developed to primarily address the security of Network Function Virtualization (NFV) as defined by ETSI. A set of security issues are considered general and applicable to any NFV deployment:

- Access to VNFs via virtualization layer
- Sharing private keys (e.g., between instances of the same VNF)
- Isolation, which persists as one the most critical issues to address in NFV
- Vulnerabilities of the physical hosts on top of which VNFs are instantiated
- Secure administration management of NFV deployments, where the one or several administration accounts remain attractive entry points for any attacker

The latest version of TR 33.848 (v0.13.0 at the time of writing) reflects a tremendous effort in identifying key security issues for aspects related to the virtualization of 3GPP functions and architectures. It already lists 30 key security issues (e.g., function isolation, container security) with security threats and potential requirements for each of them. The document also includes 8 solutions to mitigate several key issues (e.g., trust domain separation, secure bootstrap). An overview of various security areas of concern for which key issues and corresponding solutions may currently be identified in TR 33.848 is provided in Table 13-2.

7.3.2 NSA and CISA Security Guidance for 5G

[57] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574

The next subsections contain an overview of NSA and CISA guidelines on cloud infrastructure and on Kubernetes® hardening.

7.3.3 On 5G Cloud Infrastructure

In 2021, NSA and CISA released the "Security guidance for 5G cloud infrastructures" guidelines as a four-part series of publications[58] [59] [60] [61] with recommendations to approach the implementation of Zero Trust principles in 5G cloud infrastructures. As described in these publications[62], the promoted approach supports the May 2021 Presidential Executive Order on Improving the Nation's Cybersecurity.

Sometimes known as a perimeter-less security, following the "never trust, always verify" security paradigm, an operative definition of Zero Trust (ZT) and Zero Trust Architecture (ZTA) by NIST [63] is:

"Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZT architecture plan."

As stated by the NSA/CISA guidelines, the cloud-native 5G networks "will be a lucrative target for cyber threat actors". This may be considered a guiding tenet for all the efforts to develop cybersecurity strategies. Furthermore, starting from the basic assumptions that "there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership[64]", and that an attacker may already be inside the network, the ZT model enhances security by demanding explicit and continuous authorization for all interactions between resources. ZTA is necessary to protect 5G cloud deployments.

It is worth highlighting the 5G Americas Security in 5G paper[65] recommends to "Build 5G networks with a ZTA that is complemented with perimeter security to provide protection from

[58] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf

[59] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_II_Updated_508_Compliant.pdf

[60] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf

[61] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_IV_508_Compliant.pdf

[62] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[63] https://csrc.nist.gov/publications/detail/sp/800-207/final

[64] https://csrc.nist.gov/publications/detail/sp/800-207/final

[65] https://www.5gamericas.org/wp-content/uploads/2021/12/Security-in-5G.pdf

internal and external threats." As stated in 5G Americas Security in 5G[66], further information about ZT in 5G networks is provided in "Zero trust and 5G – Realizing zero trust in networks[67]", where four key security features adopted by 5G that are of most significance to enable ZTA are described:

- Secure digital identities
- Secure transport
- Policy frameworks
- Security monitoring

The ZT principles can be divided into two categories. The first category consists of principles in the design to prevent and detect wrong or threat actions. The second category consists of principles around monitoring and response.

Part 1 of the NSA/CISA series[68] "Prevent and Detect Lateral Movement" addresses prevention and detection of lateral movement in the cloud, i.e., an attacker who has successfully exploited a vulnerability to gain initial access into a 5G cloud is expected to look for unauthenticated internal services to gain more access. The recommended mitigations under the implementation of secure identity and access management (IDAM) include secure digital identities management, authenticated and authorized access to resources, security monitoring and detection of threats. The guidance related to software management address code scanning, keeping software up to date and following patch management practices (e.g., NIST SP 800-40)[69]. The secure networking aspects provide examples in terms of concrete virtualization technologies (e.g., CIS Benchmarks Securing Kubernetes®[70]), secure communication protocols (e.g., use of TLS 1.2 or later), and network access control. Recommendations on continuous monitoring and deployment of analytics systems are also provided.

In Part 2, "Securely Isolate Network Resources71[72]" [ref2], the guidelines address securing the container stack. The recommendations cover key security areas such as:

- Isolation of resources (e.g., restrict containers running in privileged mode, use of controls to prevent privilege escalation) and use of Trusted Execution Environments TEE) – (this is referred to as HMEE at ETSI NFV Chapter 7.2.3) for sensitive workloads. The TEEs can play an important role to hold the identities securely (through isolation). The TEE must be leveraged with the remote attestation.
- Hardening the container runtime (e.g., relying on Linux capabilities like seccomp), setting resource quotas.
- Implementing threat detection and incident response with examples of mitigations such as network isolating the targeted Pod, cordoning the nodes so that workloads are not scheduled on the affected node, etc.

[66] https://www.5gamericas.org/wp-content/uploads/2021/12/Security-in-5G.pdf
[67] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g
[68] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf
[69] https://doi.org/10.6028/NIST.SP.800-40r4
[70] https://www.cisecurity.org/benchmark/kubernetes
[71] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_II_Updated_508_Compliant.pdf
[72] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_II_Updated_508_Compliant.pdf

In Part 3, "Data protection"[73], the guidelines address the protection of the confidentiality and integrity of data in the multiple security domains of an infrastructure: workloads, platforms that supports the workloads, front-end and back-end networks. Overall, the recommendations represent different facets of a single goal: ensuring that only authorized services or functions have access to data within the network. Examples of recommendations to achieve the confidentiality/integrity/availability security properties in each domain include requiring that the platform supports security controls for confidentiality and integrity of data in-transit, at-rest, as well as of processes; restrict sharing of data with only authorized parties; not allowing memory inspection by any actor other than the authorized ones. Additional mitigations for the protection of data in-transit consider using secure protocols and certificate management systems. Data at-rest protection mitigations align with requirements from the "technical baseline" of 3GPP TS 33.117[74], i.e., protecting data and information in storage through encryption. The recommended mitigations for protecting data in-use are focused on leveraging TEEs.

In Part 4, "Ensure Integrity of Cloud Infrastructure" [75], the guidelines address how to ensure that 5G cloud resources (e.g., container images, templates, configuration) are not modified without authorization. On protecting the nodes, the proposed mitigations are to leverage hardware-based root of trust solutions. For ensuring the container platform integrity, recommendations include hardening the operating systems for running containers, hardening the Kubernetes® clusters, etc. For the container image management, the users should be able to store container images in an encrypted format and eventually decrypt and launch them on attested platforms. The container image design is also recommended to follow best industry practices: the container image created should be minimal (e.g., minimal numbers of layers), regularly scanned, with a controlled access to container image repositories, immutable tags, etc. Container image signing to enhance the supply chain security is also recommended.

Through this four-part series of publications, there are some primary messages:

- The cloud providers and MNOs share security responsibilities requiring operators to take responsibility to secure their tenancy in the cloud
- Strive to bring a ZT mindset into 5G cloud
- It is imperative that 5G cloud infrastructures be built and configured securely, with capabilities in place to detect and respond to threats, providing a hardened environment for deploying secure network functions
- It is critical to continuously monitor for evidence of exploitation and adversarial lateral movement within 5G cloud deployments

The Center for Internet Security (CIS) Kubernetes®[76] and Docker™ benchmarks[77] are recurrent references in these four publications. These benchmarks are also taken into account in the

[73] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf
[74] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928
[75] https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_IV_508_Compliant.pdf
[76] https://www.cisecurity.org/benchmark/kubernetes
[77] https://www.cisecurity.org/benchmark/kubernetes

Kubernetes® Hardening Guide[78] produced by NSA and CISA, introduced in the next sub-section.

7.3.4 On Kubernetes® Hardening

The NSA and CISA have recently released a Cybersecurity Technical Report (CTR) "Kubernetes® Hardening Guide" with recommendations on handling security risks associated with Kubernetes® clusters.

For the threat model, the NSA-CISA report considers that the typical sources of compromises for Kubernetes® clusters are the following:

- Attack vectors in the *supply chain*, with potential impacts at container/application, container runtime and infrastructure levels
- Malicious threat actors trying to gain access from remote locations and targeting the Kubernetes® control plane, worker nodes, and containerized applications
- Insider threats, such as administrators and containerized applications users, who can exploit vulnerabilities or abuse privileges.

As organized in the NSA-CISA report, the key recommendations may be categorized as follows:

- Kubernetes® Pod security. This includes, for example: scanning of containers and Pods for vulnerabilities or misconfigurations; applying the least privilege principle when running containers and Pods; hardening applications using SELinux® and/or AppArmor®, and define seccomp profiles; leveraging the Kubernetes® native features to enforce rules on the Pods (i.e., what Pods are allowed to do); etc.
- Network separation and hardening. For example: separating the Kubernetes® control plane components from the worker nodes; locking down access to control plane nodes using firewalls; configure TLS secure communications with certificates; secure storage of secrets at rest; etc.
- Authentication and authorization. For example: create Kubernetes®-enforced RBAC policies (e.g., so that a service interacting with Kubernetes® API server to be required to use Kubernetes® RBAC API for authentication and authorization); etc.
- Audit logging and threat detection. Examples are configure logging throughout the environment, implement log monitoring and alerting systems, persist logs to counter failures; etc. Several CNCF® (see Chapter 7.6) open-source monitoring tools are referenced (e.g., Prometheus®[79]).
- Periodically review all Kubernetes® settings and use vulnerability scans to ensure risks are appropriately accounted for and security patches are applied. For example, the CIS benchmarks for Kubernetes® are recommended.

The NSA-CISA report considers various security updates in recent Kubernetes® versions such as the deprecation of the Pod Security Policy (PSP) feature. Several security requirements discussed in this report are also exemplified through concrete configuration examples.

[78] https://media.defense.gov/2022/Aug/29/2003066362/-1/-1/0/CTR_KUBERNETES_HARDENING_GUIDANCE_1.2_20220829.PDF
[79] https://www.cncf.io/projects/prometheus/

Referenced [80]from, the open-source tool kubescape[81] may also be used to assess compliance of a Kubernetes® cluster configuration with the guidelines in this report.

7.4 Cloud Native Computing Foundation® (CNCF®)

Launched in 2015 as a part of the non-profit Linux Foundation™[82], the CNCF®[83] mission is to "make cloud native computing ubiquitous"[84] and "to drive alignment among container technologies"[85]. With support from many members[86], the CNCF® hosts 130+ projects[87] in the *graduated*, *incubating*, or *sandbox* project categories, according to their level of maturity:

- CNCF® *graduated* projects are stable, widely adopted in the industry, production ready and with thousands of contributors (see Figure 7.5-1 for the current set of graduated projects, including the prestigious Kubernetes®)
- CNCF® *incubating* projects are used in production by a small number of users with a healthy pool of contributors
- CNCF® sandbox projects are early-stage experimental projects not yet widely tested in production

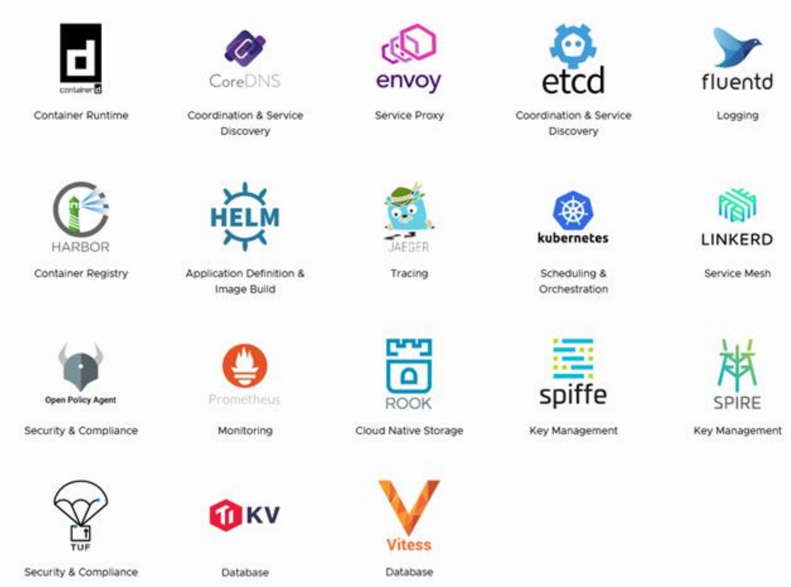


Figure 7.5-1 CNCF® Graduated Projects as of Nov. 2022 [88] (source:

[80] https://kubernetes.io/blog/2021/10/05/nsa-cisa-kubernetes-hardening-guidance/
[81] https://github.com/armosec/kubescape
[82] https://www.linuxfoundation.org/
[83] https://www.cncf.io/
[84] https://github.com/cncf/tag-security/blob/main/governance/charter.md
[85] https://www.cncf.io/announcements/2015/06/21/new-cloud-native-computing-foundation-to-drive-alignment-among-container-technologies/
[86] https://landscape.cncf.io/members
[87] https://www.cncf.io/projects/
[88] https://www.cncf.io/projects

https://www.cncf.io/projects)

Many organizations have added their own cloud native projects or products to the CNCF landscape. The full extent of the cloud native solutions falling under the CNFC umbrella may be grasped by surveying this *CNCF cloud native landscape*[89], which compiles and organizes all cloud native open-source projects and proprietary products into the following big categories[90]:

- *Layers* of the CNCF® landscape are said to build on each other: Provisioning, Runtime, Orchestration & Management, App Definition and Development are the currently defined *layers*. Every layer is further broken into sub-categories. For instance, the Provisioning layer encompassing the tools to "*create and harden* the foundation on which cloud native apps are built", includes the following sub-categories: Automation & Configuration, Container Registry, Security & Compliance, Key Management.

- *Columns*, namely: (1) *Observability and Analysis*[91], including the Monitoring, Logging, Tracing, Chaos Engineering sub-categories of projects; (2) *Platforms*, which include tools bundled together from different layers to solve a larger problem; since "all platforms revolve around Kubernetes®" [92], the four defined sub-categories of platforms are: Certified Kubernetes® – Distribution, Certified Kubernetes® – Hosted, Certified Kubernetes® – Installer, and PaaS/Container Service.

Many projects and products, in various CNCF® defined categories, are directly related to security. For example, the Security and Compliance [93] set of projects at the Provisioning *layer*, comprise 81 projects (of which 18 are CNCF projects, including the OPA™[94] and TUF™[95] *graduated* projects) to address security topics such as: image management (signing, scanning, etc.), policy enforcement, audit, certificate management.

The CNCF landscape also includes a CI/CD category[96] covering tools to enable fast and efficient development with embedded quality assurance. For the specific secure CI/CD and supply chain area, the CNCF® Security Technical Advisory Group published a reference whitepaper[97] with recommendations on how to design a secure software supply chain. Four key principles are promoted, in line with:

- Trustworthiness of each step in the supply chain
- Automate everything (to reduce human errors)
- Clearly defined build environments, with limited scope and authorization
- Mutual authentication between all human and machine participants

[89] https://landscape.cncf.io/
[90] https://landscape.cncf.io/guide#introduction--what-is-the-cloud-native-landscape
[91] https://landscape.cncf.io/guide#observability-and-analysis
[92] https://landscape.cncf.io/guide#platform
[93] https://landscape.cncf.io/guide#provisioning--security-compliance
[94] https://www.openpolicyagent.org/
[95] https://theupdateframework.io/
[96] https://landscape.cncf.io/card-mode?category=continuous-integration-delivery&grouping=category
[97] https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/sscsp.md#executive-summary

The list of projects that become part of the CNCF® landscape gets larger as new needs and business opportunities arise. Likewise, the rising number of graduated and matured projects demonstrates the positive aspects of open-source software and the engagement of the developer community towards providing secure services and useful applications for the cloud. However, 5G and future public mobile networks depend on a high degree of standardization to be able to prevent vendor lock-in and increasing the potential for vendor competition and improve supply chain security. Hence, matured projects must be absorbed into standards specification if they are to be used in inter VNF solutions or remain more confined to intra VNF implementations where that can help in VNF vendor competition.

8 Recommendations

8.1 Actions to Promote Secure Virtualized 5G Deployments

8.1.1 Intra Government Partnering

For the supply chain, we encourage the FCC to consider ways to partner across the federal government to continue to incentivize digital solutions in 5G network deployments to mitigate supply chain risk.

- Software security technologies designed into software packages or code can address security risks by ensuring trust and preventing software from being exploited by bad actors or for malignant uses.
    - The ability to deploy trusted software updates, including the firmware of compromised devices.
    - Automating security policies to, for example, seek out and prevent placement of user or administrator credentials in software code.
- Encouraging use of software bills of materials (SBOMs), as defined by NTIA and CISA, to convey evidence of trust for the environment in which software was built.
- Hardware security technologies built into hardware infrastructure can further protect against supply chain risks. Solutions include but not limited to:
    - hardware roots-of-trust to verify, protect, or restore system, data, or code integrity.
    - Secure co-processors for more robust identity verification.
    - Origin and identity attestation for components in a hardware system.
- For sensitive applications, data security technologies can protect confidential data through the supply chain. Solutions include but not limited to:
    - Digital rights management,
    - Information flow controls,
    - Data tagging and,
    - Where appropriate, the use of secure virtual or data lockbox environments.

We encourage the FCC to monitor and collaborate with other government agencies who have similar concerns and are undertaking proactive actions or developing tools (e.g., NIST cyber security framework, NIST AI risk management framework, DoD, Intelligence Community, etc.) relevant to the secure and successful application of virtualization and related technologies including Zero Trust.

- To facilitate adoption of virtualization and cloud technologies, the FCC may need to undertake a review of current metrics (e.g., outage tracking) used in regulation of communications service providers.

8.1.2 Public Private Sector Partnering

We encourage the FCC to convene a virtualized 5G industry information sharing group comprised of experts from government, research, academia, service providers, and equipment providers. This syndicated development of common patterns of migration could be convened and incented including driving standards development or product capabilities (analogous to the allowances that 5G non-standalone option affords).

This group would securely exchange data on operational issues/concerns, best practices/processes, metrics, security issues/remediation, and operational learnings that emerge from the application of virtualization technology to 5G deployments. Consider an ISAC-like structure (Info Sharing & Analysis Center) where different factions (even competitors) collaborate and share for the benefit of the US national interests.

- The partnership would share knowledge and develop ‘playbooks’ of specific recommendations and best practices for leveraging virtualization in the deployment of 5G (and beyond) networks. This concept is like the Telecomm Security Requirements proposed by the UK’s National Cyber Security Center[98](NCSC).
- The playbooks would include advice on migration and legacy technology coexistence scenarios.
- The playbooks would be voluntary and advisory but maintained in an ongoing / living forum such that evolving best practices and knowledge can be continually applied.

8.2 Overcoming Obstacles and Increasing Vendor Diversity

To overcome obstacles and increase 5G vendor diversity for virtualized systems including Distributed Unit (DU), Central Unit (CU), Radio Unit (RU) and Service Based Architecture (SBA), the Workgroup recommends:

- Industry certifications can increase confidence in the software delivered and deployed.
  - Industry should continue to use its existing processes for equipment certification. Industry should also evaluate the need and relevance to establish a new

[98] https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector

certification for the deployment of network functions in virtualized environments.

- Provide incentives for rural carriers to improve security.
    - The FCC should also consider creating incentives for rural carriers to improve their security, including by taking advantage of the scale enjoyed by the large MNOs, which can be achieved by small carriers through use of cloud-based services. These incentives might be financial, e.g., though the Universal Service Fund or rip-and-replace programs.

To address best practices for reliability and interoperability by enabling the 5G ecosystem to be open and create interworking between small and large vendors in the same 5G system.

- In line with the recommendations in 8.1.1, we encourage both the FCC and NIST (and other U.S government agencies as necessary) via the interagency process to develop consistent and co-branded guidance, rather than through individual agency efforts to manage an iterative process focused on realizing the intended security and assurance outcomes.

- Use existing processes established after the May 2021 Executive Order on Improving the Nation’s Cybersecurity for Federal agencies to enhance 5G software security assurance, this would foster continued collaboration and partnership between and among agencies and vendors by increasing transparency and as-needed information exchange, facilitating shared security expectations, and building trust needed to make informed risk decisions.
    - It would recognize and embrace the diverse software ecosystem (from single person opensource projects to multinational enterprises), the breadth of technologies, and the pace of innovation.
    - Threat actors have learned that they are more powerful when they collaborate and continuously evolve, and in an ideal process, software participants would similarly scale knowledge, efficiencies, and improvements.
    - We believe the foundation of this ideal process is the automated secure exchange of verifiable software artifacts between all participants in a supply chain.
- Creating recommendations for isolation in a multi-tenant cloud environment.
- Creating recommendations for multi-cloud deployment architectures.

8.3 Skilling Needed to Support Virtualized 5G Networks

- Build the Workforce**.** Cloud based 5G networks will bring more diversity and innovation to the 5G and next generation wireless networks. For the technology and the new entrants in the market to be successful, the operators, the system integrators, and anyone involved in deploying these networks will need to be trained and qualified. As this is a new technology, it is reasonable to expect that we do not yet have a sufficiently trained workforce, and investment in skilling will be required.
- Specifically, provide support in building and sustaining a leading talent pipeline which

emphasizes Radio / RF and the crossover capabilities between the IT and Telecom domains.
- Support creation of certification for virtualized telco environments.

9 Conclusions

The scope of this report covers the widespread adoption of virtualization practices originally developed for the IT market within the 5G domain. Most 5G deployments at scale are expected to be hybrid legacy and virtualized network elements. To achieve a completely cloud-native implementation of a RAN and Core network, it will be necessary to migrate, in place, a large multi-vendor and complex legacy installed base of traditional equipment and deployment paradigms that date back decades. Since the installed base represents a very large investment, with a long-life cycle, it will likely need to be amortized over time. Thus, there will be a lengthy period of co-existence and each service provider will have unique circumstances to contemplate. Inter-agency Governmental and private sector cooperation is paramount to ensure system, financial and ecosystem integrity.

10 Appendix A – Glossary of Acronyms

Abbreviation	Definition
3GPP	3rd Generation Partnership Project, https://www.3gpp.org/
5G	Fifth Generation
5GC	5G Core
5GS	5G System
AI/ML	Artificial Intelligence / Machine Learning
AN	Access Network
API	Application Programming Interface
CBRS	Citizens Broadband Radio Service
CI / CD	Continuous Integration / Continuous Delivery
CISA	Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/
CONUS	Continental United States
CoS	Class of Service
CSC	Communication Service Customer
CSP	Cloud or Communication Service Provider
CSRC	Computer Security Resource Center, https://csrc.nist.gov/
CU	Central Unit
DDoS	Distributed Denial of Service
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency, https://www.disa.mil/
DMCC-S	DoD Mobility Classified Capability-Secret
DMUC	DoD Mobility Unclassified Capability
DN	Data Network
DNN	Data Network Name

DoD	Department of Defense
DSCP	Differentiated Services Code Point
DU	Distributed Unit
E2E	End to End
eNB eNodeB	E-UTRAN Node B, also known as Evolved Node B, is the element in E-UTRA of LTE that is the evolution of the element Node B in UTRA of UMTS
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FW	Firmware
gNB	node providing NR user plane and control plane protocol terminations towards the UE, and connected via the NG interface to the 5GC
GSMA	Global System for Mobile Communications Association, https://www.gsma.com/
GST	Generic Slice Template
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force, https://www.ietf.org/
IIoT	Industrial Internet of Things
LTE	Long-Term Evolution
MANO	Management Automation and Network Orchestration
MEF	The Metro Ethernet Forum, https://www.mef.net/
NF	Network Function
NFV	Network Function Virtualization
NFVIaaS	Network Function Virtualization Infrastructure as a Service
ng-eNB	node providing E-UTRA user plane and control plane protocol terminations towards the UE, and connected via the NG interface to the 5GC
NG-RAN Node	either a gNB or an ng-eNB.
NIPRnet	Non-classified Internet Protocol (IP) Router Network
NIST	National Institute of Standards and Technology, https://www.nist.gov/
OCONUS	Outside of the Continental United States
ORAN	Open Radio Access Network
PCP	Priority Code Point
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
SCA	Side Chanel Attack
SDN	Software Defined Networking
SDO	Standards Developing Organization
SD-WAN	Software Defined Wide Area Network
SIPRNet	Secret Internet Protocol Router Network
SLO	Service Level Objective
SLR	Service Level Requirement
UDM	Unified Data Management

UDR	Unified Data Repository
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VMM	Virtual Machine Manager
VNF	Virtual Network Function
VNFaaS	Virtual Network Function as a Service
ZT	Zero Trust

11 Appendix B – List of Threats

WG3 PAPER: APPENDIX – DRAFT V1.0
Potential Threat Vectors to 5G Network

The 5G virtualization of specialized RAN components (i.e., open hardware equipment, software, and interfaces) to ensure interoperability in a multi-vendor ecosystem provides further standardized disaggregation of the RAN, potentially expanding the threat surface and introducing potential new security risks. Although traditional RAN has S1-C, S1-U, X2-C, X2-U, F1, E1, and Fronthaul interfaces that are each similarly prone to a range of like threats, the O-RAN architecture introduces additional interfaces, thus increasing the threat surfaces. Many of the new types of threats are anticipated to be those related to inter-vendor operation.

It is safe to assume that the risks associated with the Open RAN (ORAN Alliance) architecture can be reasonably generalized to 5G network deployments by virtue of introducing the Open Fronthaul (FH) interface, including the addition of the Near-Realtime (RT) RAN Intelligent Controller (RIC) and Non-RT RIC functions as the fundamental gateway in any 5G network allowing access to the overall virtualized RAN environment including its core and backhaul.

The range of anticipated 5G threats, derived in cooperation with CSRIC VIII Working Group 2 (WG2), is listed in Table A-1, providing a ready-reference compendium of threats to develop and implement mitigation steps for reducing potential security risks.

Although most security technologies to thwart threats are focused on keeping the attacker and malicious entities outside of the network, oftentimes attackers will be successful in compromising portions of the 5G/ORAN network through alternate or backdoor mechanisms and by exploiting vulnerabilities due to a lack of measure. To ensure reliability, recovery from compromises needs to be accomplished rapidly and with minimal manual effort as possible. This is especially important in 5G/ORAN far-edge scenarios where the large number of sites and virtualized elements makes it prohibitively expensive to send technicians into the field for recovery.

Thus, an increasing area of concern is 5G's ability to self-heal and automatically recover from failures and security breaches. This is increasingly important as malware and ransomware are being weaponized by nation states whose goal is to take down critical infrastructure. Disrupting communications is a prime target for nation states, and this can be accomplished by infecting

5G/ORAN infrastructure with code which, on command, can take down a radio access network, a MEC server, or the packet core network. Ransomware is a rising threat for telecommunications and is considered in Table 13-1.

Table 11-1 5G Threat Matrix (Virtualization Focus)

Security Threat	Target Point/ Network Element	Vulnerability Attack Mechanism	Affected Technology	Security Concern C- Confidentiality I- Integrity A- Availability
Resource (slide) threat	5G/Open FH RU and DU interfaces primarily at S-Plane on the PTP network at radio layer interface Hypervisor, shared cloud resources	Similar to replay attack threat but focused on resource degradation to take control of the network	NFV, Cloud	C, I, A
Jamming attacks	5G/Open FH RU and DU interfaces primarily on the PTP network at radio layer interface	Electronic signals used to overpower the functionality and performance of 5G systems opens up attack surfaces by desensitizing and accessing VMs and virtualized layers	SDN, NFV	C, I, A
Distributed Denial-of-Service (DDoS) attacks to degrade network resources (See Table A-2 for additional attack variants)	5G/Open FH RU and DU interfaces and Centralized control elements primarily at S-Plane on the PTP network at radio layer interface	Attacker conducts malicious tasks to prevent the legitimate parties from accessing the resources of the network or system and coded packets are sent under these attacks to rapidly consume bandwidth resources of the targeted system Malicious routing and bringing down the network Three broad types of DDoS attacks: Application layer attacks (where the server generates the response to an incoming client request, Protocol attacks, and Volumetric attacks.	SDN, NFV, Cloud, IoT, 5G	I, A
Virtualized functions or assets not independently secured or that rely on perimeter protection	Virtualized RAN functions that migrate to the cloud	5G cloud deployments may reside in a 3rd-party's facility, such as with MEC, a 3rd-party may be managing infrastructure, and the software platform has components from other 3rd-parties with potential vulnerabilities	Cloud, NFV	C, I, A
Inadequate or insufficient orchestrated security controls that leverage AI/ML and that	Each RAN vendor will need to interact with transport and aggregation layer RT controls within network slice and	Within service provider 5G networks, each RAN vendor must adhere to orchestrated security controls which will leverage AI/ML for real-time threat and anomaly detection.	SDN, NFV	C, I, A

affect real-time threat and anomaly detection	platform for RIC in case of virtual network function migration due to node failure arising from cyberattack or equipment failure.			
Configuration attack threat	SDN (virtual) switches and routers	Attacker gains control of switch settings for routers and other virtualized equipment to set/rest to their advantage	SDN, NFV	C, I, A
Saturation attack threat (Similar to replay attacks but using multiple, simultaneous disruption stimuli)	SDN controller and switches	Attacker saturates and overpowers network functions thereby degrading network response allowing for control/manipulation of virtualized components	SDN	C, I, A
Penetration attack threat	Virtual resources, cloud, IoT	Surgical penetration of network vulnerability points or entry to gain specific control of selected network elements of functions	SDN, NFV, Cloud, IoT, 5G	C, I, A
User identity theft threat	User information database	Like impersonation threat but specifically targeting virtualized cloud database domains	SDN, NFV, Cloud, IoT, 5G	C
TCP level attack threat	SDN controller-switch communication	Attacker induces pauses, interrupts, and rerouting of critical data or access	SDN, IoT, 5G	C, I, A
Reset & IP spoofing attack threat	SDN control channels	Attacker exploits control channel to gain control, reset switches, and conduct spoofing (imposter) attacks	SDN	C, I
Scanning attack threat	Open air interfaces	Similar to passive eavesdropper scenario but more aggressive in ascertaining network states and spectrum bands that can be actively exploited in subsequent deeper attacks	IoT, 5G	C, I
Security keys exposure attack threat	Unencrypted channels associated with IoT and 5G network	Exposing and sharing key management, user/device authentication, and user access control to soften entry and create additional entry points peering into the 5G network and IoT data interfaces	IoT, 5G	C, I
Semantic information attack threats	Subscriber location Virtual modems	Attacker detects and deflects search capabilities to degrade network functionality and reduce situational awareness	IoT, 5G	C, I
Open-source ecosystem threat	Affects all levels of virtualization deployment and maintenance	Open source enables a diverse multivendor ecosystem and promotes interoperability but also opens possibilities up for bad actors	SDN, NFV, Cloud	C, I, A

Secure 5G/Open RAN DevSecOps CI/CD	Affects all levels of virtualization deployment and maintenance	Evolution of Secure Software Development CI/CD enables software developers to frequently deliver code changes to respond to security threats and vulnerabilities.	SDN, NFV, Cloud	C, I, A
Policy and standards threats	Affects all levels of 5G/O-RAN virtualized machines	Proprietary and market forces (including non-trusted sources) could introduce gaps in the network and open the door for malicious threat actors Open standards Optional v. mandatory controls University resistance to controls	SDN, NFV, Cloud, IoT, 5G	C, I, A

12 Appendix C - Mitigation Considerations

Type of Risks	**Mitigation Techniques**	**Standards Sources**
Supply Chain Risks	To ensure a high level of security and resilience for end-products, suppliers need to have a secure product development process and to have security by design as a basic principle, systematically and verifiably applied. In the case of 5G networks, where key elements will be software-based, this process must take particular care of matters such as secure software development, security assessment and testing, version control, secure software update and alike. This would typically also include systematic source code review process, application of coding best practices, use of static and dynamic code analysis, external code review process and individual product vulnerability scanning. Suppliers need to have adequate measures in place to adequately manage such security risks. The role of authorities in ensuring the adequate level of security for products and equipment that will be built in the 5G networks deployed nationally depends on specific legal framework adopted and the related regulatory powers. The Open RAN ecosystem should follow industry best practices for the development of a trusted supply chain of rApps and xApps, to include the development of secure application development guidelines, processes for independent evaluation, processes for vulnerability assessments, recommendations on the development of applicable software bill of materials (SBOM), software integrity mechanisms, and a common approach for secure onboarding of rApps and	Open Radio Access Network Security Consideration, by NSA and CISA, 2022 ENISA Security in 5G Specifications, Controls in 3GPP Security Specifications (5G SA), Feb 2021 NIST SP 800-171 Rev.1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022

	xApps	
Cross VM shared resource threats Security Operation Threats Multi-Tenant AAA risks 5G Microservices Threats	Use network separation to control the amount of damage a compromise can cause. Use firewalls to limit unneeded network connectivity and use encryption to protect confidentiality. Use strong authentication and authorization to limit user and administrator access as well as to limit the attack surface. Capture and monitor audit logs so that administrators can be alerted to potential malicious activity. Periodically review all Kubernetes® settings and use vulnerability scans to ensure risks are appropriately accounted for and security patches are applied Use HSM (Hardware Security Module) to defend against SCA type of attacks.	Kubernetes® Hardening Guide, Cybersecurity Technical Report, U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), v1.2, August 2022. Open Radio Access Network Security Consideration, by NSA and CISA, 2022
Container Image threats Platform exploits threats Multi-Vendor VNF Threats	Run containers and Pods with the least privileges possible. Scan containers and Pods for vulnerabilities or misconfigurations. Capture and monitor audit logs so that administrators can be alerted to potential malicious activity. User container-specific host OSs instead of general-purpose ones to reduce attack surfaces Deploy container-specific vulnerability management tools and process for images to prevent compromises. Consider using hardware-based counter measurements to provide a basis for trusted computing. Use container-aware runtime defense tools.	NIST SP 800-190, Application Container Security Guide, Souppaya, M., Morello, J., Scarfone, K., U.S. NIST, September 2017.
NFV Infrastructure Security Threats VNF (Virtualized Network Function) Threats Network Slicing threats	HSM measurements provide the verification of the system integrity. The BIOS, Firmware, and connected hardware components can be measured so that a good known boot state is verified, or any changes can be detected. Deploy tamper-resistant and cryptographically signed hardware labeling system to provide identification of system assets and resources to prevent mislabeling attacks.	NIST SP 1800-33B 5G Cybersecurity ETSI GS NFV-IFA 032 V4.3.1. Network Functions Virtualization (NFV) Release 4; Management and Orchestration; Interface and Information Model Specification for Multi-Site Connectivity Services; Annex C, Risk and Regulatory Concerns; Annex D,

	Remote attestation provides proof of system integrity. Encrypt VNF workload image in the shared storage location, and enforce the security policy governing access to the decryption key Use infrastructure security monitoring tools to identify suspicious activities In network design, segment network helps to apply policy driven access control.	Risk Analysis and assessment
API Security Risks	Enforce the regular updating of the asset management processes to include all API endpoint servers, also require removing older APIs from all production environments. Enforce the updating of the log management system, deploy the security information and event management (SIEM).	NIST SP 800-128, Guide for security-focused configuration management of information systems.

13 Appendix D – 3GPP SA3 Virtualization Aspects

Based on 3GPP TR 33.818, a set of security functional requirements deriving from virtualization is provided in Table 13-1 below. Many of these requirements are related to ETSI NFV specifications.

Table 13-1 Security requirements derived from virtualization in 3GPP TR 33.818 (v17.1.0)

Requirement Name	Requirement Description	TR 33.818 related section
VNF package and VNF image integrity	1) VNF package and image shall contain integrity validation value (e.g., MAC). 2) VNF package shall be integrity protected during on boarding and its integrity shall be validated by the NFVO.	5.2.5.5.3.3.5.1
GVNP lifecycle management security	1) VNF shall authenticate VNFM when VNFM initiates a communication to VNF. 2) VNF shall be able to establish securely protected connection with the VNFM. 3) VNF shall check whether VNFM has been authorized when VNFM access VNF's API. 4) VNF shall log VNFM's management operations for auditing.	5.2.5.5.7.1
Secure executive environment provision	The VNF shall support comparing the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The	5.2.5.5.7.2

	VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.	
Instantiating VNF from trusted VNF image	A VNF shall be initiated from one or more trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the operators.	5.2.5.5.7.3
Traffic Separation	The virtualized network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 [x] for further information.	5.2.5.5.8.5.1
Inter-VNF and intra-VNF Traffic Separation	The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affect each other.	5.2.5.5.8.5.2
Secure virtualization resource management	1. To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, the VNF shall alert to the OAM when the VNF cannot detect a VNFC message. 2. A VNF shall log the access from the VIM.	5.2.5.6.7.2
Secure executive environment creation	When an attacker tampers with a driver which was provided by the hardware and used to create the executive environment, the virtualization layer shall alert the driver error to the administrator for checking the error and finding the attack at latter.	5.2.5.6.7.3
VM escape protection	To defend the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualization layer and then control the layer, the virtualization layer shall implement the following requirements: The virtualization shall reject the abnormal access from the VNF (e.g., the VNF accesses the memory which is not allocated to the VNF) and log the attacks.	5.2.5.6.7.4
Secure hardware resource management	The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.	5.2.5.7.7.2
Secure hardware resource management	When a compromised Virtualization layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the	5.2.5.7.7.3

information	hardware, the hardware shall trigger an alert. The administrator can check the alert and find the attack at latter. Note: Whether the virtualization layer is trust or not is based on operator's decision.	
Trusted platform	The host system shall implement a Hardware-Based Root of Trust (HBRT) (e.g., TPM, HSM)) as Initial Root of Trust [ref-ETSI-NFVSEC-012]. The trust state of the platform shall be measured, and a trusted chain shall be built [ref-ETSI-NFV-SEC008].	5.2.5.7.7.4

An overview of various security areas of concern for which key issues and corresponding solutions may currently be identified in TR 33.848 (v0.13.0) is provided in Table 15-2 below.

Table 13-2 Key security issues to solutions mapping in TR 33.848 (v0.13.0)

Area of concern	Key issue short description	Key issue#	Solution#
Network Functions (NFs)	Establishment of trust domains for NFs	1	1
	Availability of NFs	3	2
	Isolation	6	4
	Location: where is my NF?	12	1
	Attestation of 3GPP function level	13	1, 4, 5, 6
	Mixed VNF and physical NF deployments	16	
	Sensitive VNF pinning (related to a specific HW)	30	
	VNF lifecycle management and migration	29	
	Startup paradox for sensitive VNFs	18	
	Test isolation and assurance	8	
VM & Hypervisor	Breakout	21	
Containers	Security	25	4
	Breakout	26	
	Secrets embedded in images	27	
Management	Single point of failure	22	7
	APIs	28	
	Single administrator domain	10	3, 7
	Third party hosting (confidentiality of data, attestation of hosting environment)	20	
Data	Confidentiality of sensitive data	2	2
	Data location and lifecycle	5	2
	Storage and location of keys and data	11	1
	Encrypted data processing	15	4
	Data synchronicity through network	24	

	Memory introspection	7	4
	VNF host spanning (read data in transit)	14	2
	Software catalogue image exposure (integrity and confidentiality protection)	17	
NW slice	Trust domain and isolation	9	1, 8
	Time information manipulation	19	
Others	IP layer (IPsec) vs. Application layer (TLS) security	23	
	Common SW environment	4	2

NOTE: Annex B of TR 33.848, which is reserved to include a summary of the identified key security issues and how the various proposed solutions address them is expected to supersede the Table 15-2 mapping.